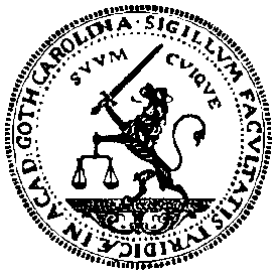

JURIDISKA FAKULTETEN

VID LUNDS UNIVERSITET

Emma Folkesson

En bakdörr till effektiv brottsbekämpning

Straffprocessrättens hindrande av end-to-end-krypterad kommunikation

JURM02 Examensarbete

Examensarbete på juristprogrammet

30 högskolepoäng

Handledare: Karol Nowak

Termin: HT 2023

Innehåll

Summary

A concerning development of organized crime in Sweden has caused debate about the state's ability to uphold law and order effectively. At the same time, increased access to, and use of, encrypted communication services amongst criminals poses a challenge to law enforcement agencies. Closed end-to-end encrypted communication services hampers the use of covert coercive measures in law enforcement. Existing legislation regarding authorities access to the content of electronic communication are insufficient given today's encryption technology.

In the European Union and the United Kingdom, emerging regulatory proposals aim to impose obligations on communication service providers to monitor all communication on their platforms for specific illegal content. The Chat Control Regulation and the Online Safety Bill therefore both constitute direct hindrances to end-to-end encryption in communication services. In Sweden, similar legislation is being considered to impose liability on communication service providers to facilitate the enforcement of secret coercive measures. Such liability effectively means that end-to-end encrypted services cannot technically be provided.

The essay's primary objective is to examine the function of Swedish criminal procedure law in the context of legislation seeking to restrict encrypted communication. The essay conclude that criminal procedure law is characterized by populist criminal justice policy. Through a policy argumentation and legal analysis, the essay first establish that the current political climate affects the views and opinions on the function of criminal procedure law. Moreover, the current judicial landscape indicates an offensive approach toward an effective law enforcement policy. The essay concludes that legislation restricting end-to-end encryption aligns with the prevailing understanding of the function of criminal procedure law. However, the technical complexity of the regulatory framework is problematic, and it is important that thorough preparatory legislative drafting is properly implemented to ensure that the regulation is comprehensible to the public.

Sammanfattning

En oroväckande utveckling av organiserad brottslighet i Sverige har skapat debatter om rättssamhällets förmåga att upprätthålla lag och ordning. Samtidigt har en ökad tillgång till, och användning av, krypterade kommunikationstjänster inom den kriminella verksamheten försvårat brottsbekämpande myndigheters arbete. Slutna end-to-end-krypterade kommunikationsmöjligheter begränsar möjligheten att effektivt använda straffprocessuella tvångsmedel i brottsbekämpningen. Nuvarande reglering av myndigheters åtkomst till innehållet i elektroniska kommunikationer är inte tillräcklig för att hantera dagens krypteringstekniker.

I EU och Storbritannien avser nya lagförslag att införa skyldigheter för leverantörer av kommunikationstjänster att skanna all kommunikation för särskilt olagligt material. Både Chat Control-förordningen och Online Safety Bill utgör därmed direkta hinder för end-to-end-kryptering i kommunikationstjänster. I Sverige utreds en liknande lagstiftning som bland annat ska ansvarsbelägga leverantörer av kommunikationstjänster att möjliggöra för verkställandet av straffprocessuella tvångsmedel. Ett sådant krav innebär att end-to-end krypterade tjänster inte tekniskt kan upprätthållas.

Uppsatsens huvudsakliga syfte är att granska den svenska straffprocessrättens funktion i relation till lagstiftning som vill begränsa möjligheten till krypterad kommunikation. Uppsatsen konkluderar att straffprocessrätten präglas av en dynamisk karaktär som är nära kopplad till en populistisk kriminalpolitik. Genom en rättsanalytisk metod och rättspolitisk argumentation konstateras först att rådande politiska läge påverkar synen på straffprocessrättens grundläggande samhällsfunktion. Vidare fastställs att nuvarande rättsläge indikerar en offensiv syn på effektiv brottsbekämpande lagstiftning. Slutsatsen dras att regelverk som begränsar kryptering överensstämmer med rådande uppfattning om att straffprocessrätten ska verka för en effektiv brottsbekämpning. Den tekniska komplexiteten i regelverket är dock problematisk, och det är viktigt att noggranna lagförberedande utredningar genomförs för att säkerställa att regelverket är begriplig för allmänheten.

Förord

Med en gedigen timme till godo vill jag tacka juristprogrammet i Lund för min gränslösa förmåga att hantera tidspress på minimalt med sömn. Jag ser fram emot att utveckla detta vidare i min framtida karriär!

I övrigt vill jag särskilt tacka min pappa, som oavsett uppsatsämne eller tid på dygnet lyckas glida in med en relevant artikel i min mailinkorg. Jag vill också uppmärksamma min gamla svensklärare till morfar som alltid ger mig viktiga lektioner i ett semikolons placering dagen innan inlämning.

Självklart vill jag också rikta ett stort tack till min handledare Karol som har kommit till undsättning vid ett flertal kritiska tillfällen under processens gång.

Jag kommer att sakna den ändlösa tillgången till kaffe på Juridicums fjärde våning, men nu är det dags att ge sig av!

Stockholm, 3 januari 2024 klockan 09:43.

Emma Folkesson

Förkortningar

Chat Control-förordningen	Förslag till Europaparlamentets och rådets förordning om fastställande av regler för att förebygga och bekämpa sexuella övergrepp mot barn, COM(2022) 209 final
CSAM	Child sexual abuse material
Förordningen om tillfälligt undantag	Europaparlamentets och rådets förordning (EU) 2021/1232 av den 14 juli 2021 om ett tillfälligt undantag från vissa bestämmelser i direktiv 2002/58/EG vad gäller användning av teknik hos tillhandahållare av nummeroberoende interpersonella kommunikationstjänster för behandling av personuppgifter och andra uppgifter i syfte att bekämpa sexuella övergrepp mot barn på nätet
E2E-kryptering	End-to-end kryptering
E-dataskyddsdirektivet	Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation
E-handelsdirektivet	Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden
EU	Europeiska unionen
HDA	Lag (2020:62) om hemlig dataavläsning
Kodexdirektivet	Europaparlamentets och Rådets direktiv (2018/1972) av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation
LEK	Lag (2022:482) om elektronisk kommunikation
Preventivlagen	Lag (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott
Prop.	Proposition
SOU	Statens offentliga utredningar

1 Inledning

1.1 Bakgrund

Under september 2023 var det 11 personer i Sverige som sköts till döds. Det är den högsta månadssiffran sedan polisen började föra statistik över det dödliga skjutvapenvåldet år 2016.[1] Den bekymmersamma utvecklingen har väckt en oro över samhällets förmåga att upprätthålla ordning och säkerhet, särskilt i ljuset av den organiserade brottsligheten i Sverige. En aspekt som återkommande diskuteras är den ökade användningen av krypterade kommunikationstjänster inom den kriminell verksamheten. Den moderna och lättillgängliga tekniken försvårar för brottsbekämpande myndigheter i arbetet med att förhindra och utreda allvarlig brottslighet.[2]

Dagens teknik möjliggör för avancerad kryptering på våra mest använda digitala kommunikationsplattformar. För tjänster som exempelvis Apple's iMessage, Facebook's Messenger, Signal och WhatsApp tillämpas end-to-end kryptering. Krypteringstypen innebär att meddelanden som skickas från en avsändare till en mottagare är fullständigt krypterade och inte kan läsas av någon tredje part. Det utgör en utmaning för brottsbekämpande myndigheter när befintliga tekniska verktyg som används för att lokalisera, övervaka och förhindra brottslighet blir mindre effektiva eftersom den krypterade information inte kan nås.[3]

Brottsbekämpande myndigheter har återkommande höjt rösten för hur krypterade kommunikationstjänster underlättar för den organiserade brottslighetenen.[4] I Sverige har det exempelvis framkommit hur kriminella nätverk rekryterar, planerar och koordinerar sina verksamheter genom användandet av krypterade kommunikationssystem.[5] I syfte att hantera de utmaningar som krypterade kommunikationssystem innebär för

[1] Schwartz & Wiklund (2023); Polisen, *Sprängningar och skjutningar - Polisens arbete*.
[2] SOU 2022:52 s. 125-130; Prop. 2022/23:126, s 67-72.
[3] Prop. 2019/20:64 s. 56 och 66; Prop. 2022/23:126, s 67-72.
[4] SOU 2017:89 s. 201-202.
[5] SOU 2022:52 s. 125-130; se exempelvis Hovrätten för Västra Sverige, dom 2022-04-08, mål nr B 6938–21, s. 23-30; Svea hovrätt, dom 2022-04-21, mål nr B 1462–22, s. 48-49.

brottsbekämpningen pågår en politisk debatt kring vilka verktyg som brottsutredande myndigheterna bör ha tillgång till i sitt arbete. Två initiativ som särskilt diskuteras i uppsatsen är Storbritanniens Online Safety Bill och EU:s Chat Control-förordning. Båda lagförslag vill införa ett ansvar för leverantörer av kommunikationstjänster att kunna skanna allt innehåll på deras plattformar. De nya regelverken försöker hantera utmaningarna med kryptering genom att reglera i vilken utsträckning tjänsteleverantörer tillåts erbjuda och upprätthålla krypterade kommunikationsmiljöer på marknaden.[6]

Den pågående debatten berör en avvägning mellan perspektiv för brottsbekämpning och en rätt till säker kommunikation. Inom den svenska straffprocessrätten är den övergripande funktionen att skydda samhället, en uppgift som konstant måste balansera mellan en effektiv brottsbekämpning och respekten för individens rättigheter.[7] En aktuell problemformulering är hur den ökade användningen av end-to-end-krypterade kommunikationer kan regleras och begränsas för att tillgodose straffprocessuella behov i Sverige.

1.2 Syfte och frågeställning

Uppsatsens syfte är att utreda hur den svenska straffprocessrättens grundläggande funktion förhåller sig till sådan lagstiftning som vill begränsa möjligheten till en säker och krypterad elektronisk kommunikation. Genom att undersöka och redogöra för den svenska straffprocessrättens och kriminalpolitikens utveckling, analysera lagstiftningen för brottsbekämpande myndigheters tillgång till elektronisk kommunikation i Sverige och granska förslag på regelverk som förespråkar statlig insyn i all krypterad elektronisk kommunikation, är uppsatsens avsikt att besvara frågeställningen:

I vilken utsträckning kan den svenska straffprocessrättens grundläggande funktion anses förenliga med lagstiftning som begränsar användningen av end-to-end-krypterade kommunikationsmedel?

[6] Se exempelvis Svar på skriftlig fråga JU202 3/00879, 2022/23:526; Woodhouse (2022) *Analysis of the Online Safety Bill*, s. 116-119; SOU 2023:22, s. 3-4 och 21.
[7] Se exempelvis Packer (1964), s. 6-9 och13-19; Jareborg (2001), s. 20; SOU 2022:19 s. 69.

1.3 Forskningsläget

Det finns flera forskningsområden som är relevanta att ta ställning till för uppsatsens syfte. Dock ska noteras att forskning som specifikt berör en reglering av elektronisk kommunikation på ett sätt som förhindrar användandet av end-to-end-kryptering inte är särskilt omfattande. Särskilt bristfällig är forskningen i förhållande till det svenska rättssystemet där ämnet främst har behandlats av statliga utredningar och intresseorganisationer i samband med lagutredningar och debatter. Hittills har ingen etablerad doktrin eller forskning presenterats, vilket utgör en ingång för uppsatsens inriktning.

Generellt kan konstateras att regelverk mot användningen av krypterade kommunikationsmöjligheter i brottsbekämpande syfte ständigt utvecklas och påverkas av teknologiska framsteg. En konsekvens är att den snabba och avancerade tekniska utvecklingen gör att forskningen ofta hamnar efter. Ämnet har blivit relevant i takt med ökad användning av krypteringstekniker och ökad oro för att teknikerna underlättar för brottslig verksamhet. En betydande del av befintlig forskning fokuserar därför på etiska överväganden kring reglering av krypterade kommunikationsmedel i förhållande till potentiellt begränsande lagstiftning mot mänskliga rättigheter. Det finns omfattande forskning och praxis som behandlar rätten till integritet och privatliv i samband med statliga ingripande åtgärder för brottsbekämpande ändamål.[8] Därför har uppsatsen valt ett annat perspektiv med hänsyn till att integritetsfrågor regelbundet studeras inom närliggande rättsområden.

1.4 Metod

För att uppnå uppsatsens syfte och besvara frågeställningen krävs en varierad metodologi som inkluderar olika tillvägagångssätt och metoder. En väsentlig del av uppsatsen använder en rättsanalytisk metod för att analysera rättsläget ur ett bredare perspektiv än att endast fastställa och redogöra för den gällande rätten. Den rättsdogmatiska metoden, som är en del av den rättsanalytiska

[8] Se exempelvis Gunnel Lindbergs verk om *Straffprocessuella tvångsmedel - när och hur får de användas?,* samt avgöranden från Europadomstolen och EU-domstolen om staters brottsbekämpande åtgärder i relation till individens rätt till integritet och privatliv.

metoden, innefattar det objektiva och renodlade konstaterandet av innebörden av den gällande rätten. Den rättsanalytiska metoden är därför bättre lämpad för uppsatsens syfte eftersom den tillåter användningen av ett bredare underlag än traditionella rättskällor. Metoden möjliggör för en mer kvalificerad analys av rättsläget i relation till värderingar och politiska intressen som påverka gällande, dåtida och framtida rättsläge.[9] I uppsatsen tillämpas metoden främst vid analysen av svensk lagstiftning om elektronisk kommunikation och straffprocessuella tvångsmedel samt de föreslagna regelverken för brottsbekämpande myndigheters tillgång till krypterad kommunikation.

En komparativ metod används i samband med redogörelsen för krypteringens historia och vid undersökningen och granskningen av framtida lagförslag som utmanar användningen av kryptering. Eftersom uppsatsens syfte inte inkluderar någon djupare jämförelse mellan det svenska rättssystemet och vare sig Storbritanniens eller EU:s regelverk eller eventuella framtida regelverk, begränsas den komparativa metoden till att utvärdera och reflektera över gemensamma rättspolitiska överväganden och deras effekter.[10]

En rättspolitisk argumentation används för att relatera juridiska argument till övergripande samhällspolitiska mål och värderingar för att stödja eller kritisera ett rättsligt ställningstagande eller frågeställning. Den rättspolitiska argumentationen är relevant för att diskutera de bredare samhällseffekterna av en viss rättsregel eller regelverk, som möjliggör för en djupare diskussion om en framtida reglering av end-to-end-kryptering. Enligt Sandgren kan en rättspolitisk argumentation syfta till att analysera en lagstiftning utifrån ett särskilt perspektiv för ett särskilt ändamål. I uppsatsen kommer särskilt perspektiv som berör samhällsmål för brottsbekämpning och effektivitet i straffprocessrätten stå i fokus för den rättspolitiska argumentationen.[11] Argumentationen används främst vid undersökningen av straffprocessrättens syften, och under analyserande avsnitt när olika perspektiv jämförs.

[9] Sandgren (2021), s. 53-55.
[10] Sandgren (2021), s. 62-63.
[11] Sandgren (2021), s. 53-55.

1.5 Material

I uppsatsen presenteras två lagförslag som utgör grundvalen för den diskussion som förs om regleringar som hindrar användningen av end-to-end-kryptering för elektronisk kommunikation. Förslagsregelverken som redogörs för är Storbritanniens Online Safety Bill och Europeiska unionens (EU) Chat Control-förordning. Det finns flera anledningar till att nämnda förslag har valts som undersökningsgrund för uppsatsen. Dels är båda regelverken mycket relevanta för debatten som pågår om balansen mellan brottsbekämpning kontra användningen av krypterad elektronisk kommunikation. Dels innehåller båda förslagen bestämmelser som förmodligen kommer att antingen införas, eller åtminstone påverka, det svenska regelverket inom en relativt snar framtid. Särskilt är Chat Control-förordningen värd att analysera, eftersom en framtida förordning kommer att behöva implementeras i svensk lagstiftning. Dessutom är både Storbritanniens och EU:s gällande regelverk om elektronisk kommunikation och möjligheten till krypterade kommunikationsmöjligheter i grunden utformade efter liknande principer, värderingar och regler som i Sverige, eftersom de ursprungligen är baserade på samma EU-rätt.

För att framställa innehållet i lagförslagen har huvudsakligen texten från de föreslagna bestämmelserna använts.[12] För att fördjupa förståelsen för regelverkens innebörd har andra källor som officiella dokument och uttalanden från Storbritanniens och EU:s formella utredningar och lagstiftningsorgan, nyhetsartiklar och debattartiklar använts. Alternativa källor har spelat en betydande roll. Dels för att ämnet är så pass nytt att officiella källor, erkänd forskning och tillförlitlig opartisk information är knapp, dels för att uppsatsens analyserande inslag kräver en bredd på debatten som förs om lagförslagens möjliga effekter. Trots att noggrannhet i källurvalet och en strävan efter neutralitet har beaktats, ska noteras att vissa kritiska källor medvetet har valts i syfte att belysa olikheter i åsikter.

[12] Notera att den version av regelverken som presenteras och diskuteras i uppsatsen utgår från den senast officiella versionen för den 1 oktober 2023.

För att undersöka och förstå innebörden av kryptering har en central del av materialet grundat sig på internationell forskning. Eftersom kryptering är en teknologi med global relevans har forskare och författare från olika geografiska områden bidragit till det övergripande kunskapsunderlaget och värdefulla insikter om krypteringens olika aspekter.

För att redogöra för det svenska regelverket för elektronisk kommunikation och användningen av hemliga tvångsmedel i brottsutredande verksamhet har lagtext, förarbeten och doktrin använts. Kompletterande material inkluderar beredande dokument, riksdagsprotokoll och andra relevanta skrivelser för att stödja förståelsen av lagstiftarens och samhällets åsikter och motiv i ämnet. För att undersöka straffprocessrättens funktion och utveckling har främst rättsvetenskaplig litteratur varit vägledande. Särskilt har modeller och teorier om straffrättsprocessen och kriminalpolitiken diskuterats utifrån rättsvetare som Henrik Tham, Dag Victor, Herbert Packer, Per Ole Träskman och Nils Jareborg.

1.6 Avgränsningar

I uppsatsen är det särskilt den allvarliga brottsligheten som hanteras av Polismyndigheten och i viss mån Säkerhetspolisen som utgör utgångspunkten för den straffprocessrätt och de tvångsmedel som utreds. I synnerhet berörs användningen av krypterade kommunikationstjänster inom den svenska nätverksbrottsligheten som ett genomgående tema. Vidare avgränsar uppsatsen sig från att beröra bevisvärde och bevisfrågor, och konstaterar endast möjligheten för myndigheter att, i sitt brottsbekämpande arbete, få tillgång till kommunikationsinnehåll.

Det ska klargöras att uppsatsen inte inkluderar en tekniskt korrekt eller utförlig beskrivning av varken end-to-end-kryptering, införandet av bakdörrar eller verkställande av övervakande teknik. Uppsatsen är inte menad att redogöra för den exakta teknologin utan nöjer sig med att beskriva fastställda begreppsinnebörder och definitioner på området.

En avgörande avgränsning är att uppsatsen inte kommer definiera eller utreda begrepp om personlig integritet eller rätten till privatliv. Det finns redan omfattande och välgrundad forskning som berör de mänskliga rättigheterna för området inom Sverige, EU och Europa. Den befintligt djupa och omfattande forskningen kring individens rätt till privatliv och integritet är tillräcklig för att stödja en generell användning av termerna.

För att klargöra ytterligare kan noteras att rätten till integritet och rätten till privatliv utgår särskilt från Regeringsformen 1974:152 (RF), där målsättningsstadgandet återfinns i 1 kap. 2 § och rättighetsstadgandet i 2 kap. 6 §. Dessutom återspeglas Europakonventionens (EKMR) gällande rätt i Sverige i enlighet med 2 kap. 19 § RF, där artikel 8 specifikt fastställer individens rätt till skydd för privat- och familjeliv, sitt hem och sin korrespondens. En motsvarande rättighet återfinns även i Europeiska unionens stadga om de grundläggande rättigheterna (EU:s rättighetsstadga), framför allt i artikel 7. För en djupare diskussion om gränsdragning och innebörd av befintliga mänskliga rättigheter som rör integritet och privatliv hänvisas till alternativ forskning. Avslutningsvis ska därför användningen av termerna om rätt till integritet och privatliv i denna uppsats tolkas från ett allmänt perspektiv, grundat på vedertaget accepterat bruk av benämningarna.

För att redogöra för den nuvarande svenska regleringen kring elektronisk kommunikation och straffprocessuella möjligheter för brottsbekämpande myndigheter att få tillgång till elektroniskt kommunicerat innehåll, koncentrerar sig utredningen främst på svenska lagar och förarbeten. För att förstå viss svensk reglering är det nödvändigt att inkludera kommentarer och hänvisningar till relevant EU-rättsligt regelverk på området. Uppsatsen avgränsar sig dock från att ge en fullständig översikt av det aktuella regelverket inom EU för elektronisk kommunikation och myndigheters befogenheter vid brottsutredningar. Beslutet grundar sig delvis på avsikten att bibehålla fokus på Sverige, men också på grund av uppsatsens begränsade omfång som omöjliggör en heltäckande diskussion om EU:s regelverk.

Med hänsyn till att det svenska regelverket som rör elektronisk kommunikation är omfattande och inkluderar regler för exempelvis datasäkerhet, datalagring och straffprocessuella tvångsmedel, måste uppsatsens undersökning avgränsas. För att hålla sig till syftet koncentrerar sig utredningen på den lagstiftning som direkt påverkar brottsutredande myndigheters möjligheter att nå tillgång till innehåll i elektronisk kommunikation. Det innebär att redogörelse för exempelvis generella datalagringsskyldigheter eller uppgiftsbehandling inte kommer att diskuteras mer än absolut nödvändigt.

I uppsatsen kommer inte tvångsmedlet genomsökning på distans, reglerat i 28 kap. 10 a § rättegångsbalken (1942:740), att behandlas. Tvångsmedlet skiljer sig från andra nämnda hemliga tvångsmedel eftersom det snarare är kopplat till reglerna om husrannsakan, där tillstånd endast kan beviljas för en specifik brottsutredning. Genomsökning på distans förutsätter också autentieringsuppgifter, såsom lösenord, för att kunna komma åt dold eller krypterad information och innebär inte samma typ av tekniska intrång som de diskuterade hemliga tvångsmedlen.

1.7 Disposition

Uppsatsens struktur omfattar sex kapitel som systematiskt besvarar huvudfrågeställningen. Det inledande kapitlet ger en bakgrund till den pågående politiska debatten om krypterade kommunikationstjänster och deras roll inom den kriminella nätverksbrottsligheten i Sverige. Det introducerar även uppsatsens syfte, frågeställning, tillämpade metoder, material och avgränsningar.

I kapitel två börjar undersökningen med en redogörelse för krypterade kommunikationstjänsters framväxt och funktion samt en historisk kontext och diskussion om end-to-end-kryptering och betydelsen för den moderna teknikberoende brottsligheten. I det tredje kapitlet diskuteras innebörden av den svenska straffprocessrättens funktion med särskilt fokus för olika teorier om rättssäkerhet och brottsbekämpning.

Det fjärde kapitlet presenterar två lagförslag som begränsar möjligheten till end-to-end-krypterad kommunikation, Storbritanniens Online Safety Bill och EU:s Chat Control-förordning. I följande kapitel fem ges en redogörelse för gällande rätt inom området för elektronisk kommunikation och lämpliga straffprocessuella tvångsmedel i Sverige som ger brottsbekämpande myndigheter tillgång till elektronisk kommunikation.

Det sjätte kapitlet utgör en avslutande analys där lagförslagen jämförs med först gällande svensk rätt och sedan med den svenska straffprocessrättens funktionskrav. En diskussion förs om svensk straffprocessrätt kan anses förenlig med en lagstiftning som begränsar användningen av end-to-end-krypterade kommunikationsmedel.

2 En bakgrund till krypterade kommunikationstjänster

2.1 Kapitelinledning

Kapitlet inleder uppsatsens undersökning och ger en översikt av kryptering i en historisk kontext och krypterade kommunikationstjänster. Vidare sker en fördjupning i end-to-end-kryptering och innebörden av att installera så kallade bakdörrar i sådana krypterade system.

Avslutningsvis följer en redogörelse för dagens teknikberoende brottslighet och dess koppling till krypterade kommunikationstjänster. Kapitlet utgör en central faktagrund för den fortsatta diskussionen om krypterad elektronisk kommunikation samt innebörden och konsekvenserna av rådande lagförslag.

2.2 Kryptering i en historisk kontext

2.2.1 Evolutionen: militärt maktspel till digitalt paradigm

Digital kryptering är en central teknologi som möjliggör för användare att säkra data under överföringar av elektronisk information. Själva krypteringen är enkelt förklarat den process som förvrider informationen på ett sätt som gör den obegriplig för en part som inte har tillgång till den krypteringsnyckel som har använts för att förvrida datan.[13] Krypteringsnyckeln kan beskrivas som ett lösenord till att komma åt och förstå den information som genom kryptering har omvandlats till ett annars oförståeligt format. Endast den som har rätt nyckel kan återställa informationen till sitt ursprungliga tillstånd. På internet är digital kryptering ett fundamentalt fenomen för att skydda informationens konfidentialitet och integritet.[14]

Traditionellt har kryptering ansetts vara en militär teknologi som politiskt ofta varit en viktig del i en nations maktspel. Intresset för en stat att utveckla sofistikerade krypteringssystem för internt och hemligt bruk har präglat

[13] Monsees (2022), s. 283-286; Singh (2000), s. 11-16.
[14] Singh (2000), s. 345-348; Kerr & Schneier (2017), s. 5-8.

krypteringsteknologins historia. Ett starkt exempel är den tyska militärens utvecklande och användande av Enigman under 1920-talet och framåt som i flera årtionden möjliggjorde den tyska militärens framfart. Utan en närmre diskussion på ämnet kan Enigman konstateras vara en central faktor i andra världskrigets framfart genom militära kommunikationsmöjligheter, och kan anses symbolisera den vitala innebörden av en stats tillgång till krypteringsverktyg.[15]

I takt med internets uppkomst och den digitala framfarten ser möjligheterna för kryptering helt annorlunda ut idag. Kryptering är inte längre förbehållet ett statligt verktyg utan är en avgörande teknologi som används för både privat och offentlig verksamhet. Teknologins utveckling möjliggör användandet av komplexa algoritmer som går långt utöver människans egen förmåga för att kryptera information.[16]

2.2.2 En inblick i ”kryptokrigen”

Som en del av vardagen är den digitala tekniken i stort fokus för debatter om övervakning, integritet, dataskydd och cybersäkerhet. Inom cyberpolitiken debatteras återkommande frågan om vem som har kontroll över den skenande avancerade krypteringen, och vem som bestämmer över åtkomsten till digitala data.[17] Termen ”Crypto wars”[18], som på svenska kan översättas till kryptokrigen, summerar den intensiva politiska debatten om kryptering och dess påverkan på regeringars förmåga att få åtkomst till digitalt krypterad information och kommunikation. Debatten, som sträcker sig över både landsgränser och politiska arenor, involverar diskussioner om balansen mellan individens rätt till privatliv och statens behov av att upprätthålla säkerhet och brottsbekämpning. Å ena sidan finns förespråkarna för stark kryptering som en grundläggande rättighet för att skydda individens privatliv och säkerhet online. Deras argument innefattar att kraftfull kryptering är avgörande för att förhindra obehörig åtkomst och övervakning av digital

[15] Monsees (2022), s. 283-284; Singh (2000), s. 133-146 och 177-181.
[16] Monsees (2022), s. 283-286.
[17] Monsees (2022), s. 283-286.
[18] Diffie & Landau (1998), s. 394.

kommunikation. Å andra sidan finns företrädare för regeringar och myndigheter som hävdar att för stark kryptering kan utgöra ett hinder för brottsbekämpning och nationell säkerhet. De fruktar att kriminella och terrorister kan utnyttja kryptering för att undvika upptäckt och förföljelse, vilket gör det svårt för myndigheter att förebygga och utreda brott.[19] Kryptokriget har manifesterat sig genom olika händelser och lagförslag som försöker reglera användningen av kryptering.

Särskilt under 1990-talet var det den amerikanska regeringen som formade reglerna för den globala krypteringspolitiken. Den starka tekniska utvecklingen i landet möjliggjorde att modern och för tiden komplicerad krypteringsteknik utvecklades i landet. Genom kontrollerad reglering kring export av den framåtgående tekniken var det USA som tidigare höll i kopplet för resterande världens tillgång till vetenskapen.[20]

En möjlighet för statligt missbruk är, och har länge varit, en stående invändning mot en statlig möjlighet att inkräkta i användningen av säkra krypteringsverktyg. Missnöjet mot en inskränkande statlig krypteringsreglering aktualiserades särskilt när den amerikanska regeringen, under 1990-talets exploderande teknologiska uppsving, ville implementera vad som kan beskrivas som ”bakdörrar” till krypteringsverktyg på marknaden. Genom att använda förinställda tillgångar till krypteringssystem önskade staten försäkra sig om att det alltid fanns en möjlighet att kringgå krypteringen för att erhålla sig tillgång till viss kommunikation.[21]

En annan metod som var aktuell för tiden var viljan att införa ett system med neutrala nyckelavlämningsmetoder, på engelska "key escrows". Termen hänvisar till processen att deponera, lagra eller överföra krypteringsnycklar till en tredje part, vanligtvis en myndighet eller en betrodd institution. Den tredje parten fungerar som en agent och lagrar krypteringsnycklarna för senare användning. Tanken var att den särskilda krypteringsnyckeln till en

[19] Diffie & Landau (1998), s. 10-14, 125-127 och 137-143; Kerr & Schneier (2017), 28-33.
[20] Monsees (2022), s. 284-286.
[21] Monsees (2022), s. 283-286; Diffie & Landau (1998), s. 51-55 och 169-171; Denning (1996), s. 89-94. Se även vidare beskrivning av bakdörrar i kapitel 2.4.

krypterad kommunikationstjänst alltid skulle lagras vid en oberoende statlig institution dit exempelvis rättsvårdande myndigheter kunde begära åtkomst om så behövdes.[22] Både användningen av bakdörrar och införandet av nyckelavlämningssystem möttes med kritik från människorättsorganisationer som hävdade att metoderna utgjorde betydande inskränkningar i den personliga integriteten och stod i strid mot demokratiska principer.[23]

2.2.3 Post-Snowden eran

Efter Edward Snowdens världsomvälvande avslöjande om hur USA:s National Security Agency (NSA) i princip hade obegränsade möjligheter att avlyssna och övervaka både amerikanska och icke-amerikanska medborgare fick debatten om integritet och övervakning en nytändning. En del av den nya samhällsdiskussionen om det övervakade samhället var nu ännu mer fokuserad på krypterade tjänster eftersom en stor mängd av den interpersonella kommunikationen numera skedde online. Vissa kallar den nya tidens diskussioner om kryptering för ”Kryptokrigen II”.[24]

Uppdagandet av den omfattande övervakningen från NSA och andra underrättelsetjänster accelererade en politisk inriktning mot en allmän tillgång till privata krypterade kommunikationsmöjligheter och ett ökat integritetstänk. Meinrath och Vitka betonar att kryptokrigen II utvecklas till en mer omfattande konflikt i dagens digitala samhälle jämfört med kryptokriget på 1990-talet. Författarna menar att balansgången mellan individens rättigheter och intressen från företag och regeringar idag konstant utmanas och skiftar beroende på händelser i omvärlden. Exempelvis resulterade den folkliga indignationen efter Snowdens avslöjande bland annat till införandet av WhatsApps assymetriska kryptering. Även EU:s ökade

[22] Denning (1996), s. 85-94; Kerr & Schneier (2017), s. 31-32.
[23] Kerr & Schneier (2017), s. 31-32; Monsees (2022), s. 283-286.
[24] Meinrath & Vitka (2014), s. 123.

ansträngningar för att stärka personlig integritet på nätet kan direkt anses utmynna i dataskyddsförordningen[25] som trädde i kraft år 2018.[26]

Situationen idag är en värld där övervakningskapaciteter alltmer är inbyggda i internetarkitekturens struktur. Meinrath & Vitka menar att medvetenheten om att allas elektroniska kommunikation och data är eller kan vara mottaglig för en omfattande övervakning pressar allt fler människor, företag och organisationer att använda ytterligare åtgärder för att säkra sin information. End-to-end-kryptering, som utvecklas vidare i nästkommande kapitel, är en stark företrädare på marknaden för det integritetssäkrande syftet. För att motverka den ökande användningen av kryptering ställs de säkerhetsinriktade åtgärderna inför en kraftfulla brottsbekämpande politik, som regelbundet strävar efter att reglera statens tillgång till krypterade kanaler. Den senaste tidens diskussioner om inbyggandet av så kallade bakdörrar i kryptografiska tjänster bygger på argument om att brottsbekämpande myndigheter behöver kunna få tillgång till elektronisk kommunikation för att säkerställa allmän säkerhet och nationell trygghet.[27] Mer om bakdörrarnas innebörd diskuteras vidare i kapitel 2.4.

2.3 Betydelsen av modern krypteringsteknik

2.3.1 Innebörden av End-to-end kryptering

End-to-end-kryptering (E2E) är en metod för digital kommunikation som garanterar att ett informationsutbyte mellan två parter förblir absolut privat. Det innebär att information från en avsändande part krypteras på ett sätt som endast kan dekrypteras av den mottagande parten. Det grundläggande syftet är att förhindra att innehållet i en interaktion mellan två individer blir känt av en annan part.[28]

[25] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG.
[26] Monsees (2022), s. 283-286; Meinrath & Vitka (2014), s. 123-127.
[27] Meinrath & Vitka (2014), s. 123-127; Ermoshina & Musiani (2019), s. 343-350; Ermoshina, Musiani & Halpin (2016), s. 244-245.
[28] Greenberg (2014); Ermoshina, Musiani & Halpin (2016), s. 244-245; Ermoshina & Musiani (2019), s 343-350; Macdonald (2022), s. 4-5.

E2E kan kort beskrivas i tre avgörande faser. Först sker kryptering vid avsändningen av data. Det innebär att information redan på den avsändande enheten krypteras genom att omvandlas till en oigenkännlig form med hjälp av en krypteringsalgoritm och en krypteringsnyckel. I den andra fasen sker en säker överföring där den krypterade informationen skickas över ett nätverk, exempelvis via internet eller ett mobilnät. Under överföringen är informationen oanvändbar för alla utom de som innehar den korrekta dekrypteringsnyckeln. När meddelandet når den mottagande enheten dekrypteras det med rätt nyckel och återgår till sitt ursprungliga, läsbara format. Således säkerställer E2E att ingen annan än avsändaren och mottagaren kan läsa, tolka eller få tillgång till informationen under överföringen. Det inkluderar alla mellanhänder, som internetleverantörer, tjänsteleverantörer, myndigheter och potentiella angripare. Eftersom ingen läsbar information är tillgänglig för utomstående parter elimineras också risken för dataläckor eller intrångsattacker.[29]

I dagens digitala landskap utgör kryptering en fundamental pelare för en säker och integritetsbevarande onlineupplevelse. Den omfattar en bred skala av digitala tjänster, från trygga banktransaktioner till säkra meddelandetjänster och har blivit en oumbärlig komponent i kommunikationsverktyg som en trygg garant för användarnas integritet och konfidentialitet. Tekniken utgör en viktig försvarsmur för att skydda säkerheten i digital kommunikation. E2E-kryptering har ett universellt tillämpningsområde som omfattar både privat, affärsmässig och statlig kommunikation. I dagens digitala era är krypteringen inte bara en teknologisk nödvändighet utan också en oumbärlig följeslagare för att säkerställa att digital interaktion präglas av säkerhet, integritet och förtroende.[30]

2.3.2 Införandet av ”bakdörrar” i krypteringssystem

Vid redogörelsen för lagförslagen om inskränkningar i E2E-kommunikationssystem i kapitel 4 står införandet av så kallade "backdoors" i fokus för diskussionen. Begreppet bakdörrar översatt till svenska, är en

[29] Se exemeplvis Kerr & Schneier (2017), s. 2-8; Nadeem (2023).
[30] Monsees (2022), s. 283-286.

metod där tjänsteleverantören omprogrammerar sina säkra krypteringssystem för att kunna komma åt en krypteringsnyckel. Det innebär att tjänsteleverantören skapar sig en möjlighet att få tillgång till ett krypterat kommunikationsutbyte som tredje part.[31] Metoden kringgår den nödvändiga auktoriseringen och använder en ingångspunkt i krypteringsmekanismen som avsiktligt införts av tjänsteleverantören för att möjliggöra åtkomst till den information som annars hade förblivit krypterad för alla parter utom avsändaren och mottagaren.

Definitionen av E2E-kryptering innebär i grunden att endast avsändaren och mottagaren har faktisk tillgång till den överförda informationen. Det betyder att E2E-krypteringen, så som den har beskrivits i det föregående kapitlet, utgör en oöverstiglig barriär för utomstående parter att avkryptera sådan informationsutväxling. I praktiken kan inte ett system definitionsmässigt beskrivas som E2E-krypterat om det har införts en bakdörr till krypteringen, eftersom det möjliggör åtkomst till kommunikationen för en tredje part.

2.4 Dagens teknikberoende brottslighet

2.4.1 Hur digitalisering har påverkat brottsutvecklingen

Under de senaste åren har teknologiska framsteg, i kombination med förändringar inom brotts- och samhällsutvecklingen, skapat en utmaning för brottsbekämpande myndigheter. Det ökade utbudet och användningen av krypterade kommunikationstjänster har resulterat i en situation där myndigheter inte kan skapa sig tillgång till sådan elektroniskt kommunicerad information. Användandet av straffprocessuella tvångsmedel är inte längre lika givande i den krypterade digitala miljön.[32]

Som kort diskuterades i uppsatsens bakgrund befinner sig den organiserade brottsligheten i Sverige i en period av betydande tillväxt, där ökat våldskapital har resulterat i allvarliga konsekvenser för samhället. I synnerhet har

[31] Kerr & Schneier (2017), s. 18-19; Ludlow (1996), s. 7; Denning (1996), s. 90-94; se också Macdonald (2022), s. 6-7.
[32] SOU 2017:89, s. 16-17.

medborgarnas säkerhet utsatts i ljuset av ett skenande antalet skjutningar och sprängningar med flera civila skador och dödsfall.[33] Brottslighetens karaktär har skiftat och pekar på de kriminella nätverkens breda kopplingar över både städer och länder som ständigt skapar svårigheter i det brottsbekämpande arbetet. Nätverksvåldet ökar i både grovhet och omfattning och sätter stor press på den svenska statens möjligheter att hantera en utmanande situation.[34] Ökningen av en teknikberoende brottslighet har väckt uppmärksamhet hos regeringen. Den digitala utvecklingen i samband med en oroande uppgång av dödligt skjutvapenvåld har motiverat flera tillsatta utredningar om utvidgade brottsutredande verktyg och åtgärder med inriktning på den digitala sfären.[35]

2.4.2 Digital kommunikation inom kriminella nätverk

Kriminella nätverk har anpassat sig till den digitala eran och utnyttjar teknologins möjligheter för samordning och kommunikation. Flera uppmärksammade nätverkshärvor belyser den centrala roll som digital kommunikation spelar i dagens kriminella verksamhet. Den teknikberoende brottsligheten ställer nya krav på att brottsbekämpande myndigheter anpassar sig för att förstå hur modern teknik används inom den organiserade kriminaliteten. Det innebär att brottsutredande myndigheter aktivt behöver söka och använda nya metoder för att förstå, utreda och kunna lagföra brottslighet i det moderna samhället.[36]

Vid flera tillfällen har tidigare krypterade kommunikationstjänster, som exempelvis Encrochat och Anom, dekrypterats och undersökts av brottsbekämpande myndigheter. Den kommunikation som tillgängliggjorts från kommunikationstjänsterna bevisar omfattningen av den kriminella verksamhet som bedrivs på plattformar som till synes använder kryptering.[37]

[33] SOU 2022:52 s. 125-130; Tham (2022), s. 27 och 30; Polisen, ”Sprängningar och skjutningar - Polisens arbete”.
[34] SOU 2017:89 s. 194-198 och 201-203.
[35] SOU 2022:52 s. 125-130; se exempelvis SOU 2012:44, SOU 2017:89 och SOU 2023:60.
[36] SOU 2022:52 s. 125-130; Prop. 2022/23:126 s 67-72; se exempelvis Hovrätten för Västra Sverige, dom 2022-04-08, mål nr B 6938–21, s. 23-30; Svea hovrätt, dom 2022-04-21, mål nr B 1462–22, s. 8-9 och 48-49.
[37] Prop. 2022/23:126 s 67-72; se exempelvis Hovrätten för Västra Sverige, dom 2022-04-08, mål nr B 6938–21, s. 23-30; Svea hovrätt, dom 2022-04-21, mål nr B 1462–22, s. 9-11.

I alla typer av verksamheter, lagliga och kriminella, finns ett behov av kommunikation kring logistik och eventuella problem mellan involverade parter. Som förväntat strävar en betydande del av den organiserade brottsligheten efter att framgångsrikt bedriva sin verksamhet utan att upptäckas av det legala samhället och statliga myndigheter. Det är därför särskilt viktigt att digital kommunikation sker med hög säkerhetsmedvetenhet, där olika krypterade kommunikationstjänster naturligtvis utgör en betydande fördel för den kriminella verksamhetens funktion.[38] Under utredningen av lagen (2020:62) om hemlig dataavläsning (HDA) gestaltades hur individer inom kriminella nätverk kommunicerar genom digitala plattformar och applikationer som möjliggör krypterade samtal istället för traditionella mobilsamtal. Det är vanligt att telefoner som beslagtas från kriminella individer är utrustade med en nivå av kryptering som är helt ny på den digitala marknaden.[39]

2.4.3 Särskilt om uppmärksammade krypteringsverktyg

Det är alltmer förekommande att internetbaserade kommunikationstjänster och onlineplattformar har förinbyggda funktioner i sina system som automatiskt krypterar informationsflöden på tjänsten. Det är idag mer regel än undantag att programvaran i kommunikationstjänsterna erbjuder en användarvänlig och lättillgänglig krypteringstjänst för privatpersonen i sin dagliga kommunikation. Kommersiella företag som Facebook, WhatsApp och Signal erbjuder en kryptering i sina telefonapplikationer som enkla och billiga alternativ för gemene man.[40] Även smarttelefoner som exempelvis Apples Iphone är till stor del krypterad och erbjuder end-to-end kryptering för sina kommunikationsmedel iMessage och FaceTime.[41] Särskilt är just Anom, Encrochat, SKY ECC, Ghost, Signal och Telegram exempel på hur krypterade kommunikationstjänster återkommande har uppmärksammats för att användas som viktiga verktyg inom organiserad brottslighet.[42]

[38] SOU 2012:44 s. 212 och 220-222; SOU 2017:89 s. 201-202; SOU 2022:52 s. 125-130.
[39] SOU 2017:89 s. 201-202.
[40] SOU 2017:89 s. 201-202; Prop. 2019/20:64 s. 56 och 66.
[41] Apple (2022).
[42] SOU 2022:52, s 140-143.

I juli 2020 sprider nyhetsmedier över hela världen hur en omfattande fransk polisinsats resulterat i ett stort antal kriminella misstänkts och anhållits i samband med att den krypterade kommunikationstjänsten Encrochat dekrypterats. Kommunikationsverktyget hade möjliggjort ett säkert och krypterat informationsutbyte som utnyttjats för brottslig verksamhet i stora delar av världen.[43] I Sverige är ett uppmärksammat exempel på effekterna av Encrochats dekryptering det omfattande åtalet mot det så kallade Vårbynätverket. Åtalet och efterföljande domar fastslog bland annat hur flera kända svenska artister bevisats inblandade i en omtalad kidnappning, som med hjälp av chatthistorik från Encrochat bidragit till en fällande dom.[44]

En annan uppmärksammad polisinsats gick under namnet Operation Trojan Shield, som i juni 2021 ledde till flertalet gripanden efter att polismyndigheter runt om i världen med framgång introducerat den fejk-krypterade kommunikationstjänsten Anom på den kriminella marknaden. Anom upprättades år 2019 av den amerikanska underrättelse- och säkerhetstjänsten FBI i syfte att få tillgång till de kriminellas kommunikationer. Intentionen var att kriminella individer skulle använda applikationen i tron om att den varit skyddad från myndigheters övervakningsmetoder. Anom marknadsfördes till kriminella organisationer som ett avancerat nytt system med enheter som påstods vara omöjliga att dekryptera av rättsväsendet. Egentligen hade tjänsten en inbyggd funktion som innebar att en hemlig kopia av varje meddelande som skickats via Anom samlades in, registrerades och arkiverades av brottsbekämpande myndigheter.[45]

Genom FBI:s samarbete med Europol omfattade operationen Trojan Shield ett samarbete mellan 16 länder där särskilt Sverige och Nederländerna spelade

[43] Se exempelvis Attunda tingsrätt, dom 2021-02-22, mål nr B 10010–20, s. 14-20; Svea hovrätt, dom 2021-05-21, mål nr B 2251-21, s. 8; Eskilstuna tingsrätt, dom 2021-02-26, mål nr B 210–21 s. 5, och Svea hovrätt, dom 2021-05-07, mål nr B 3203-21, s. 6.
[44] För avgöranden angående Vårbynätverket se Södertörns tingsrätt, deldom 2021-03-04, mål nr B 11907-20, Södertörns tingsrätt, dom 2021-07-14, mål nr B 3712-21, B 11907-20 och B 5660-21, och Svea hovrätt, dom 2022-02-18, mål nr B 9407-21 och B 3900-21. 6938–21 s. 23-24. Se också för vidare information om Vårbynätverket och Enchrochat Lodding & Örhstedt (2021).
[45] Heed & Jörnmark (2021); Göteborgs tingsrätt, dom 2021-12-17, mål B 9647–21, s. 11-13; Solna tingsrätt, dom 2022-03-16, mål nr B 10459-20, s. 42-49.

en framträdande roll. Operationen avslutades den 7 juni 2021 när den tekniska lösningen stängdes ner och Anom-enheterna inte längre kunde kommunicera via tjänsten. Svensk polis hade kontinuerligt övervakat kommunikationer mellan Anom-enheter som kunde kopplas till svenska användare.[46]

Encrochat och Anom representerar bara två av många exempel på till synes krypterade kommunikationstjänster som har utnyttjats av kriminella organisationer. Kapitlet illustrerar en oroande trend där avancerade krypterade tjänster blir alltmer integrerade i den organiserade brottsligheten.

2.4.4 Särskilt om uppdragskulturen

De brottsbekämpande myndigheternas tillgång till krypterade informationsplattformar har utöver att resulterat i operativa framgångar också bidragit till ökad förståelse för olika brottsområden och deras modus operandi. Tidigare anonyma kriminella nätverk och framstående aktörer har dessutom kunnat identifieras och kartläggas. Insikterna har ökat kunskapen om de kriminella aktörernas motiv, tillvägagångssätt och den övergripande strukturen inom den kriminella miljön.[47]

Till följd av dekrypteringssucceér av krypterade kommunikationstjänster har avslöjats att dödligt våld inom kriminella nätverk ofta iscensätts på beställning och föregås av kommunikation mellan flera inblandade aktörer. För att kort redogöra för den nätverksbaserade kriminaliteten i Sverige präglas den moderna brottsligheten av vad som kan beskrivas som en uppdrags- eller beställningskultur. Oftast tilldelas uppdraget att genomföra våldsdåd någon längre ner i gruppens hierarki som ofta är både yngre och mer våldsbenägna individer.[48] Kunskaper från granskningen av

[46] Göteborgs tingsrätt, dom 2021-12-17, mål B 9647–21, s. 13; Solna tingsrätt, dom 2022-03-16, mål nr B 10459-20, s. 42-49; se också Heed & Jörnmark (2021).
[47] SOU 2022:52, s 137-143.
[48] Se exempelvis SOU 2022:52, s 137-143; Polismyndigheten (2021), s. 17; se också om barn och unga i kriminella nätverk i Brå, Rapport 2023:13.

kommunikationschattar ger tydliga exempel på hur sådana konversationer och diskussioner om konkreta mordplaner kan gestalta sig.[49]

Tillgången till krypterade kommunikationsmöjligheter har format den organiserade brottsligheten till en anonym och utbredd verksamhet. Unga individer utsätts för nyrekrytering och manas in i miljöer med beställningar på kriminella handlingar från anonyma ledare högre upp i gänghierarkierna.[50] Ett uppmärksammat exempel är hur individen Rawa Majid, även benämnd som ”Kurdiska räven” och ansedd ledare för nätverket betecknat Foxtrot, har bedrivit sin verksamhet under senare år. Trots att den påstådda ledarfiguren inte har befunnit sig i Sverige har han instruerat till, och medverkat i, flera gängrelaterade konflikter och våldsdåd.[51] Det bevisar hur digitaliseringen, tillgången och användandet av krypterad kommunikation möjliggör en allt mer utvecklad form av nätverksrelaterad brottslighet som fysiskt separerar gängframträdande maktfigurer från brottslighetsutövande unga rekryter.[52]

2.5 Krypterad kommunikation i ett större perspektiv

Efter en längre redogörelse av den krypterade kommunikationens centrala betydelse för den moderna kriminaliteten ska poängteras att kryptering även används för andra verksamheter och syften. Det ska inte underskattas hur kryptering är en absolut nödvändig teknik för att upprätthålla ett rättssäkert och integritetsskyddande informationsutbyte inom både offentliga och privata digitala sfärer.[53]

En ytterligare aspekt som kort bör nämnas är synen på vad som utgör en kriminell handling. Vad som är eller inte är brottslig verksamhet skiljer sig mellan stater och länder. I Sverige är det exempelvis en självklarhet att

[49] SOU 2022:52, s 137-143 och 157-159; se också Hovrätten för Västra Sverige, dom 2022-04-08, mål nr B 6938–21, s. 39-40 och Svea hovrätt, dom 2022-02-18, mål nr B 9407-21 och B 3900-21. 6938–21 s. 72.
[50] Brå, Rapport 2023:13, s. 7, 19-20 och 64-71.
[51] Mosesson (2023); se exempelvis Attunda tingsrätt, dom 2023-04-05, mål nr B 5322-21 och B 5369-22.
[52] Polismyndigheten (2023), s. 3, 9-11 och 18-19; Brå, Rapport 2023:13, s. 7, 19-20 och 64-71.
[53] Se exempelvis MSB (2023); Cleris (2013).

personers sexuella läggning aldrig ska leda till kriminalisering,[54] medan det enligt Ungerns rättsordning är olagligt att sprida material som kan anses främja homosexualitet.[55] Krypterade kommunikationsmöjligheter är nödvändigt för att privatpersoner, oppositioner eller andra i sitt land utsatta grupperingar ska kunna bedriva verksamheter som vi i Sverige normalt anser vara helt legitima i demokratiska samhällen. Vid en diskussion om användandet av krypterad kommunikation i kriminella miljöer måste det därför påminnas om att definitionen och omfattningen av vad en kriminell miljö är kan skilja sig mellan samhällen, regeringar och länder.

Som avgränsningskapitlet fastställer är rätten till privatliv och personlig integritet också fundamentala ämnen för debatten om krypterad kommunikation i samhället. Det ingår dock inte i uppsatsens ramverk att vidare diskutera rättigheterna, men deras relevans för den allmänna diskussionen om kryptering ska ändå markeras.

[54] Arbetsmarknadsdepartementet (2022).
[55] Fors (2021).

3 Straffprocessrättens syfte och funktion

3.1 Kapitelinledning

Det straffrättsliga systemet kan anses ha en särpräglad ställning inom juridiken. Straffrätten utgör statens främsta maktmedel för att styra människans beteende och förmedla tillhörande straff.[56] Straffprocessrätten är den juridik som reglerar förfarandet för straffrättens genomförande. Det inkluderar regler för förundersökning, rättegångsförfarandet, beviskrav, domstolarnas befogenheter och rättigheter som tillkommer både misstänkta och åtalade.[57] Uppsatsens fokuserar på den straffprocessrättsliga juridiken där brottsbekämpande åtgärder i ofta preventiv bemärkelse står i centrum. Det är dock både relevant och nödvändigt att i viss mån diskutera ideologier och modeller som berör straffrätten, eftersom det också har påverkat utvecklingen av dagens straffprocessrätt.

Kapitlet redogör för olika synsätt, teorier och funktioner som präglar svensk straffprocessrätt. En historisk översikt av rättsområdets utveckling presenteras för att ge läsaren en grundläggande förståelse för de ideologiska grunder som format systemet. Därefter diskuteras teorier och modeller som formar straffprocessen i syfte att utforska och beskriva kännetecken för olika synsätt på straffprocessrättens krav och funktion i samhället. Genom att kontextualisera området spelar kapitlet en central roll i att analysera hur regelverk som begränsar E2E-krypterad kommunikation kan anses förenliga med den svenska straffprocessrättens grundläggande funktion.

3.2 Tidiga rättsfilosofiska teorier om rättsområdet

Under det upplysningsfilosofiskt präglade 1700-talet bidrog inflytelserika filosofer som Jeremy Bentham, Immanuel Kant och Cesare Beccaria med rättsfilosofiska teorier som ställde krav på ett formaliserat straffrättsligt system som garanterade ett rättsligt skydd för individen och allmänheten.

[56] Ulväng (2009), s 150.
[57] Ekelöf, Andersson & Bylund m.fl. (2018), s. 25-28.

Kraven på hög rättssäkerhet var utmanande för tiden där straffrätt ansågs nödvändigt för att upprätthålla ett samhälle med rättssäkerhet, men statlig inverkan som överskred den målbilden ansågs förkastlig.[58]

I 1864 års strafflag introducerades ett mer enhetligt och humant rättssystem som fokuserade likabehandling, förutsägbarhet och legalitet.[59] Johan Hagströmer, en för tiden inflytelserik och internationellt känd rättsvetare, förespråkade att det var just rättsvetenskapen som ska utforma straffrätten och leda till ändringar i kriminalpolitiken. Hagström diskuterade återkommande balansen mellan kriminalpolitiken och ändringar i straffrätten, och uttryckte bland annat hur straffrätten inte ska uppfylla sociala syften i samhället.[60]

I takt med den moderna straffrättens framfart från slutet av 1800-talet och i början på 1900-talet dominerade ett individualpreventionsperspektiv där statens främsta uppgift ansågs vara att skydda samhället från brottslingar.[61] Cesare Lombroso var en framstående förespråkare för teorier som betonade statens roll som ett verktyg för att skydda allmänheten från brottslighet.[62] Professor Johan C. W. Thyréns tankar präglade istället en utvecklingen av det svenska lagstiftningsarbetet som betonade viktigheten av den retoriska rättvisan. Thyrén menade att hur samhället uppfattar rättvisa och legitimitet i en rättsordning spelar roll för att upprätthålla förtroendet för rättssystemet. Ett rättssystem bör därför vara praktiskt och flexibelt, inte principfast.[63]

3.3 Victor om den kriminalpolitiska offensiven

I samband med brottsbalkens ikraftträdande år 1965 förstatligades den svenska polisen och höga förväntningar på effektivitet präglade organisationens utveckling.[64] Den politiska inblandningen i det straffrättsliga systemet tog en intressant vändning under 1900-talet. Fram till 1960-talet och införandet av den nya brottsbalken var politiken närmast frånvarande och

[58] Häthén (1990), s. 40-47.
[59] Svensson (2016), s. 70-73; Häthén (1990), s. 211.
[60] Svensson (2016), s. 77.
[61] Häthén (1990), s. 66-68.
[62] Häthén (1990), s. 68; Svensson (2016), s. 83.
[63] Svensson (2016), s. 85.
[64] Tham (2022), s. 43.

karaktäriserades av vetenskaplig forskning och experters utlåtanden. Beslutsfattandet och beredningen av lagstiftningen låg på en begränsad grupp juridiska ledamöter, och en allmän debatt om kriminalpolitiska frågor var generellt begränsad. Under det tidiga 1980-talet blev rättsområdet mer politiskt färgat, där särskilt straffrätten och straffprocessrätten blev utsatt för en politisering.[65] Först på 1990-talet började kriminalpolitiken formas genom partipolitiska profiler som trängde undan andra aktörer från både rampljuset och inflytandet av den vidare kriminalpolitiska utvecklingen.[66]

Dagens omtalade kriminalpolitik med en tydlig korrespondens mellan straffrätten, straffprocessrätten och partipolitiska ställningstagande var innan 1970 och 1980-talet inte alls en självklarhet. Dag Victor, juris doktor och tidigare justitieråd i Högsta domstolen, uttrycker redan 1995 hur ”situationen närmast betecknas som huggsexa”[67] vid en beskrivning av partipolitiska manifesteringar av kriminalpolitiska åtgärder.[68] Redan då var de liberala partierna framträdande i den kriminalpolitiska offensiven, något som definitivt kan anses vara förenlig med dagens partipolitiska tillstånd.[69]

Även om Victor inte uttryckligen talar om den brottsförebyggande eller brottsbekämpande verksamheten framhåller han att dess inverkan på upprätthållandet av lag och ordning är ytterst viktig. Professorn poängterar hur lag och ordning ständigt speglar samhällsdebatten om det straff- och processrättsliga systemets syfte och funktion.[70] Victor identifierar en politiserad utveckling av kriminalpolitiken under de senaste årtiondena och noterar att lagstiftningsmakten har ökat markant. Expertkommittéer har ersatts av parlamentariska grupper, och utredningsarbeten sker snabbare med ökat politiskt påtryckningsmoment. Förändringarna får direkta konsekvenser för lagstiftningen som påverkar det brottsförebyggande och

[65] Andersson & Nilsson (2017), s. 213; Tham (2022), s. 46.
[66] Victor (1995), s. 57-62.
[67] Victor (1995), s. 61.
[68] Dag Victor var även verksam vid Brottsförebyggande rådet och Justitiedepartementet, som hovrättslagman och byråchef hos Riksåklagaren, och har medverkat som sakkunnig i flera offentliga utredningar.
[69] Victor (1995), s. 61-62; se även Tham (1995), s. 85-87.
[70] Victor (1995), s. 71-72.

brottsbekämpande arbetet, särskilt för polisväsendet.[71] Victor beskriver den lagstiftande makten som en politisk verksamhet som är föremål för demokratisk kontroll. Domstolar och förvaltningsmyndigheter, inklusive brottsutredande och bekämpande myndigheter, är opolitiska men är alltjämt bundna av den politiska lagstiftningen.[72]

3.4 Träskman om brottskontroll vs brottsbekämpning

Per Ole Träskman, tidigare professor i straffrätt och författare av flera verk inom det straffrättsliga, processrättsliga och kriminalpolitiska området, diskuterar i artikeln ”Vem är kriminalpolitikens nyckelperson: brottslingen, brottsoffret eller ”jag” själv?”[73] vad kriminalpolitikens bakomliggande syfte egentligen är. Träskman utgår ifrån Inkeri Anttilas och Patrik Törnudds[74] slutsatser om att kriminalpolitiken i huvudsak har två målsättningar, att begränsa lidandet och kostnaderna för samhället som orsakas av brottsligheten och att rättvist fördela lidandet och kostnaderna mellan brottslingen, brottsoffret och samhället.[75]

Träskman påpekar att det politiska fokuset har förskjutits från tidigare tonvikt på brottskontroll till dagens inriktning mot brottsbekämpning. Nuvarande kriminalpolitik betonar sällan målet att upprätthålla en lämplig nivå av kriminalitet och balanserad brottskontroll. I stället fokuserar debatten på att bekämpa brottslighet, öka säkerheten genom repressiv kontroll och införa strängare åtgärder mot kriminella för ökad effektivitet. Träskman menar att modern kriminalpolitisk diskussion manifesterar en tydlig straffinriktad populism.[76] Uttrycket refererar till en politisk inriktning som antar en hårdare syn på brottsbekämpning för att attrahera till stöd från allmänheten, även om förespråkade åtgärder inte är de mest effektiva eller balanserade.

[71] Victor (1995), s. 71-75.
[72] Victor (1995), s. 63-64.
[73] Träskman (2008), s. 497.
[74] Inkeri Anttila var professor i straffrätt vid Helsingfors universitet och Patrik Törnudd var direktör för Kriminologiska forskningsinstitutet i Helsingfors.
[75] Anttila & Törnudd (1973).
[76] Träskman (2008), s. 498.

Träskman framhåller också att de senaste decenniernas lagreformer i Sverige ständigt fokuserar på det brottspreventiva arbetet. Det förekommer an alltmer målinriktad efterspaning av förutsedda brottslingar i samhället som kan delas upp i en kollektiv och en selektiv spaningsverksamhet. Selektiva spaningsåtgärder riktas mot målgrupper som misstänks vara involverade i specifika framtida kriminella handlingar, exempelvis individer med kopplingar till terrororganisationer. Området omfattar all lagstiftning som syftar till att identifiera och kartlägga terrororganisationer och kriminella nätverk samt deras involverade kontakter.[77]

Kollektiva spaningsåtgärder riktas mot befolkningen som helhet genom insamling och registrering av information om generella aktiviteter. Syftet är att identifiera beteendemönster som kan väcka misstankar, exempelvis särskilda flygresor och användning av elektroniska medier som telekommunikation, överföring av betalningar, sms, e-post och liknande. Ett tydligt lagstiftningsexempel är den, för tiden, kontroversiella lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (signalspaningslagen) som utgör en möjlighet till förebyggande brottsövervakning i syfte att identifiera hot mot Sveriges säkerhet.[78]

3.5 Packer om rättssäkerhet vs effektivitet

3.5.1 Utgångspunkter

Straffrättspolitiken är den del av kriminalpolitiken som avser utformningen av straff- och processrätten i relation till kraven på effektivitet, rättssäkerhet och mänskliga rättigheter. Den moderna straffrättspolitiken åsyftar att balansera den grundläggande, och grundlagsstadgade, rättssäkerheten mot ett effektivitetskrav.[79] Enligt Nils Jareborg, professor emeritius i straffrätt och inflytelserik rättsvetare, finns det i huvudsak två framträdande modeller för hur kriminalpolitiken och straffrättspolitiken drivs, den defensiva och den offensiva.[80] Båda modeller bygger på den amerikanska juristen och

[77] Träskman (2008), s. 504-505.
[78] Träskman (2008), s. 505.
[79] Jareborg (2001), s. 20; Jareborg (1995), s. 22.
[80] Jareborg (1995), s. 20-24 och 26-27; Packer (1964), s. 2-8.

kriminologen Herbert Packers kända teorier om straffprocessens två motpoler genom ”the Due Process Model” och ” the Crime Control Model”. Packer argumenterar för att de två modellerna representerar två olika synsätt på straffprocessrätten och att det finns en spänning mellan dem. Han diskuterar i sin inflytelserika artikel ”Two Models of the Criminal Process” som publicerades redan 1964 hur samhället behöver balansera mellan snabb och effektiv brottsbekämpning å ena sidan och skyddet av individuella rättigheter å andra sidan.[81]

I följande kapitel framställs de två modellerna utifrån Packers ursprungliga ideologi tillsammans med inslag av Jareborgs tillhörande teorier. Den defensiva modellen beskrivs som ”den defensiva rättssäkerhetsmodellen” och den offensiva modellen som ”den offensiva effektivitetsmodellen”.

3.5.2 Den defensiva rättsäkerhetsmodellen

Den defensiva rättssäkerhetsmodellen bygger på principen om en absolut rätt till rättssäkerhet och rättvisa som aldrig bör underordnas brottspreventiva åtgärder som kan inskränka de ovillkorliga rättigheterna. Modellen centreras kring straffprocessrättsliga principer och garantier som skyddar individens rättigheter och har som främsta syfte att förhindra statligt maktmissbruk och överdriven repression. Likvärdighet för alla individer oavsett samhällsposition bör genomsyra all straffprocessrätt och dess tillämpning. Individers lagstridiga handlingar bör behandlas på ett moraliskt acceptabelt sätt genom opartiska institutioner.[82] Jareborg drar en parallell mellan den defensiv modellen och den klassiska straffrätten[83] som politiskt har växt fram genom borgerskapets frigörelse med liberalism och demokratisering som framträdande ideologiska uppfattningar. Liberalismens övertygelse om en tydlig maktfördelning mellan statens organ för att minimera risken för maktmissbruk återspeglar sig i Packers rättssäkerhetsmodell.[84]

[81] Se Packer (1964).
[82] Jareborg (1995), s. 24, 26-27; Packer (1964), s. 6-9 och 13-19.
[83] Se vidare resonemang i Jareborg (1995), s. 23.
[84] Jareborg (1995), s. 23-24.

Brottsbekämpning anses vara nödvändig för att upprätthålla den allmänna ordningen, men det betonas att varje steg i processen måste följa rättssäkerhetsprinciper för att skydda individuella rättigheter och garantier. Den maktutövning som straffprocessrätten kan bidra till kräver ett särskilt ansvar från statsmakten för att förhindra missbruk och godtycke. En central komponent i Due Process Model är att straffprocessen måste vara föremål för kontrollmekanismer för att undvika att endast ett effektivitetsperspektiv styr lagstiftning och verkställighet. Som yttersta konsekvens menar den rättsäkerhetsfokuserade modellen att den högsta formen av effektivitet kan likställas med en form av tyranni.[85]

Den defensiva modellen utgår från en presumtion om att brottsutredande myndigheter inte har en självklar och ostridig förmåga att på ett tillfredsställande sätt utreda brott. Modellen understryker möjligheten att fel ofta uppstår, och inte sällan på grund av den mänskliga faktorn. Som tidigare poängterats är risken för maktmissbruk påtaglig, och befogenheter som tilldelas brottsutredande myndigheter inom straffprocessens ramar kan och kommer att utnyttjas på ett diskriminerande sätt. Det framhålls särskilt att marginaliserade grupper och andra utsatta samhällsklasser blir synnerligen drabbade av brottsutredande myndigheters potentiella maktmissbruk.[86]

Rättsäkerhetsmodellen framhäver starka konsekvenser mot ett brottsbekämpande system som uteslutande tar sikte på ett effektivitetsperspektiv. Modellen menar att effektivitet inte kan utgöra en godtagbar anledning till att den personliga integriteten inskränks, och det kan inte accepteras att individens frihet åsidosätts för det brottsbekämpande arbetet.[87] De processrättsliga befogenheter som brottsbekämpande myndigheter har ålagts genom kriminalpolitiska genomslag är inte överordnade rätten till privatliv.

I förhållande till straffprocessrättsliga tvångsmedel anses det vara förödande när brottsutredande myndigheter får utökade befogenheter som riskerar

[85] Packer (1968), s. 165f. Packer, (1964), s. 16.
[86] Packer (1968), s. 163 och 170.
[87] Packer (1968), s. 179.

godtyckligt bruk. Åtgärder för hemlig övervakning utgör ett betydande intrång i privatlivet, och bör endast användas vid konkret och mycket allvarlig brottslighet. För att vidta sådana ingripande åtgärder krävs betydande inflytande från en opartisk part, som en domstols godkännande, för att förhindra maktmissbruk. Rätten till privatliv anses vara en grundläggande förutsättning för att garantera individens tankefrihet, där brottsutredande arbete och befogenheter står i konflikt med den enskildes rättigheter.[88]

Avslutningsvis kännetecknas den defensiva modellen av straffprocessrättens funktion att skydda enskilda från statligt maktmissbruk. Rättssäkerhet och rättvisa får aldrig underordnas motiv för brottsbekämpning eller brottsprevention. Jareborg antyder att modellen förkastar idén om att straffprocessrätten bör lösa sociala och samhälleliga problem. Istället är dess funktion att skydda individen från överträdelser av makt från myndigheter.[89]

3.5.3 Den offensiva effektivitetsmodellen

Den offensiva modellen menar att straffprocessrättens främsta syfte är att bekämpa brott och minimera dess påverkan på samhället. En central idé är att bristande förtroende för rättssystemet kan underminera straffprocessens funktion. Kriminalpolitiken och efterföljande straffprocessrätt ska alltid sträva efter att uppnå förmågan att effektivt förebygga, upptäcka, utreda och lagföra brottsligheten. Metoder som ökar straffprocessens förmåga att uppnå det nämnda effektivitetssyftet bör prioriteras framför metoder som fokuserar på att bibehålla och skydda brottsmisstänktas, och andra medborgares, individuella rättigheter. Således är straffprocessrättens och kriminalpolitikens huvudsakliga mål är att vara effektiv och leda till önskade resultat.[90]

I kontrast till den defensiva modellen betonar det offensiva synsättet statens nödvändiga kontroll över kriminaliteten för att upprätthålla medborgarnas lydnad och individens frihet. Effektiv brottsbekämpning och en straffprocess som främjar det syftet är centralt. Modellen fokuserar på en kvantitativ

[88] Packer (1968), s. 196-197.
[89] Jareborg (1995), s. 24-25.
[90] Packer (1968), s. 158-160.

bekämpning av brott, och regelverk och befogenheter bör anpassas därefter. Modellen förespråkar ofta ett kontinuerligt utvidgande av de brottsutredande myndigheternas straffprocessuella verktyg för att maximera effektiviteten. Eftersom informationen som utredningsarbetet leder till anses vara säker och tillförlitlig finns det inget hinder mot att integritetsinskränkande åtgärder skulle kunna företas av myndigheterna. Särskilt under förundersökningsstadiet krävs tillgång till nödvändiga utredningsverktyg för att uppnå målet med effektiv brottsbekämpning. Eftersom brottsutredande myndigheter inte har några avsikter eller motiv att ingripa mot laglydiga medborgare som inte är involverade i brottslig verksamhet, finns ingen anledning att tro att deras rättigheter kommer att kränkas.[91]

Den mest framträdande kritiken metoden lyfter mot straffprocessuella regelverk är problemet med ineffektivitet. Det offensiva synsättet menar att en stat inte uppfyller sin funktion som samhällsskyddande när prevention och ett bekämpande av skadliga och brottsliga beteenden inte dominerar alla resonemang, åtgärder och beslut. Jareborg diskuterar hur individualpreventiva åtgärder inom straffrättssystemet har tappat i effektivitet och minskat förtroendet för defensiva straffrättsmetoder. Den defensiva inställningen har ersatts av en offensiv inriktning, där starka argument framhåller behovet av effektiv brottsprevention och bekämpning. Jareborg framför att den tidigare kopplingen mellan effektiv brottsbekämpning och en behandlande syn på påföljd som lösning nu har övergått till en mer allmän inriktning om preventiva åtgärder för att öka effektiviteten.[92]

Sammanfattningsvis anses alla åtgärder som faktiskt motverkar kriminalitet i samhället rättfärdigade och nödvändiga för det brottsbekämpande arbetet. Straffprocessuella tvångsmedelsåtgärder, som exempelvis hemlig avlyssning, är därför väsentliga verktyg i statens kamp mot den organiserade brottsligheten som enligt ett effektivitetsperspektiv måste kunna användas av polisen.[93]

[91] Packer (1968), s. 158, 162 och 177.
[92] Jareborg (1995), s. 27-29; Se även Tham (1995), s. 94-95.
[93] Packer (1968), s. 196; Jareborg (1995), s. 29-30.

3.6 En avslutande kommentar

Sammanfattningsvis belyser kapitlet straffprocessrättens komplexa roll och utveckling. Vad som kan anses utgöra straffprocessens funktion och syfte i samhället är inte ostridigt uppställt i något regelverk eller doktrin, och måste därför tolkas utifrån olika syften, modeller och teorier.

Från de tidiga rättsfilosofiska teorierna till dagens politiserade kriminalpolitik och modeller för straffprocessrätt, har syftet ständigt visat sig balansera kraven på effektivitet och rättssäkerhet med politisk populism. Genom Träskmans beskrivning av den politiserade kriminalpolitikens utveckling mot en effektiv brottsbekämpning konstateras att den svenska demokratin uppmuntrar en allt strängare reglering för att effektivt kämpa mot kriminaliteten. Det poängteras samtidigt hur lagstiftningsarbetet för straffprocessreglering inte längre karaktäriseras av expertkommittéer och rättsvetenskaplig forskning. Victor framhåller hur ett ökat politiskt påtryckningsmoment skyndar på utredningsarbeten som formar straffprocessrätten till gällande samhällsdebatter och åsikter.

Även om Packers modeller utvecklades på 1960-talet, kvarstår de som ett tidlöst teoretiskt ramverk som ger en fördjupad förståelse av straffprocessrättens grundläggande principer. Modellerna används som en dikotomi för att analysera sådan lagstiftning som utökar brottsbekämpande myndigheters tvångsmedelsåtgärder i Sverige. Debatten mellan defensiva och offensiva synsätt illustrerar en ständig spänning mellan att skydda individens rättigheter och att effektivt bekämpa brottslighet inom den straffprocessuella regleringen. Vidare analys om den straffprocessuella funktionen i relation till lagförslag som inskränker möjligheten till krypterade kommunikationstjänster utvecklas i analysen i kapitel 6.

4 Förslag på lagstiftning som påverkar krypterade kommunikationstjänster

4.1 Inledning och kapiteldisposition

Som diskuterats i kapitel 2 har en ökad betoning på digital säkerhet, särskilt när det gäller krypterade data, blivit en naturlig och nödvändig utveckling för vårt tekniskt avancerade samhälle. Den ökade tillgängligheten av krypterade kommunikationsmedel har dock föranlett att regeringar och brottsbekämpande myndigheter strävar efter att införa bakdörrar i krypteringssystemen med syften relaterade till nationell säkerhet och brottsbekämpning.

I kommande kapitel riktas fokus särskilt mot två framträdande och aktuella lagförslagspaket på området: Online Safety Bill i Storbritannien och Chat Control-förordningen inom EU. Initiativ som på olika men motsvarande sätt syftar till att begränsa möjligheterna till helt insynsskyddade E2E-krypterade kommunikationskanaler på sina respektive marknader. Genom att utforska bakgrunden till, och innehållet i, nämnda förslag ämnar kapitlet redogöra för bakomliggande syften, motiv, innebörd och konsekvenser av regelverken.

4.2 Storbritanniens ”Online Safety Bill”

4.2.1 Bakgrunden till förslaget

I det moderna samhället är internet en alltmer integrerad del i både den privata och offentliga sfären. I Storbritannien har det konstaterats att över 90% av medborgarna är online som en naturlig del i vardagen. Den tekniska och kulturella utvecklingen har medfört nya samhällsproblem som utmanar de regelverk som styr den digitala världen. Nya dimensioner av barns utsatthet på nätet är en av många utmaningar som tillkommit i takt med onlinesamhället tillväxt.[94] År 2020 bekräftade organisationen Internet Watch Foundation över 150 000 fall av barnpornografi på internet i Storbritannien.

[94] Woodhouse (2022) *Analysis of the Online Safety Bill*, s. 8.

Den brittiska regeringen har också noterat att samtliga fem terroristrelaterade händelser under 2017 hade centrala online-komponenter, och att över 21% av alla kvinnor i Storbritannien har utsatts för misogyniskt missbruk online.[95] Problemområdena visar på utbredda och komplexa svårigheter i dagens cybercentraliserade värld och har motiverat Storbritanniens vilja att agera.

År 2020 presenterade den brittiska regeringen Online Harms White Paper[96] med målet att skapa en säkrare internetmiljö och återställa förtroendet för digitala plattformar. White Paper utvecklades senare till Online Safety Bill[97], en lagstiftning som konkretiserar de ambitioner som formulerats i det ursprungliga dokumentet. Motivet är att utveckla ett regelverk som ska kunna anpassa sig till den snabba teknologiska utvecklingen i samhället. [98]

Lagförslaget adresserar den ökande förekomsten av skadliga beteenden online och den höga graden av anonymitet och sekretess som digitala plattformar erbjuder för kriminaliteten i samhället. Det brittiska parlamentet anser att brottsligheten utnyttjar den omfattande tillgången till anonyma kommunikationsmöjligheter utan risk för påföljder. Med tanke på att användningen av onlinetjänster betraktas som en oumbärlig del av modern tillvaro strävar Storbritanniens regering nu efter att implementera den nya regleringsramen för att hantera problemet med olagligt och skadligt innehåll på internet.[99]

4.2.2 Regelverkets innehåll

Online Safety Bill är namnet på den nya uppsättningen lagar som i Storbritannien ska skydda barn och vuxna på nätet. Den 19 september 2023 meddelade den brittiska regeringen att lagförslaget har passerat en sista debatt och omröstning i parlamentet, och erhöll senare kungligt godkännande av

[95] Trengove m.fl. (2022), s. 1-4; Internet Watch Foundation (2022); Woodhouse (2022) *Analysis of the Online Safety Bill*, s. 8.
[96] DCMS (2022) *Online Harms White Paper*.
[97] Online Safety Act 2023.
[98] Trengove m.fl. (2022), s. 1-2; Woodhouse (2022) *Analysis of the Online Safety Bill*, s. 8-13.
[99] Trengove m.fl. (2022), s. 1-2; Woodhouse (2022) *Analysis of the Online Safety Bill*, s. 8-13.

kung Charles den 26 oktober. Lagförslaget har flera politiska målsättningar som bland annat syftar till att öka användares säkerhet online, förbättra rättsväsendets förmåga att bekämpa olagligt innehåll samt öka användarnas möjlighet att själva hålla sig säkra online.[100]

Lagförslagets grundidé är att göra tjänsteleverantörerna för digitala kommunikationstjänster ökat ansvariga för användarsäkerheten på deras plattformar. Leverantörerna får genom lagförslaget något som kan liknas en omsorgsplikt, en ”duty of care”, för den information som sprids via kommunikationstjänsten.[101] Förslaget antar en ansvarsmodell där omsorgsplikten gäller för internetleverantörer av både användar-till-användartjänster och söktjänster. Användar-till-användartjänster är tjänster där användare interagerar med varandra online, vilket är det normala interaktionsättet på plattformar som exempelvis Facebook och X, tidigare Twitter. Söktjänster är digitala verktyg för att indexerar information och låter användare navigera på internet, som exempelvis Google och Bing.[102]

Omsorgsplikten är definierad i breda termer i lagen och kan beskrivas genom tre distinkta skyldigheter; att skydda användare från olagligt innehåll, att vidta särskilda skyddsåtgärder för barns säkerhet, och att vidta åtgärder för att främja transparens, ansvarsskyldighet och yttrandefrihet för att ge användaren kontroll över innehållet som visas på plattformen.[103] Trots att produktion och spridning av brottsligt innehåll, som exempelvis barnpornografi och terroristpropaganda, redan är olagliga syftar lagförslaget till att ålägga tjänsteleverantörer skyldigheten att kontrollera och begränsa den potentiella spridningen av sådant material.[104] Tjänsteleverantörernas reglerade åtaganden om öppenhet, ansvarsskyldighet och yttrandefrihet infördes som svar på kritik mot ett tidigare utkast av lagförslaget. Tidigare föreslogs en

[100] Online Safety Act 2023, särskilt klausul 1; Woodhouse m.fl. (2023) *Research Briefing.*
[101] Trengove m.fl. (2022), s. 1-4; Woodhouse (2022) *Analysis of the Online Safety Bill*, s. 5-6 och 12; Woodhouse m.fl. (2023) *Research Briefing.*
[102] Online Safety Act 2023, särskilt clause 3-8; Woodhouse (2022) *Analysis of the Online Safety Bill*, s. 5 och 21-24; Trengove m.fl. (2022), s. 3.
[103] Woodhouse (2022) *Analysis of the Online Safety Bill*, s, 27-29; DCMS (2023) *Overview of expected impact of changes to the Online Safety Bill.*
[104] Trengove m.fl. (2022), s. 3; se särskilt klausul 12 i Online Safety Act 2023; Woodhouse m.fl. (2023) *Research Briefing.*

ytterligare skyldighet för tjänsteleverantörerna att skydda användarna från innehåll som ansågs skadligt, även om det inte var olagligt. Det riktades kritik mot att staten hade befogenhet att klassificera lagligt innehåll som skadligt vilket skapade oro för inskränkningar av yttrandefriheten i Storbritannien.[105]

Nuvarande lagförslag innebär att tjänsterna måste erbjuda verktyg för att användarna ska kunna kontrollera vilket innehåll som visas på plattformen. Företag måste tillhandahålla inställningar enligt en lista över innehållskategorier som kan anses särskilt skadliga för användaren. Det inkluderar innehåll som exempelvis uppmuntrar till självmord, självskada, ätstörningar eller är kränkande för bland annat religion, kön eller sexuell läggning, och som en användare ska kunna filtrera bort.[106] Det innebär att leverantörerna måste kunna upptäcka och kategorisera innehåll på tjänsten.

Lagförslagets införande av skyldigheter för onlinetjänsternas leverantörer är nytänkande för det rättsliga området. Den ansvarsbörda som läggs på leverantörerna avviker från den ordning som tidigare har gällt för Storbritannien genom EU:s e-handelsdirektiv[107]. Enligt e-handelsdirektivet är huvudregeln att leverantörer av onlineplattformar inte anses vara ansvariga för skadligt eller olagligt material på sina plattformar, förutsatt att de inte har kännedom om innehållet eller tillräcklig information för att bli medvetna om dess existens. Online Safety Bill utvidgar avsevärt regelverket genom att införa en rättslig kontroll över spridning av innehåll på onlineplattformar där ansvaret läggs över på tjänsteleverantören. [108]

4.2.3 Innebörden för krypterade kommunikationstjänster

Syftet med det diskuterade lagförslaget är att införa en lagstadgad omsorgsplikt för vissa tjänsteleverantörer. Det innebär bland annat en

[105] Trengove m.fl. (2022), s. 1-5; DCMS (2023) *Overview of expected impact of changes to the Online Safety Bill, s.* 15-21.
[106] DCMS (2023) *Overview of expected impact of changes to the Online Safety Bill,* s. 15-21. Se särskilt klausul 14, 15 och16 i Online Safety Act 2023.
[107] Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden ("Direktiv om elektronisk handel"). Se vidare i kapitel 5.3.
[108] Se exempelvis art. 12,13, 14 och 15 I e-handelsdirektivet; Trengove m.fl. (2022), s. 4-9.

skyldighet att moderera innehållet som sprids för att skydda användare mot olaglig och skadlig information. Nedan följer en beskrivning av hur den föreslagna lagen påverkar tjänsteleverantörernas möjlighet att erbjuda och använda end-to-end-kryptering för sina kommunikationstjänster.

Enligt regelverket ska den brittiska myndigheten Office of Communications (Ofcom)[109] tilldelas befogenhet att övervaka och genomdriva lagen.[110] I rollen kommer Ofcom att utarbeta praxis för genomförandet av omsorgsplikten, och fastställa vilka tjänsteleverantörer som omfattas av bestämmelsernas skyldigheter. Den föreslagna lagen föreslår dessutom att statssekreteraren för avdelningen för digitalisering, kultur, media och sport (DCMS) tilldelas befogenheten att justera undantag och fastställa trösklar för att kategorisera tjänsteleverantörer inom eller utanför omsorgspliktens omfattning.[111]

För att uppfylla sina skyldigheter i enlighet med lagförslaget måste tjänsteleverantörerna använda ackrediterad teknik för att identifiera, kategorisera och eventuellt ta bort skadligt innehåll. Omsorgsplikten indikerar att tjänsteleverantörerna behöver övervaka eller åtminstone ha åtkomst till användarnas kommunikationer för att uppfylla sina åtaganden. För tjänsteleverantörer som tillhandahåller E2E-kryptering innebär detta att de endast kan efterleva omsorgsplikten genom att antingen ta bort eller försvaga den kryptering de erbjuder. Även om lagen inte explicit förbjuder E2E-kryptering tvingas tjänsteleverantörerna att kompromissa med tjänsternas integritet för att undgå sanktioner om kraven inte upprätthålls.[112]

För att ytterligare diskutera E2E-krypteringens framtid enligt regelverket är det relevant att notera hur Ofcom får befogenheten att kräva att tjänsteleverantörer ger övervakningsmyndigheten tillgång till visst krypterat innehåll under särskilda omständigheter, och under hot om grova böter.

[109] Myndighetens uppgift är att bevaka allmänhetens och konsumenternas intressen och tillgång till tele-, datakommunikations-, radio- och tv-företag i Storbritannien.
[110] Woodhouse (2022) *Analysis of the Online Safety Bill*, s. 5-6; Online Safety Act 2023, se exempelvis klausul 41-54.
[111] Online Safety Act 2023, se exempelvis klausul 44; Voge & Wilton (2022), s. 9-10. Se också DCMS (2022) *Online Harms White Paper*.
[112] Voge & Wilton (2022), s. 9-11; Macdonald (2022), s. 1, 6-7; Online Safety Act 2023, se exempelvis chapter 5 och klausul 231.

Lagförslaget ger ministern en omfattande diskretionär befogenhet att bestämma vilka leverantörer och tjänster som omfattas av bestämmelsen, och därmed måste inskränka sina krypterade system.[113]

Klausul 121 i lagförslaget ger Ofcom möjligheten att reglera och övervaka innehåll relaterat till terrorism och sexuella utnyttjanden av barn online. Det kräver att leverantörer använder ackrediterad teknik för att identifiera och ta bort terrorismrelaterat och barnexploaterande innehåll. Det gäller oavsett om kommunikationen av sådant material sker i ett offentligt digitalt rum eller i en privat chatt. Om tjänsteleverantören inte har tillgång till sådan teknik måste leverantören göra sitt bästa för att utveckla eller skaffa en sådan teknik som uppfyller vissa standarder som DCMS har fastställt.[114] Så sent som den 27 oktober 2023 framhöll Andy Yen, en etablerad förespråkare för internetsäkerhet och personlig integritet, att det för närvarande inte finns någon ackrediterad teknik som samtidigt upprätthåller en nivå av integritetsskydd för kryptering.[115]

Vidare befäster klausul 100 Ofcoms auktoritet att kräva information från tjänsteleverantörerna för att kunna fullgöra sina funktioner enligt regelverket. Information som krävs kan exempelvis vara olika rapporter eller statistik över vilket innehåll som sprids på den aktuella tjänsten. Det fastslås också i klausul 102 och 109 att det utgör ett brott mot regelverket om tjänsteleverantören inte lämnar över begärd information till Ofcom i ett format som Ofcom kan förstå. Det betyder att om den information som ska överlämnas är krypterad, eller på annat sätt oläslig för Ofcom, utgör det ett lagbrott som kan leda till betydande böter. Enligt Schedule 13 framgår att bristande efterlevnad av reglerna om informationsdelning till Ofcom kan resultera i böter på upp till 18 miljoner pund eller 10% av den globala årsomsättningen, beroende på vilket belopp som är högre.[116]

[113] Voge & Wilton (2022), s. 9-11; Macdonald (2022), s. 1 och 6-7; Online Safety Act 2023, se exempelvis chapter 5 och klausul 231.
[114] Online Safety Act 2023, klausul 121.
[115] Yen (2023).
[116] Online Safety Act 2023, klausul 102, 109, 100, 111, 113 och schedule 13; Woodhouse (2022) *Analysis of the Online Safety Bill*, s. 54-57.

Enkelt uttryckt innebär informationssystematiken mellan leverantörerna och Ofcom, i samband med det höga sanktionssystemet, att leverantörerna åläggs att antingen försvaga krypteringen på sina plattformar, eller på annat sätt tillhandahålla särskilda möjligheter att skapa sig tillgång till privata kommunikationer. Lagstiftaren hävdar att regelverket inte eliminerar möjligheten till E2E-krypterade kommunikationer på den brittiska marknaden eftersom företagen har möjlighet att installera bakdörrar i sina krypterade system för att kunna uppfylla sina skyldigheter.[117] Det uppstår därmed en definitionsfråga huruvida en sådan krypteringsbakdörr kan anses förekomma vid E2E-krypterade former.[118]

I sammanhanget har det framhållits att begreppet krypteringsbakdörr utgör en oxymoron, eftersom kryptering, särskilt i formen av end-to-end, per definition inte kan möjliggöra för en tredje part att få åtkomst till informationsutbytet. Att införa en möjlighet för en utomstående aktör att skaffa sig tillgång till en krypteringsnyckel innebär i praktiken att E2E-kryptering inte kan upprätthållas.[119] Det går därför inte att hävda att E2E-kryptering kommer att kunna erbjudas av tjänsteleverantörer som omfattas av den specifika regleringen enligt lagförslaget. Vidare bör det betonas att Ofcoms omfattande befogenheter att självständigt formulera och omformulera ramarna för regelverket skapar en dynamisk marknad där relationerna och skyldigheterna för kommunikationstjänster enligt Online Safety Bill kan förändras. Det adderar en ytterligare dimension av osäkerhet för tjänster med E2E-kryptering i Storbritannien.

4.2.4 Kort om aktuell kritik

I ljuset av konstaterandet att E2E-kryptering till stor del påverkas av Online Safety Bill har flera framstående tjänsteleverantörer, företag och organisationer framfört stark kritik mot det nya regelverket. I februari 2023 meddelade Meredith Whittaker, ordförande för Signal Foundation som är

[117] Se resonemang i Woodhouse (2022) *Analysis of the Online Safety Bill*, s. 116-119.
[118] Voge & Wilton (2022), s. 12.
[119] Macdonald (2022), s. 1 och 6-7; Voge & Wilton (2022), s. 12. Se även kapitel 2.2.2 och 2.2.3 om end-to-end kryptering och införande att bakdörrar.

leverantör till den E2E-krypterade chattjänsten Signal, att leverantören kommer att lämna den brittiska marknaden om Online Safety Bill antas. Whittaker framhåller att kraven i lagförslaget innebär att tjänster som är E2E-krypterade mellan kommunicerande parter inte längre tillåts, och konstaterar att Signal inte kommer kompromissa med sin integritetsförsäkrande krypteringsteknik.[120] Signal har sedan sitt grundande år 2014 betraktas som ett godkänt krypterat kommunikationsverktyg inom USA:s senat, för tjänstemän inom både FN och Europeiska kommissionen, samt har hyllats av den tidigare NSA-anställde Edward Snowden.[121]

Apple och WhatsApp är två andra marknadsledande företag som erbjuder E2E-krypterade kommunikationsmöjligheter som hårt kritiserat lagförslagets skyldigheter för tjänsteleverantörer. I en intervju med BBC har Apple uttryckt att regelverket bör modifieras för att skydda E2E-kryptering i linje med rätten till personlig integritet. Båda tjänsteleverantörerna har meddelat att de inte avser att kompromissa med sin E2E-kryptering, oavsett argument från den brittiska regeringen. De kräver att lagförslaget revideras för att säkra rätten till krypterade kommunikationskanaler.[122] Någon sådan ändring är dock inte i sikte.

4.3 Europeiska unionens Chat Control-förordning

4.3.1 EU:s arbete mot sexuella övergrepp mot barn på nätet

I juli 2020 presenterade Europeiska kommissionen en strategi för att bekämpa sexuella övergrepp mot barn inom EU. Som en inledande åtgärd introducerades ett lagförslag som tillät leverantörer av elektroniska kommunikationstjänster att frivilligt använda tekniska åtgärder för att upptäcka sexuella övergrepp mot barn på sina plattformar. I augusti 2021 trädde den tillfälliga förordningen (EU) 2021/1232[123] (förordningen om

[120] Vallace (2023a); Wright (2023); Tucker (2023).
[121] Le-Khac & Raymond Choo (2022), s. 28.
[122] Vallace (2023b).
[123] Europaparlamentets och rådets förordning (EU) 2021/1232 av den 14 juli 2021 om ett tillfälligt undantag från vissa bestämmelser i direktiv 2002/58/EG vad gäller användning av teknik hos tillhandahållare av nummeroberoende interpersonella kommunikationstjänster för

tillfälligt undantag) i kraft. Förordningen möjliggör för nummeroberoende interpersonella kommunikationstjänster[124] att behandla vissa uppgifter om elektronisk kommunikation för att bekämpa sexuella övergrepp mot barn online. Regleringen skapar ett temporärt undantag från vissa bestämmelser om konfidentialitet i det övergripande direktivet om elektronisk kommunikation inom EU 2002/58/EG[125] (e-dataskyddsdirektivet).[126] Detaljer om hur det tillfälliga regelverket påverkar den svenska lagstiftningen beskrivs vidare i kapitel 5.3.

Den tillfälliga undantagsförordningen gäller till och med den 3 augusti 2024. Som nästa steg i EU:s strategiska arbete mot sexuella övergrepp mot barn planeras att presentera ett mer permanent regelsystem som på lång sikt ska kräva att leverantörer av onlinetjänster upptäcker och rapporterar material med sexuella övergrepp mot barn till myndigheterna.[127] Det aktuella lagförslaget för permanent inkorporering presenteras i nedanstående kapitel.

4.3.2 Bakgrunden till förslaget

Chat Control-förordningen, eller i folkmun kallat Chat Control 2.0, är det lagförslag från EU-kommissionen om fastställande av regler för att förebygga och bekämpa sexuella övergrepp mot barn[128]. Den 11 maj 2022 presenterade EU-kommissionen ett förslag till en EU-förordning som ska underlätta i bekämpningen av sexualbrott mot barn på nätet som sker över olika digitala mötesplatser. En stark initiativdrivande faktor till den skarpa åtstramningen gällande övervakning av digital kommunikation motiveras är de nästan 30 miljoner fall av sexuella övergrepp mot barn som rapporterades i Europa

behandling av personuppgifter och andra uppgifter i syfte att bekämpa sexuella övergrepp mot barn på nätet.

[124] En nummeroberoende interpersonell kommunikationstjänst definieras exempelvis i Lag (2022:482) om elektronisk kommunikation i 1 kap. 7 §, som en kommunikationstjänst som inte är beroende av traditionella telefonnummer eller nationella nummerplaner. Begreppet omfattar alla typer av internetberoende kommunikationsverktyg som exempelvis tjänster som Whatsapp, Facebook, iMessage och Signal.

[125] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation).

[126] Se exempelvis Prop. 2021/22:136 s. 106 och 322.

[127] Regeringskansliet Faktapromemoria 2020/21:FPM6, s 1-2.

[128] Se även IT-ord.idg.se.

under år 2021. Den skrämmande verkligheten har förvärrats av den ökade digitaliseringen och användningen av sociala medier och chattjänster.[129]

Förslaget grundar sig på bland annat på bestämmelser i Europeiska unionens stadga om de grundläggande rättigheterna (EU-stadgan) och Förenta nationernas konvention om barnets rättigheter (barnkonventionen), som tydligt fastställer att skydd och välfärd för barn utgör mänskliga rättigheter. EU-kommissionen understryker nödvändigheten av att skydda barns rättigheter även inom den digitala sfären, vilket motiverar en ny reglering. Förslaget vill harmonisera lagstiftningen på EU-området för spårning och analys av elektronisk kommunikation. EU-kommissionen argumenterar för att det nuvarande fragmenterade regelverket inom det expansivt växande teknikområdet riskerar att inte upprätthålla ett tillräckligt skydd för mänskliga fri- och rättigheter.[130] Kritiken och diskussionerna som presenteras vidare i kommande kapitel, menar att införandet av Chat Control skapar ett samhälle av massövervakning där all kommunikation inom EU automatiskt kommer att skannas i syfte att lokalisera bland annat barnpornografiskt material.[131]

4.3.3 Regelverkets innehåll

Chat Control-förordning är ett omfattande regelverk som innefattar flera områden med skyldigheter och åtaganden för olika tjänsteleverantörer på marknaden.[132] Särskilt relevant för uppsatsens syfte är lagförslagets introducerarande av en övergripande skyldighet för alla tjänsteleverantörer att spåra, blockera, avlägsna och rapportera material som involverar sexuella övergrepp mot barn (förkortat som CSAM, som står för *child sexual abuse material*)[133]. I följande avsnitt beskrivs närmre den reglering av tjänsteleverantörers och företags ansvar att skanna och övervaka innehållet på sina plattformar genom användningen av särskild teknik.

[129] Chat Control-förordningen, s. 1-3.
[130] Chat Control-förordningen, s. 1-3.
[131] Se exempelvis Skriftlig fråga 2022/23:526 av Niels Paarup-Petersen (C); IMY (2023); se också Chat Control-förordningen, artikel 1.
[132] Se ”leverantörer av värdtjänster eller interpersonella kommunikationstjänster” i Chat Control-förordningen, s. 2-3 samt artikel 1(2) och artikel 2.
[133] För begreppsdefinition se exempelvis Chat Control-förordningen (engelsk version), s. 10.

En central aspekt av förslaget är införandet av så kallad spårningsteknik. Det innebär att leverantörer förväntas använda en godkänd teknologi för automatisk skanning, kategorisering och genomsökning av material på sina plattformar som är baserat på fördefinierade indikatorer för CSAM.[134] Arbetsgången för regelverkets verkställande inleds genom att en behörig myndighet utfärdar en spårningsorder för en viss tjänsteleverantör. En spårningsorder innebär att leverantören måste vidta särskilda tekniska åtgärder för att kunna skanna plattformens innehåll efter särskilt eftersökt material.[135] Leverantören åläggs i samband med spårningsordern en informationsskyldighet att på ett tydligt och begripligt sätt meddela användarna vars kommunikationer är utsatta för spårning att deras konfidentialitet i tjänsten påverkas. Det är dock avgörande att informationsskyldigheten inte står i strid med effektiviteten för att verkställa spårningsordern. Vad det exakt innebär framgår inte av förordningen.[136]

I artikel 10 specificeras särskilt den teknik som tjänsteleverantörerna förväntas använda. Där fastställs att när en tjänsteleverantör mottagit en spårningsorder verkställs den genom installerandet och användandet av teknik som ska spåra spridningen av CSAM.[137] En nyckelkomponent för genomförandet av lagförslaget är tillgången till den avgörande spårningstekniken, som enligt artikel 10(2) ska tillhandahållas kostnadsfritt av det nyinrättade EU-centrumet. EU-centrumet, som föreslås av EU-kommissionen som ett opartiskt organ, förväntas spela en central roll i förordningens implementering och genomförande, och tilldelas omfattande befogenheter. Enligt exempelvis artikel 43(2) och artikel 51 klargörs att EU-centrumet bland annat ska ansvara för tillhandahållandet, granskningen och utvecklingen av den effektiva och centrala spårningstekniken som berörda tjänsteleverantörer inom EU-området tvingas implementera i sin erbjudna tjänst. [138] Det ska dock konstateras att en tjänsteleverantör inte nödvändigtvis

[134] Chat Control-förordningen, s. 19-28; se också exempelvis artikel 1, 7 och 10.
[135] Se särskilt Chat Control-förordningen, artikel 7.1.
[136] Chat Control-förordningen, artikel 10.5.
[137] Chat Control-förordningen, artikel 10.1.
[138] Chat Control-förordningen, artikel 40-43 och 51 samt s. 7.

måste använda just den teknik som EU-centrumet erbjuder, så länge den egna tekniken uppnår organets riktlinjer för vad tekniken ska åstadkomma.[139]

Utöver teknikansvaret är en fundamental roll för EU-centrumet att driva en indikatordatabas för att möjliggöra effektiv och tillförlitlig sökning efter CSAM. Indikatorerna fungerar som kännetecken för relevant olaglig kommunikation, exempelvis försök till kontakt med barn i sexuella syften, som genom spårningstekniken ska kunna identifiera och kategorisera spridningen av sådant material på plattformen. Intentionen med det nya EU-organet är att etablera ett starkt samarbete med både Europol nationella brottsbekämpande myndigheter.[140]

Sammanfattningsvis innebär regelverket att tjänsteleverantörer på EU:s marknad blir helt underställda EU-centrumets behörighet att begära rapporter och information från leverantörerna om sina användare och sitt innehåll. Därutöver tvingas alla leverantörer att använda sådan teknik som EU-centrumet anser tillförlitlig på området, som enligt av EU-centrumets fastställda indikatorer kan spåra relevant olaglig kommunikation och CSAM.

4.3.4 Innebörden för krypterade kommunikationstjänster

För att direkt adressera regelverkets innebörd för E2E-krypteringen utgör Chat Control-förordningen ett direkt hinder för användningen av sådan säker kryptering för kommunikationstjänster inom EU.[141] Tjänsteleverantörer som exempelvis Facebook, Instagram, Snapchat, Signal och WhatsApp som erbjuder kommunikationsplattformar måste införa en möjlighet att kunna övervaka och skanna allt informationsutbyte för CSAM.

Europeiska dataskydsstyrelsen (EDPB) och Europeiska datatillsynsmannen (EDPS) inkom med ett yttrande angående förordningen i juli 2022 där det konstateras att förordningen omöjliggör en effektiv kryptering.[142] Yttrandet fastställer att kravet på tjänsteleverantörerna att vidta tekniska åtgärder för att

[139] Chat Control-förordningen, s. 29-30.
[140] Chat Control-förordningen, s. 4, 12 och 36-37, samt artikel 2 och 44-46.
[141] EDPB-EDPS, Joint opinion 04/2022.
[142] EDPB-EDPS, Joint opinion 04/2022.

säkra konfidentialiteten för användarna, i samband med plikten att effektivt möjliggöra spårning av CSAM, sätter leverantörerna i en tekniskt omöjlig situation. Vidare diskuteras hur det för närvarande inte finns någon teknologisk lösning som kan upptäcka CSAM i en E2E-krypterad miljö. De europeiska dataskyddsmyndigheterna hävdar att införandet av verktyg för interception och analys av kommunikation fastställer en systematisk skyldighet för leverantörerna att tekniskt kunna genomföra en sådan handling.[143] För att företagen ska kunna upprätthålla sin skyldighet krävs det därför att systemet som används för tjänsten tillåter åtkomst till innehållet, och därmed måste företagen på marknaden vara redo att införa en bakdörr till sina E2E-krypterade system.

I den kompletterande konsekvensbedömningen från Europaparlamentet framhålls det även där hur E2E-kryptering omintetgörs av förordningen. Särskilt betonas hur kravet på specifika modereringsteknologier enligt förslaget direkt och grundläggande motsätter sig definitionen av E2E-krypterad kommunikation.[144] Särskilt är det reglerna i artikel 10 som debatteras i frågan om funktionen av kryptering i ljuset av Chat Control. Det går inte att tolka förordningen på annat sätt än att artikeln, för effektivt verkställande, kräver av leverantörerna att använda en spårningssökande godkänd teknik som effektivt kan genomsöka och flagga allt relevant innehåll med CSAM. Som upprepande konstaterats är det med dagens teknik definitionsenligt inte möjligt att genomföra en sådan genomsökning och samtidigt upprätthålla en helt E2E-krypterad kommunikationsform.

4.3.5 Kort om aktuell kritik

Förslaget har mött hård kritik från särskilt människorättsorganisationer, journalister och tjänsteleverantörer. Länder som Nederländerna, Tyskland, Österrike och Irland har tydligt motsatt sig förslaget med argumentet att det begränsar medborgarnas möjligheter att utöva grundläggande rättigheter. Europaparlamentets forskningsgrupp (EPRS), EDPB och EDPS förespråkar att tjänsteleverantörers skyldigheter att skanna innehållet i kommunikation

[143] EDPB-EDPS, Joint opinion 04/2022, s. 6, 17 och 27.
[144] EPRS, Complementary impact assessment 04/2023, s 83.

hotar rätten till integritet.[145] Journalister och nyhetsrapportörer påpekar att lagstiftningen utmanar det traditionellt okontroversiella källskyddet när kommunikation utan yttre insyn inte längre är garanterad.[146] Justitieminister Gunnar Strömmer uttryckte tidigt sitt och regeringens stöd för förslaget men har nyligen intagit en mer avvaktande hållning.[147]

En betydande kritik berör den ökade arbetsbelastningen för tjänsteleverantörerna för att upprätthålla alla förpliktelser om att skanna, rapportera och ta bort innehåll. Europaparlamentets kompletterande konsekvensanalys av lagförslaget understryker att informationssamhället och utvecklingen av säker datahantering riskerar att stagnera när företag och utvecklare i stället måste fokusera på att utveckla och underhålla teknologier för informationsskanning. Situation har väckt en oro inför framtiden eftersom det kan ha en negativ inverkan på den tekniska utvecklingen inom EU, när mindre tid och resurser ägnas åt utvecklingen av säker datahantering.[148]

Jan Karlung, VD för internetleverantören Bahnof, har uttryckt att ”Chat Control är en demokratisk katastrof”[149]. Han påpekar att den bakdörr som EU-kommissionens förslag förutsätter för skanning av all kommunikation i praktiken möjliggör att all kommunikation kan blir utsatt för övervakning av myndigheter. Jan Karlung menar därför att förordningsförslaget kommer göra EU till ”en av historiens största övervakningsapparater”[150].

[145] Cantwell (2023); EPRS, Complementary impact assessment 04/2023, s. 85.
[146] Hyllert & Wiman Snäll (2023).
[147] Cantwell (2023); Svar på skriftlig fråga JU202 3/00879, 2022/23:526; Melchior (2023).
[148] EPRS, Complementary impact assessment 04/2023, s. V.
[149] Karlung (2023).
[150] Karlung (2023).

5 Det svenska regelverket för tillgång till elektronisk kommunikation

5.1 Introduktion och kapiteldisposition

I följande kapitel redogörs för den svenska lagstiftning som reglerar brottsbekämpande myndigheters tillgång till individers elektroniska kommunikation. Syftet är att undersöka vilka aktuella möjligheter som brottsbekämpande myndigheter har för att avlyssna och övervaka innehållet i elektronisk kommunikation. Särskilt fokuseras på tjänster och leverantörer som erbjuder krypterade kommunikationskanaler. Observera att det för uppsatsens syfte endast är relevant att djupare diskutera regelverk som berör tillgång till innehållet i elektroniska kommunikationer.

Inledningsvis presenteras några grundläggande utgångspunkter för de brottsutredande myndigheternas uppdrag. Därefter ges en översikt över aktuella regelverk och utredningar som reglerar användningen av elektronisk kommunikation och tjänsteleverantörers skyldigheter i Sverige. Avslutningsvis redogörs för relevant straffprocessuell tvångsmedelslagstiftning och utredningar om framtida möjliga förändringar på området. Syftet med kapitlet är att ge läsaren förståelse för hur Sveriges straffprocessuella regelverk hanterar och resonerar kring krypterad elektronisk kommunikation inom ramen för det brottsbekämpande arbetet.

5.2 Några grundläggande utgångspunkter

5.2.1 Kort om brottsbekämpande myndigheters uppdrag

Sveriges polismyndigheter, bestående av Polismyndigheten och Säkerhetspolisen, har ett stående uppdrag att förebygga, förhindra och utreda brott. Ledningen av kvalificerade brottsutredningar samt beslut i åtalsfrågor hanteras av åklagare vid Åklagarmyndigheten eller Ekobrottsmyndigheten som även för det allmännas talan vid en kommande brottmålsprocess. Vissa andra myndigheter som Försvarsmakten, Tullverket och Skatteverket har också ett visst brottsbekämpande uppdrag, men generellt är det

Polismyndigheten som ska utreda och beivra brott under allmänt åtal i Sverige. Särskilda brottsformer som exempelvis terrorbrott eller brott mot rikets säkerhet omfattas av Säkerhetspolisens uppdrag.[151]

Säkerhetspolisens verksamhet bygger på en utbredd underrättelseverksamhet, vilket innebär att förebygga, förhindra och upptäcka den brottsliga verksamheten. En skillnad mot den ordinära[152] verksamheten inom Polismyndigheten är att Säkerhetspolisen inte kan bedriva en effektiv verksamhet endast utifrån anmälningar om brott, utan kräver en förmåga att identifiera händelser som kan utmynna i brottslighet. Sådan typ av underrättelseverksamhet bedrivs ofta i ett skede där det inte föreligger tillräckliga bevisa för att inleda en förundersökning.[153]

5.2.2 Allmänt om elektronisk kommunikation och uppgifter

Elektronisk kommunikation innebär att överföra informationssignaler i en elektronisk form. Kommunikationsformen inkluderar flertalet olika medier som exempelvis radio, tv, data eller telefoni. En elektronisk kommunikationsform är en central och växande del i vardagen för många, både i professionella och privata sammanhang. Användningen av e-post, samtal, chattfunktioner och ständig anslutning till internet via applikationer och plattformar har blivit normen för den svenska gemene mannen.[154]

Tjänsteleverantörer i detta sammanhang är, som diskuterats i tidigare kapitel, de företag som tillhandahåller någon typ av digital kommunikationsmöjlighet till användarna på marknaden. För att signalerna som framför kommunikationen på deras plattformar ska kunna navigera sig korrekt mellan användarna genereras viss information om varje sådant utbyte. Informationen om ett meddelande eller ett samtal kallas för metadata. Metadata innehåller ingen information om vad som står skrivet i meddelandet eller vad som har sagts under samtalet, utan omfattar information som bland annat telefon- eller

[151] SOU 2022:19 s. 69.
[152] Observera att även Polismyndigheten bedriver sådan verksamhet i särskilda fall.
[153] SOU 2022:19 s. 69-70.
[154] SOU 2022:19 s. 70; SOU 2017:75 s. 77.

abonemangsnummer, IP-adresser, användarnamn, tidpunkter för samtal eller vilka mobilmaster som ett meddelande skickats igenom.[155]

Metadata för varje enskilt meddelande genererar endast data som rör det specifika meddelandet. Vid tillgång till flera meddelanden och kommunikationsutbyten kan en sammanställd metadata konstruera ett nätverk av information som kan vara relevant. Det kan bli möjligt att dra slutsatser om vilka användare eller personer en individ har kommunicerat med, var en person har befunnit sig under kommunikationen och när den har ägt rum. Sådan information kan vara värdefull för brottsbekämpningen.[156]

För att brottsbekämpande myndigheter ska kunna ta del av uppgifter om elektronisk kommunikation och metadata måste informationen uppfattas i realtid, eller genom datalagring. Informationen kan tas del av i realtid om det exempelvis finns ett beslut om ett relevant hemligt tvångsmedel.[157] Om informationen inte uppfattas direkt krävs det att informationen lagras, vanligtvis hos tjänsteleverantören. Vissa trafikuppgifter måste lagras hos tjänsteleverantören av tekniska eller administrativa skäl.[158] Utöver det förekommer särskilda lagstadgade lagringstvång för vissa tjänsteleverantörer som gäller för viss typ av information under angivna tidsperioder. Detta kallas för datalagring, och syftet är att brottsbekämpande myndigheter ska kunna få tillgång till den typen av information i efterhand.[159]

5.2.3 Kort om regelverket inom EU

Inom ramen för elektronisk kommunikation finns det ett flertal relevanta EU-rättsakter som påverkar det svenska regelverket. I följande kapitel 5.3 - 5.6 kommer relevanta direktiv och förordningar kortfattat diskuteras i samband med relationen till nämnda svenska bestämmelser. Inledningsvis ska kort redogöras för utgångspunkterna i EU-rätten för elektronisk kommunikation.

[155] SOU 2022:19 s. 70-71; Pomerantz (2015), s. 20-22.
[156] SOU 2022:19 s. 70-71.
[157] Se vidare i kapitel 5.5.
[158] Se om trafikuppgifter i 1 kap. 7 § LEK.
[159] SOU 2022:19 s. 71.

Ett av de grundläggande direktiven är e-dataskyddsdirektivet som föreskriver ett krav för medlemsstater att säkerställa att konfidentialiteten upprätthålls för elektronisk kommunikation och tillhörande behandling av uppgifter.[160] E-dataskyddsdirektivet och den tillfälliga förordningen om undantag från konfidentialitet i brottsbekämpande syften[161], benämns vidare i relationen till LEK i kapitel 5.5.

Kortfattat kan också nämnas det gällande direktivet om elektronisk handel (e-handelsdirektivet)[162] där en särskild ansvarsregim för digitala mellanhandstjänster stadgas. E-handelsdirektivet skapar undantag från nationella regler som lägger ansvar på värdar för kommunikationsplattformar, under särskilda omständigheter. Exempelvis är gällande huvudregel att en leverantör av vissa onlinetjänster kan undkomma ansvar för olagligt material som sprids på plattformen, om det kan visas att leverantören inte har faktisk kännedom om den olagliga informationen eller verksamheten som bedrivs genom tjänsten.[163] Direktivet har kortfattat nämnts i relation till Online Safety Bill i kapitel 4.2.2.

5.3 Lagen om elektronisk kommunikation

5.3.1 Bakgrund och syfte

Den 3 juni 2022 trädde den nya lagen (2022:482) om elektronisk kommunikation (LEK) i kraft och ersatte den tidigare lagen med samma namn.[164] Det nya regelverket genomfördes för att implementera Europaparlamentets och Rådets direktiv (2018/1972) av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (kodexdirektivet) i svensk rätt. Lagen, och direktivet, syftar huvudsakligen till att skydda tillgången till säkra och effektiva elektroniska kommunikationsmedel för både myndigheter och privatpersoner. I LEK:s

[160] SOU 2022:19 s. 72.
[161] Se kapitel 4.3.1.
[162] Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (”Direktiv om elektronisk handel”).
[163] Se exempelvis artikel 12, 14 och 15 i e-handelsdirektivet.
[164] Se SFS 2003:389.

första paragraf framgår även att ”Sveriges säkerhet liksom elektroniska kommunikationers betydelse för yttrandefrihet och informationsfrihet”[165] särskilt ska beaktas.[166]

Det nya kodexdirektivet grundar sig i utvecklingen av det moderna samhället där sektorn för elektronisk kommunikation är en grundläggande förutsättning för den digitala ekonomin. En framstående förändring är att konsumenter och företag förlitar sig överhängande på tjänster för data- och internettillgång framför traditionella telefonitjänster. Den digitala omställningen kräver att branschen för tjänsteleverantörer kan tillgodose den ökade efterfrågan och samhälleliga behoven. Målet med regelverket att främja en heltäckande och obegränsad internettillgång på den inre marknaden genom ett harmoniserande och konkurrensfrämjande regelsystem. Kodexdirektivet strävar också efter att vara anpassat till den snabbt föränderliga digitala marknaden och utvecklingen i ett dynamiskt elektroniskt kommunicerande samhälle.[167]

5.3.2 Regler om säkerhet för uppgifter & innehåll

5.3.2.1 Utgångspunkter för säkerhet och skydd av uppgifter

Enligt 8 kap. 1 § LEK har tillhandahållaren av en allmän elektronisk kommunikationstjänst en generell skyldighet att vidta ändamålsenliga åtgärder för att kunna hantera och motverka risker som hotar säkerheten i tjänsten. Åtgärderna ska både vara tekniska och organisatoriska, och förebygga säkerhetsincidenter mot användare och andra tjänster.[168] En allmänt tillgänglig elektronisk kommunikationstjänst innebär enligt definitionsparagrafen i 1 kap. 7 § att både nummerbaserade och nummeroberoende tjänster omfattas av bestämmelsen.[169] Den typ av säkerhet som ska upprätthållas definieras också i 1 kap. 7 § och inbegriper en skyldighet att motverka säkerhetsincidenter som hotar konfidentialiteten i kommunikationen. Tjänsteleverantörer ska genomföra tillräckliga åtgärder

[165] 1 kap. 1 § LEK.
[166] 1 kap. 1 § LEK; Prop. 2021/22:136 s. 1, 103 och 109.
[167] Prop. 2021/22:136 s. 104.
[168] 8 kap. 1 § LEK; Prop. 2021/22:136 s. 311-314.
[169] Prop. 2021/22:136 s. 122-124.

för att skydda all information som lagras, överförs eller bearbetas genom den elektroniska tjänsten från obehörig åtkomst.[170] I 8 kap. 4 § LEK fastställs även en skyldighet för tjänsteleverantörer att informera användare om möjliga säkerhetshot på tjänsten.

Vidare föreligger en allmän skyldighet för tillhandahållarna av elektroniska kommunikationstjänster i 8 kap. 6 § LEK att tekniska och organisatoriska åtgärder ska vidtas för att skydda uppgifter som behandlas för tjänstens funktion.[171] Likt rekvisit i 1 § samma kapitel tas det hänsyn till både tillgänglig teknik och kostnader för att fastställa vad sådana lämpliga tekniska åtgärder innebär. I 9 kap 1 § LEK regleras vidare huvudregeln för behandling av trafikuppgifter för elektroniska kommunikationstjänster. Utgångspunkten är att sådana uppgifter ska utplånas eller avidentifieras när de inte behövs för den fortsatta elektroniska kommunikationen. Relevanta undantag för uppsatsens syfte stadgas i paragrafens andra stycke och hänvisar till 9 kap. 19 och 21 §§, samt till förordningen om tillfälligt undantag 2021/1232[172]. Nämnda undantag diskuteras vidare i nedan kapitel 5.3.2.2 om utlämning av uppgifter för brottsbekämpande ändamål.

Enligt 9 kap. 27 § LEK stadgas därutöver ett allmänt förbud mot att någon annan än berörda användare får ta del av, eller behandla, information eller uppgifter i ett elektroniskt överförbart meddelande om det inte föreligger samtycke från användaren. Undantag stadgas, som diskuteras i följande kapitel, i 9 kap. 1-3 §§ samt 31 § LEK. I stycke två stipuleras även där ett undantag för nummeroberoende interpersonella kommunikationstjänster enligt förordningen om tillfälligt undantag.[173]

5.3.2.2 Utlämning av uppgifter för brottsbekämpande ändamål

I 9 kap. 19 § LEK fastställs den grundläggande regleringen för ”Lagring och annan behandling av trafikuppgifter m.m. för brottsbekämpande ändamål”.

[170] 1 kap. 7 § och 8 kap. § 1 LEK; Prop. 2021/22:136 s. 311-316 och 318-321; se även 8 kap. 5 § LEK om skyddsåtgärder vid lagring av uppgifter för brottsbekämpande ändamål.
[171] Se också Prop. 2021/22:136 s. 122-124.
[172] Se kapitel 4.3.1.
[173] Se vidare i kapitel 4.3.1.

Där föreskrivs skyldigheter för tjänsteleverantörer av elektroniska kommunikationsnät eller kommunikationstjänster att lagra vissa uppgifter i brottsbekämpande ändamål. Datauppgifterna som omfattas är de som är:

> nödvändiga för att spåra och identifiera kommunikationskällan, slutmålet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typ av kommunikation, kommunikationsutrustning samt lokalisering av mobil kommunikationsutrustning vid kommunikationens början och slut.[174]

Som redogjorts för i kapitel 5.2.2 om metadata och datalagring är ovan beskrivning i 9 kap. 19 § LEK definitionsmässigt vad som kan beskrivas som metadata. Bestämmelsen kan därför inte användas för att få tillgång till något innehåll i en elektronisk kommunikation.

I 9 kap. 31 och 32 §§ stadgas en särskild tystnadsplikt för nummerberoende kommunikationstjänster. I 31 § första stycket andra punkten inkluderar plikten information om innehållet i ett elektroniskt meddelande.[175] Huvudregeln är att nummerberoende kommunikationstjänster inte får sprida eller dela med sig av innehållet i en kommunikation som på något sätt har uppfattats av tjänsteleverantören. Undantag stadgas i 9 kap. 33 § som identifierar vilka myndigheter som har rätt att begära ut vissa uppgifter som omfattas av tystnadsplikten från en tjänsteleverantör. I första stycket fastställs att paragrafen inte heller är tillämplig på nummeroberoende kommunikationstjänster. Undantaget stipulerar också en skyldighet för nummerberoende kommunikationstjänsters leverantörer att på begäran lämna ut särskild information. Observera dock att innehållet i ett elektroniskt meddelande inte omfattas av rätten att begära ut uppgifter i 33 §.

Genom 9 kap. 19 § om datalagring, 31 § om tystnadsplikten och 33 § om utlämningen av uppgifter i LEK kan det fastställas att information om innehåll i elektroniska meddelanden inte får begäras ut enligt någon författningsparagraf i LEK. Sammanfattningsvis konstateras att information som berör fakta om kommunikationen kan bli utsatt för begäran om

[174] 9 kap. 19 § LEK.
[175] Se 9 kap. 31 § p. 2 LEK.

utlämning och datalagring enligt LEK, men inte innehållet i det elektroniska meddelandet.[176]

5.3.2.3 Särskilt om nummeroberoende kommunikationstjänster

Som fastställts i kapitlet ovan omfattas inte nummeroberoende kommunikationstjänster som Signal, WhatsApp eller iMessage av bestämmelserna om varken datalagring i 9 kap. 19 §, tystnadsplikten i 9 kap. 31 §, eller utlämningsskyldigheten i 9 kap. 33 § i LEK.[177] I propositionen till LEK betonas behovet av en framtida moderniserad lagstiftningen för att hålla jämna steg med teknologiska förändringar och nya kommunikationsvanorna i samhället, särskilt vad gäller nummeroberoende kommunikationstjänster. Vidare konstateras att traditionella straffprocessuella tvångsmedel som övervaknings- och avlyssningsmetoder blir mindre effektiva när användningen av nummeroberoende kommunikationstjänster ökar eftersom dessa tjänster för närvarande inte omfattas av, exempelvis, datalagringskrav.[178]

Flera undantagsbestämmelser i LEK hänvisar till EU-förordningen om tillfälligt undantag 2021/1232. Som kortfattat presenterades i kapitel 4.3.1 etablerar förordningen temporära bestämmelser som möjliggör för nummeroberoende kommunikationstjänster att avvika från kraven om konfidentialitet för vissa uppgifter. I LEK fastställs därmed undantag för nummeroberoende kommunikationstjänster gällande skyldigheten att avidentifiera vissa lagrade uppgifter enligt 9 kap. 1 § i syfte att bekämpa sexuella övergrepp mot barn på nätet enligt förordningen.[179] Samma undantag gäller exempelvis även förbudet mot avlyssning enligt 9 kap. 27 § LEK. Den tillfälliga EU-förordningen möjliggör därför för nummeroberoende kommunikationstjänster på den svenska marknaden att, genom nödvändig och proportionell användning av viss godkänd teknik, behandla och lagra uppgifter för identifiering och rapportering av sexuella övergrepp mot barn

[176] Se också SOU 2022:19 s. 74-76.
[177] Se också Prop. 2021/22:136 s. 326-329.
[178] Se vidare diskussion och redogörelse i kapitel 5.4, 5 och 6 samt i Prop. 2021/22:136 s, 326-327.
[179] Se 9 kap. 1 § stycke två LEK.

på plattformen. Tekniken måste utöver att vara proportionell och nödvändig även vara välkänd och den minst integritetskränkande enligt de senaste branschstandarderna.[180] Förordningen är dock en möjlighetsskapande och inte ett skyldighetsskapande regelverk. Det innebär att tjänsteleverantörer får vidta sådana åtgärder, men inte måste.

5.3.3 En avslutande kommentar

Regelverket för elektronisk kommunikation är både tekniskt och lagstiftningsmässigt svårövergripligt och komplicerat. Lagrådet yttrar i sitt remissvar på utredningen av den nya LEK att:

> Ett ytterligare påpekande som Lagrådet vill göra är att den föreslagna lagstiftningen rör ett tekniskt komplicerat område. Detta betyder att det i vissa delar har varit svårt för Lagrådet att överblicka de mera praktiska konsekvenserna av i remissen valda lagtekniska lösningar.[181]

Vidare uttrycker Lagrådet, med hänvisning till remissvaret som lämnats även för den tidigare LEK:s utredning år 2002 att:

> Lagrådsgranskningen har således inriktats på att, med utgångspunkt i en delvis översiktlig bedömning av hur anpassningen av svensk rätt genomförs enligt lagförslaget, bidra med vissa synpunkter på förslagets utformning. [182]

Analysen kommer vidare diskutera problematiken med det tekniskt komplicerade området och diskutera den oroväckande situationen när, bland annat, remissinstanser och andra parter inte har förmågan att på ett betryggande vis förstå och kunna utreda tillhörande regelverk.[183]

[180] Se förordningen om tillfälligt undantag 2021/1232, artikel 3.
[181] Prop. 2021/22:136 s. 951-952.
[182] Se Prop. 2002/03:110 s. 588.
[183] Se vidare i kapitel 6.

5.4 Straffprocessuella hemliga tvångsmedel

5.4.1 Övergripande om straffprocessuella tvångsmedel

Straffprocessuella tvångsmedel kan beskrivas som särskilda åtgärder inom ramen för myndighetsutövning som utgör ingrepp i en individs personliga integritet utan dennes samtycke.[184] En straffprocessuell åtgärd innefattar vanligtvis inslag av tvång mot antingen person eller egendom. Det saknas dock en lagstadgad definition av vad som faktiskt är ett straffprocessuellt tvångsmedel, och en komponent av tvång är inte en nödvändig del.[185] Straffprocessuella tvångsmedel är en viktig del i det brottsutredande arbetet och används ofta under förundersökningar. Det finns även utrymme för att använda vissa tvångsmedel i preventiva syften, ett område som kraftigt utvidgas igenom lagändringar den 1 oktober 2023.[186]

Huvudsakligen regleras användandet av straffprocessuella tvångsmedel i 24-28 kap. rättegångsbalken som kompletteras av andra författningar innehållandes specialregler för särskilda typer av tvångsmedel. Två exempel på sådan speciallagstiftning som är relevant för uppsatsen är lagen (2020:62) om hemlig dataavläsning (HDA) och lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen). Det grundläggande syftet för att använda straffprocessuella tvångsmedel är för att säkerställa att brottsbekämpande myndigheter har rätt verktyg för att genomföra brottsutredningar och lagföra kriminaliteten i samhället. I rättegångsbalken beskrivs inte tvångsmedel som ett ändamål till att förebygga brott utan det berörs främst i preventivlagen.[187]

5.4.2 Övergripande om hemliga tvångsmedel

Hemliga tvångsmedel är den kategori av straffprocessuella tvångsmedel som per definition innebär att den utsatte individen inte har delgetts någon information om att åtgärden företas. Det får därför antas att ett hemligt

[184] Prop. 2013/14:237 s. 43; SOU 2018:61 s. 41.
[185] Se exempelvis Prop. 2013/14:237 s. 43 och SOU 2022:19 s. 76-77.
[186] Se exempelvis Prop. 2022/23:126 s. 1 och 62-86.
[187] Lindberg (2022a), s. 6-8.

tvångsmedel genomförs utan den berörde individens medvetande eller samtycke.[188] Regelverket för hemliga tvångsmedel har under senare tid varit utsatt för förändring. Dels på grund av en modernisering av samhället som kräver ett tekniskt modernt lagverk, dels på grund av den ökade kriminaliteten i Sverige som påskyndar ständiga politiska debatter om brottsutredande myndigheters ökade behov av verktyg i sitt arbete.[189] Idag är de hemliga tvångsmedlen i svensk rätt:

- hemlig övervakning av elektronisk kommunikation,
- hemlig avlyssning av elektronisk kommunikation,
- hemlig kameraövervakning,
- hemlig rumsavlyssning,
- hemlig dataavläsning,
- kvarhållande av försändelse (postkontroll), och
- inhämtning av uppgifter om elektronisk kommunikation.[190]

Huvudregeln för användandet av hemliga tvångsmedel är att det ska föreligga en misstanke om brott och att åtgärderna ska företas inom ramen för en förundersökning. Under särskilda förutsättningar har brottsbekämpande myndigheter en möjlighet att använda ett sådant hemligt tvångsmedel redan innan en förundersökning. Regelverket för att företa preventiva tvångsmedelsåtgärder uppdaterades senast den 1 oktober i år, 2023, och utvidgade möjligheterna för brottsbekämpande myndigheter att använda hemliga tvångsmedel i underrättelseverksamhet.[191] Det svenska systemet för tvångsmedel ställer höga krav på den myndighet och de individer som tillämpar lagstiftningen. Det är i första hand åklagarens uppgift att besluta om förekomsten av ett hemligt tvångsmedel i en specifik situation, och har därför

[188] Prop. 2013/14:237 s. 43; Lindberg (2022a), s. 6-8; SOU 2022:19 s. 76-77.
[189] Se exempelvis Prop. 2021/22:136 s. 104 och SOU 2017:89 s. 16-17 och 194-203.
[190] SOU 2022:19 s. 78.
[191] SOU 2022:19 s. 77; Prop. 2022/23:126 s 66-86; se också 1-1a §§ preventivlagen.

ansvar för att balansen mellan effektivitet i brottsbekämpandet och den personlige integriteten upprätthålls i varje enskilt fall.[192]

Nedan följer en kort redogörelse för preventivlagen och de två hemliga tvångsmedel som möjliggör för brottsbekämpande myndigheter att ta del av innehåll i elektroniska kommunikationer, hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning. Syftet är att skapa en förståelse för regelverket som styr brottsutredande myndigheters möjligheter att komma åt innehåll i krypterade elektroniska kommunikationer.

5.4.3 Övergripande om preventivlagen

Under särskilt det senaste året har flera lagändringar utvidgat tillämpningsområdet för preventivlagens bestämmelser.[193] I syfte att bekämpa allvarlig brottslighet, särskilt inom kriminella nätverk, har preventivlagen utökat möjligheterna för brottsutredande myndigheter att beviljas tillstånd för hemliga tvångsmedel. Särskilt har möjligheterna för Polismyndigheten utvidgats i syfte att bekämpa brott som skjutningar, sprängningar och narkotikahandel. Tidigare var preventivlagen främst tillämplig på Säkerhetspolisens område för specifikt allvarliga brott som exempelvis spionerи och terrorism.[194]

I propositionen till lagen argumenterar regeringen för att det finns ett påtagligt behov av att utvidga användningen av preventiva tvångsmedel för att säkerställa att brottsbekämpande myndigheter har de verktyg de behöver för att möta kraven på att effektivt förebygga och bekämpa den allvarliga brottsligheten.[195] Vidare diskuteras även behovet av att balansera kravet på effektiv underrättelseverksamhet med skyddet för medborgarnas grundläggande rättigheter och integritet. Det betonas att en rättssäkerhetsgaranti måste säkerställas genom att myndigheters underrättelseverksamhet inte riktar in sig på specifika brott eller misstänkta

[192] Ekelöf, Andersson & Bylund m.fl. (2018), s. 102; se exempelvis 27 kap. 16a och 23a §§ rättegångsbalken och 12 § preventivlagen.
[193] Se SFS 2022:1521, SFS 2023:229, SFS 2023:260 och SFS 2023:537.
[194] Prop. 2022/23:126 s. 67-70.
[195] Prop. 2022/23:126 s. 67-70.

personer. Istället bör den kännetecknas av att vara kunskaps- och underrättelsesökande. Det fastställs som avgörande att beviljandet av tillstånd för hemliga tvångsmedel i preventivt syfte är rättssäkert och att eventuella intrång i den personliga integriteten hålls på en nivå som överensstämmer med rättsliga normer.[196] Nedan presenteras relevanta bestämmelser i preventivlagen i samband med redogörelsen för respektive tvångsmedel.

5.4.4 Hemlig avlyssning av elektronisk kommunikation

I 27 kap. 18 § rättegångsbalken får meddelanden som överförs eller har överförts i ett elektroniskt kommunikationsnät i hemlighet avlyssnas eller upptas genom tekniska hjälpmedel. Tvångsmedel är tillämpligt på olika former av kommunikation som inkluderar muntlig, skriftlig och datakommunikation, och ger brottsbekämpande myndigheter möjlighet att i hemlighet övervaka eller ta del av innehållet i elektroniska meddelanden.[197]

Hemlig avlyssning får avse ett specifikt telefonnummer eller annan adress som ägs eller tidigare har ägts av den misstänkte, eller som det finns synnerlig anledning att tro har använts eller kommer att användas av denne. Samma rekvisit gäller för personer där det finns betydande anledning att anta att personen har kontaktat eller kommer att kontaktas av den misstänkte.[198] Kraven som uppställs i 27 kap. 18 a § rättegångsbalken fastställer att det för tillstånd krävs att någon är skäligen misstänkt för ett brott som ställs upp i brottskatalogen i andra stycket, och att åtgärden är av synnerlig vikt för utredningen.[199] I 18 b § framkommer också att tillstånd får beviljas för att utreda vem som skäligen kan misstänkas för ett brott som stadgas i stycke två.

Enligt första och andra paragrafen preventivlagen kan tvångsmedlet även användas utanför en förundersökning enligt särskilt uppställda rekvisit. I 1 § stadgas att ett sådant tillstånd i preventivt syfte får beviljas om det enligt omständigheterna finns en påtaglig risk[200] för att en person kommer utöva en

[196] Prop. 2022/23:126 s. 80.
[197] SOU 2022:19 s. 78.
[198] Se 27 kap. 18 a § tredje stycket.
[199] SOU 2022:19 s. 78-79.
[200] För redogörelse av rekvisitets innebörd hänvisas till Prop. 2013/14:237 s. 105-106.

sådan kriminell handling som stadgas i brottskatalogen i andra stycket. I tredje stycket samt i 1 a § stadgas också särskilda möjligheter för preventiv elektronisk avlyssning när det gäller brottslighet inom en kriminell organisation. Även i preventivlagen stadgas i 5 § ett krav på en proportionalitetsbedömning för att motivera ett preventivt tillstånd till en tvångsmedelsåtgärd. Åtgärden ska också anses vara av synnerlig vikt för att förhindra brottsligheten för att kunna rättfärdigas.

För att verkställa en hemlig avlyssning inhämtas informationen från en tjänsteleverantör för ett elektroniskt nät eller tjänst.[201] En problematik som uppmärksammats är det allt mer utbredda användandet av kryptering används för kommunikationstjänster, vilket utmanar möjligheten att genom avlyssning få ta del av begriplig information.[202] Svårigheten utgör en betydande anledning till införandet av HDA som diskuteras i nästkommande kapitel. Sammanfattningsvis kan konstateras att det hemliga tvångsmedlet för hemlig avlyssning inte ger någon praktisk möjlighet för brottsutredande myndigheter att få insyn i krypterad kommunikation.

5.4.5 Hemlig dataavläsning

5.4.5.1 Bakgrund och motiveringar

Den 1 april 2020 trädde lagen om hemlig dataavläsning i kraft. I förordet till propositionen till lagen framhölls särskilt de tekniska utmaningarna för de brottsbekämpande myndigheterna att effektivt använda befintliga hemliga tvångsmedel för att få tillgång till elektronisk kommunikation. Den relevanta informationen som myndigheterna behövde komma åt genom elektronisk avlyssning eller andra tvångsmedel blev i praktiken nästintill otillgänglig på grund av den stora mängd krypteringsmetoder som allt oftare används. Det konstaterades att myndigheterna inte hade tillräckliga verktyg för att hantera den samhälleliga tekniska utvecklingen i sitt brottsbekämpande arbete.[203]

[201] SOU 2022:19 s. 82-85; SOU 2023:78 s. 13-14 och 61-66.
[202] SOU 2017:89 s. 605; Prop. 2019/20:64 s. 70; Prop. 2011/12:55 s. 178-181.
[203] Prop. 2019/20:64 s. 1 och 70; SOU 2017:89 s. 605.

Tidigare regering ansåg det nödvändigt att introducera ett nytt hemligt tvångsmedel för att förbättra möjligheterna att komma åt krypterad information. Enligt lagstiftaren var syftet med HDA att återställa de brottsbekämpande myndigheternas kapacitet att förebygga, förhindra och utreda brottslig verksamhet i Sverige, och fungera som ett effektivt verktyg mot den grova organiserade brottsligheten.[204]

HDA kan i stort sett jämföras med tvångsmedlet för hemlig avlyssning, där den väsentliga skillnaden är var informationen inhämtas. Avlyssning av elektronisk kommunikation gäller för meddelanden som överförs i ett kommunikationsnät. Dataavläsning riktar sig mot ett specifikt informationssystem, som exempelvis en telefon eller dator, och har därför helt andra möjligheter att uppfatta och avläsa krypterade kommunikationer.[205] HDA är tidsbestämd med en gräns på 5 år och gäller fram till mars 2025. I november publicerades SOU 2023:78 med syftet att utvärdera gällande lag och tvångsmedel och föreslå permanent lagstiftning på området.[206]

5.4.5.2 Innebörden av hemlig dataavläsning

Hemlig dataavläsning ger brottsbekämpande myndigheter möjlighet att få åtkomst till elektronisk information som annars är svåråtkomlig, exempelvis på grund av kryptering. Verktyget används i huvudsak när andra tvångsmedel inte utgör praktiska alternativ. I praktiken innebär hemlig dataavläsning att myndigheterna, med hjälp av tekniska hjälpmedel i hemlighet kan inhämta uppgifter från avläsningsbara informationssystem[207] som exempelvis datorer, mobiltelefoner, internetanvändarkonton på kommunikations- eller lagringstjänster. För andra traditionella tvångsmedel krävs informationen istället från en tjänsteleverantör för ett elektroniskt nät eller tjänst.[208]

Innehållet som får avläsas enligt HDA definieras i 1 och 2 §§ och innefattar:

[204] Prop. 2019/20:64 s. 99 och 125-127.
[205] SOU 2022:19 s. 82-83 och s. 106; Prop. 2019/20:64 s. 66.
[206] SOU 2023:78 s. 13.
[207] Se vidare beskrivning i Prop. 2019/20:64 s. 102-105.
[208] SOU 2022:19 s. 82-85; SOU 2023:78 s. 13-14 och 61-66.

1. kommunikationsavlyssningsuppgifter,
2. kommunikationsövervakningsuppgifter,
3. platsuppgifter,
4. kameraövervakningsuppgifter,
5. rumsavlyssningsuppgifter,
6. uppgifter som finns lagrade i ett avläsningsbart informationssystem men som inte avses i 1–5, eller
7. uppgifter som visar hur ett avläsningsbart informationssystem används men som inte avses i 1–6[209]

Punkt ett till fem är uppgiftstyper som har sina motsvarigheter i andra permanenta hemliga tvångsmedel, som exempelvis hemlig avlyssning. Den första punkten, kommunikationsavlyssningsuppgifter definieras i 1 § HDA som innehållet i ett elektroniskt meddelande, som exempelvis texten i ett SMS eller substansen i ett telefonsamtal. Punkt sex innefattar annan information utöver vad som framkommer i punkt ett till fem som är sparad eller lagrad i ett system. Det kan exempelvis vara filer, bilder eller dokument på en mobiltelefon. Punkt sju utvidgar omfattningen av regelverket ytterligare och involverar information om hur användare interagerar med ett system i realtid, exempelvis öppnande av applikationer, tangenttryckningar eller musrörelser.[210] Innehållet i punkt sju är ämnad att tolkas oerhört brett.[211]

I praktiken innebär HDA i huvudsak två handlanden efter att tillstånd erhållits, dels att en brottsbekämpande myndigheten bereder sig hemlig tillgång till ett avläsningsbart informationssystem, dels att tillgängliga uppgifter hämtas in från systemet.[212] Hur brottsbekämpande myndigheter bereder sig tillgång till en enhet beskrivs genom teknikneutrala termer som tekniska hjälpmedel. I propositionen beskrivs att:

[209] Se 2 § HDA.
[210] SOU 2023:78 s. 17-18; Prop 2019/20:64 s. 209-214.
[211] Se även Prop. 2019/20:64 s. 102-106.
[212] SOU 2023:78 s. 62.

> Eftersom de tekniska metoderna för detta kan se olika ut och förändras över tid bör begreppet vara teknikneutralt. Därför bör det framgå att den brottsbekämpande myndigheten får läsa av eller ta upp uppgifterna med ett tekniskt hjälpmedel. Begreppet tekniskt hjälpmedel avser såväl hårdvara som programvara[213]

Vidare exemplifieras möjliga beredningstekniker till ett avläsningsbart informationssystem som installerande av elektroniska program på en enhet eller användandet av fysiska föremål, som ett chip. Reglerna för verkställigheten fastställs särskilt i 22-26 §§, och i propositionen samt i den nya utvärderingen framkommer att systematiken för genomförandet är strikt reglerat. Bland annat har inrättats en särskild HDA-funktion som utför all dataavläsning och ansvarar för inköp och framtagande av kontrollerade tekniska lösningar. Vilka exakta metoder som används är av uppenbara själ hemliga, men det kan exempelvis vara installerande av spionprogram på en enhet. Ett typexempel är hur ett infekterat samtal till ett WhatsApp-konto kan räcka för att installera spionprogramvara på enheten.[214] ”När mobilen väl är infekterad kan polisen få i princip obegränsad tillgång – avlyssna samtal, kopiera chattar, spionera via kameran och mikrofonen.”[215] är ett utmärkande citat som markerar den extensiva dimensionen av möjligheterna med HDA.

5.4.5.3 Skyldigheter för tjänsteleverantörer

Enligt 24 § HDA är vissa operatörer och tjänsteleverantörer skyldiga att medverka vid en verkställighet av en hemlig dataavläsning. De tjänsteleverantörer som omfattas är vad som framgår av 2 kap. 1 § LEK, och är därför både allmänna elektroniska kommunikationsnät samt allmänna nummerberoende kommunikationstjänster. Medverkansskyldigheten omfattar inte nummeroberoende kommunikationstjänster.[216] Skyldigheten inbegriper exempelvis kravet att tillhandahålla relevant teknisk information om det informationssystem och förbindelser som omfattas av ett

[213] Prop. 2019/20:64 s. 102.
[214] SOU 2023:78 s. 283-286; Prop. 2019/20:64 s. 103; se exempelvis Larsson (2023).
[215] Larsson (2023).
[216] SOU 2023:78 s. 82; se vidare i kapitel 5.5.

tvångsmedelsbeslut. Det kan även krävas att särskilda tekniker enligt 22 § HDA används för att möjliggöra för dataavläsning.[217]

5.4.5.4 Tillstånd och begränsningar

Reglerna om hemlig dataavläsning är tillämpliga under specificerade omständigheter både under och utanför en pågående förundersökning. Dessa regler har genomgått flera utvidgningar, särskilt genom de ändringar i lagstiftningen som trädde i kraft den 1 oktober 2023. Enligt 3 § HDA får ett tillstånd till hemlig dataavläsning endast beviljas om skälen för åtgärden väger upp för det intrång åtgärden innebär. För tillstånd krävs det alltid att en proportionalitetssbedömning genomförs både innan och under verkställigheten. Som tidigare nämnts krävs det att andra möjliga tvångsmedel redan har uttömts eller inte kan anses tillräckliga.[218] I 4-6 §§ HDA fastställs i vilka uttömmande fall tvångsmedlet kan användas i en förundersökning. 4 § hänvisar till samma regel som gäller för hemlig avlyssning, och kräver att någon är skäligen misstänkt för ett brott som ställs upp i brottskatalogen i 27 kap. 18 a § rättegångsbalken och att åtgärden är av synnerlig vikt för utredningen. Enligt 4 b, c och 5 §§ HDA får tillstånd i vissa fall beviljas för att utreda vem som skäligen kan misstänkas för ett brott som stadgas i 27 kap. 18 b, 19 b och 29 d §§ rättegångsbalken.

I 7-8 §§ HDA möjliggörs för hemlig dataavläsning i underrättelseverksamhet. Regleringen liknar preventivlagens bestämmelser för hemlig avlyssning som diskuterades i kapitel 5.3. Sammanfattningsvis får hemlig dataavläsning beviljas för ett brottsförhindrande syfte om det finns en påtaglig risk för att en person ska utöva särskild brottslig verksamhet och åtgärden anses vara av synnerlig vikt för att förhindra den brottsligheten. I HDA likt preventivlagen stadgas särskilda bestämmelser i syfte att träffa personer som är involverade i organiserad brottslig verksamhet.[219] Det föreligger även ett förbud mot tvångsmedlet för särskilt skyddsvärda verksamheter fastställda i 11 § HDA.

[217] SOU 2023:78 s. 287-289: Prop. 2019/20:64 s. 237-239.
[218] Prop. 2019/20:64 s. 214-215.
[219] Se 7 § HDA och 1 och 1 a §§ preventivlagen.

5.5 Kort om pågående utredning om datalagring och åtkomst till elektronisk information

I maj 2023 presenterades den statliga utredningen om datalagring och åtkomst till elektronisk information (SOU2023:22) med uppgiften att granska och utvärdera gällande föreskrifter om lagring och åtkomst av elektronisk kommunikation för brottsbekämpande ändamål. Målet är att säkerställa en kontinuerlig förbättring av brottsbekämpande myndigheternas tillgång till information, samtidigt som hänsyn tas till teknologiska framsteg, förändrade kommunikationsmönster och respekt för mänskliga rättigheter.[220]

Utredningen har särskilt övervägt att implementera en liknande lagstiftning som gäller för teleoperatörer och nummerberoende kommunikationstjänster även för nummeroberoende interpersonella kommunikationstjänster (benämnda som NOIK i utredningen). Det nämns särskilt att den omfattande mångfalden av internetbaserade tjänster som Apple iMessage, WhatsApp, Signal och Facebooks Messenger markant har påverkat dagens kommunikationsvanor.[221] Sådana tjänster saknar för närvarande exempelvis en skyldighet att lagra data för brottsbekämpande syften enligt 9 kap. 19 § LEK och undgår medverkanssskyldigheten för HDA i 22 §, vilket försvårar möjligheten till hemlig dataavläsning på sådana tjänster.[222] Utredningen konstaterar att nuvarande regelverk angående NOIK är otillräckligt för att uppnå brottsbekämpande myndigheters påtagliga informationsbehov.[223]

Ett framstående förslag är införandet av en skyldighet för NOIK att samarbeta och anpassa sin verksamhet för att möjliggöra verkställande av hemliga tvångsmedel. Utöver att förenkla möjligheten till hemlig dataavläsning syftar förslaget till att göra viss information, som tidigare endast var tillgänglig genom HDA, tillgänglig genom mindre ingripande tvångsmedel som hemlig avlyssning. Skyldigheten kommer även att inkludera E2E-krypterade tjänster,

[220] SOU 2023:22 s. 3-4 och 21.
[221] SOU 2023:22 s. 25-27.
[222] Båda regleringarna hänvisar till nuvarande lydelse av 2 kap. 1 § LEK, se kapitel 5.3.
[223] SOU 2023:22 s. 25-27.

vilket innebär att leverantörer av sådana tjänster måste anpassa sina system för att uppfylla samarbetskraven. [224] I praktiken innebär lagförslaget att alla leverantörer av alla kommunikationstjänster tvingas kompromissa med sin kryptering. En framtida ansvars- och samarbetsskyldighet enligt utredningens slutsatser kan exempelvis uppfyllas genom att tjänsteleverantörer installerar bakdörrar till sina säkra system. Det kan liknas vid kraven som ställs på leverantörer enligt Online Safety Bill och Chat Control-förordningen.[225]

5.6 En avslutande kommentar

I det efterföljande analyskapitlet kommer det presenterade regelverket och berörda utredningar analyseras i samband med lagförslagen i kapitel 4 samt straffprocessrättens funktioner och modeller i kapitel 3. Jag lämnar därför den fördjupande diskussionen till nästkommande sida för att inte upprepa mig. Men för att avslutningsvis kort sammanfatta den svenska regleringen kan det konstateras att nuvarande regelverk för elektronisk kommunikation och hemliga tvångsmedel kan uppfattas som bristfälligt i relation till dagens utbredda användning av krypterade kommunikationsmedel. Vid första anblick kan de ständigt utvidgade möjligheterna till användandet av hemliga tvångsmedel, i underrättelseverksamhet och förundersökningsverksamhet, anses ge brottsutredande myndigheter goda medel för tillgång till elektronisk kommunikation. Det ska också poängteras hur främst hemlig dataavläsning måste anses utgöra ett ytterst extensivt tvångsmedel, som omfattar insamling och avläsning av en oerhört bred mängd information. Krypterade kommunikationstjänster kan i allmänhet nås genom HDA. Däremot lider särskilt möjligheten till hemlig avlyssning, liksom gällande regler för datalagring och medverkansskyldigheter, av krypterade kommunikationer som huvudsakligen utgörs av nummeroberoende kommunikationstjänster. Det kommenteras vidare i analysen hur det svenska systemet gradvis utvecklas mot en lagstiftning som ställer krav på att tjänsteleverantörer måste underlätta för effektivt verkställande av hemliga tvångsmedel på deras tjänst.

[224] SOU 2023:22 s. 27.
[225] Se vidare i kapitel 4.

6 Analys

6.1 En jämförelse mellan svenskt regelverk, Chat Control-förordningen och Online Safety Bill

En uppenbar slutsats är att gällande regelverk om elektronisk kommunikation och hemliga tvångsmedel i Sverige är oerhört fragmenterat och svåröverskådligt. Dels möjliggör de många hänvisningarna lagarna emellan för en förvirring gällande både tillämplighet och begreppsinnebörd. Dels är rättsområdet komplext gällande vilka åtgärder som är tillåtna inom ramen för en förundersökning jämfört med preventiva brottsbekämpande insatser. Med avstamp i Lagrådets uttalanden kan det vidare konstateras att det tekniskt komplicerade regelverket är abstrakt för gemene man. Det förstärker uppfattningen om att gällande regelverk för brottsbekämpande myndigheters åtkomst till elektronisk kommunikation är ett eländigt och snårigt verk.

Både Chat Control-förordningen och Online Safety Bill vill införa skyldigheten för tjänsteleverantörer att i ett första steg kunna bereda sig tillgång till all kommunikation och informationsöverföring som pågår på tjänsten, för att i nästa steg automatiskt skanna innehållet efter särskilt material. Enligt svensk lagstiftning är det främst genom användningen av tvångsmedlet hemlig avlyssning enligt 27 kap. 18 § rättegångsbalken som brottsbekämpande myndigheter för närvarande har möjlighet att få tillgång till elektronisk kommunikation genom tjänsteleverantören. För kommunikation som är E2E-krypterad har tjänsteleverantörerna vid hemlig avlyssning inte kunnat ge tillgång till informationen till brottsbekämpande myndigheter. Det beror på att den elektroniska kommunikation som upptas är krypterad även för tjänsteleverantören. Genom att införa en lagstadgad skyldighet för tjänsteleverantörer att kunna erbjuda en faktisk tillgång till innehållet i ett tidigare krypterat kommunikationsutbyte hade tvångsmedlet kunnat användas med allt större framgång.

För tvångsmedlet hemlig dataavläsning är situationen annorlunda. Som framkommit är tvångsmedlet en ytterst ingripande åtgärd som möjliggör för

brottsbekämpande myndigheter att på egen hand ta sig in i en enhet och i princip läsa av allt elektroniskt informationsutbyte. Det inkluderar även krypterade kommunikationer under förutsättning att den som använder enheten under tiden för dataavläsningen exempelvis öppnar upp en sådan kommunikationsapplikation.

För att jämföra tvångsmedlet med Chat Control och Online Safety Bill kräver inte hemlig dataavläsning någon egentlig inblandning av en tjänsteleverantör. Tillvägagångsättet för brottsbekämpande myndigheter enligt HDA är i praktiken att hacka sig in i en enskild enhet för att genomföra en dataavläsning. Genom dataavläsning finns det därför redan stora möjligheter för brottsbekämpande myndigheter att nå tillgång till krypterade kommunikationer. Möjligheten hade dock underlättats och utvidgats om tjänsteleverantörer hade behövt vara behjälpliga. I dagsläget finns det en viss medverkanskyldighet som kan tvinga vissa tjänsteleverantörer att bistå med relevant information om sina tekniska system, samt i viss mån anpassa sina tjänster, för att möjliggöra för hemlig dataavläsning. Skyldigheterna i svensk lagstiftning kan anses likna den anpassningsskyldighet som Chat Control och Online Safety Bill vill införa för tjänsteleverantörerna. De presenterade lagförslagen vill dock införa mer långtgående krav för leverantörerna att bland annat möjliggöra för skanning av olagligt material, och kunna ge åtkomst till innehållet för relevanta myndigheter och organ.

För tillfället är den typen av medverkansskyldighet och teknikanpassning som kan krävas av tjänsteleverantörer i svensk rätt idag inte tillämplig på nummeroberoende kommunikationstjänster. I SOU 2023:78 utreds dock möjligheten att införa ytterligare anpassningsskyldigheter för både nummerberoende och nummeroberoende tjänster. När sådana utökade skyldigheter införs, vilket rättsutvecklingen tyder på, kommer den svenska lagstiftningen om hemliga tvångsmedel och elektronisk kommunikation i stor utsträckning att innebära liknande hinder för E2E-krypterade kommunikationstjänster på marknaden som Online Safety Bill och Chat Control förespråkar. Främst för hemlig avlyssning och hemlig dataavläsning införs krav på alla leverantörer av elektroniska kommunikationstjänster att

anpassa sina system för att möjliggöra verkställandet av tvångsmedlen. I praktiken innebär en framtida lagstiftning enligt SOU 2023:78 att leverantörer måste kompromissa med sin kryptering, exempelvis genom att installera bakdörrar till sina kommunikationssystem.

Oavsett om de utökade skyldigheterna enligt SOU 2023:78 om medverkan och anpassning för kommunikationstjänster införs i svensk rätt, kan det framtida regelverket inte jämföras med den generella övervakningsskyldighet som Chat Control och Online Safety Bill vill införa. I förhållande till svensk rätt är det i grunden inte införandet av skyldigheter för leverantörer att kunna nå åtkomst till kommunikationsinnehållet som kan anses särskilt kontroversiellt. Det är den övergripande och generella skanningen av all kommunikation som utgör en eskalering av de rättsliga åtgärder som vidtas för ett brottsbekämpande syfte. Enligt Chat Control och Online Safety Bill måste alla leverantörer övervaka all kommunikation enligt särskilda indikationer som ska kännetecknа viss olaglig kommunikation. Den typen av automatisk massövervakning är inte möjlig inom det svenska regelverket för hemliga tvångsmedel.

Oavsett hur utvidgade möjligheter det finns för brottsbekämpande myndigheter i Sverige att genomföra hemlig avlyssning eller dataavläsning krävs det i dagsläget alltid ett tillstånd. Visserligen indikerar den rättsliga utvecklingen att myndigheter tilldelas ökade befogenheter för preventiv användning av tvångsmedel och har större möjligheter att avlyssna eller bevaka individers kommunikationer även utan specifik brottsmisstanke. De straffprocessuella möjligheterna för övervakning av elektronisk kommunikation kan dock inte anses utgöra en tillståndslös allomfattande massövervakning. Som precis fastställts i stycket ovan kan detsamma inte sägas för varken Chat Control-förordningen eller Online Safety Bill.

Sammanfattningsvis föreligger det en stor diskrepans mellan de diskuterade lagförslagen och det svenska regelverket gällande en generell övervakning av elektronisk kommunikation. När det gäller den faktiska E2E-krypteringen och tjänsteleverantörers skyldigheter att bryta krypteringen på begäran av en

brottsbekämpande myndighet kan likheter konstateras mellan regelsystemen. Inom svensk rätt är det idag endast nummerberoende tjänster som kan tvingas anpassa sina system för att möjliggöra för straffprocessuella hemliga tvångsmedels genomförande. Det kan dock anses sannolikt att skyldigheten kommer att utvidgas till alla leverantörer av kommunikationstjänster på den svenska marknaden. Att begränsa möjligheten till E2E-krypterad kommunikation, i likhet med vad som förespråkas i Online Safety Bill och Chat Control, ligger därför i framkant för det svenska straffprocessuella rättssystemets framtidsutsikter.

6.2 Förhållandet till straffprocessrättens yttersta funktion

Redogörelsen för den svenska straffprocessrättens utveckling och modeller för dess bakomliggande syften och funktioner visar på områdets komplexitet Det framgår att straffprocessrättens grundläggande målsättning inte är definierat i varken lag eller doktrin, vilket gör tolkningen beroende av olika tillämpliga modeller och ideologier.

Efter politiseringen av kriminalpolitiken på 1990-talet betraktas den lagstiftande makten som reglerar straffprocessrätten som en ren politisk verksamhet. En ökad lagstiftningsmakt under de senaste årtiondena, driven av politiskt opinionstryck, har snabbt förändrat det brottsförebyggande och brottsbekämpande arbetet. Träskman betonar övergången från brottskontroll till dagens inriktning mot brottsbekämpning. Han pekar på hur lagreformer i Sverige alltmer fokuserar på det brottspreventiva arbetet med riktad kontroll av förutsedda brottslingar. Kriminalpolitiken associeras med en straffinriktad populism, där politiker och beslutsfattare antar en hårdare inställning till brottsbekämpning för att vinna stöd från allmänheten, snarare än att basera åtgärder på evidens, forskning eller långsiktiga strategier.

Victors och Träskmans teorier får särskild relevans vid diskussion om de starka politiska påtryckningarna för att bekämpa sexuella övergrepp mot barn på nätet, vilket tydligt återspeglas i debatten om Chat Control och Online

Safety Bill. För lagförslagen, särskilt Chat Control, är ett centralt syfte att förhindra och bekämpa sexuella övergrepp mot barn som sker på krypterade kommunikationstjänster. Den politiska debatten om att skydda barn på nätet och motverka spridning av CASM-material är svår att opponera sig emot med tanke på det extensiva allmänneliga stödet för sådana målsättningar. Den offensiva politiken snabbar på utredningsarbeten som allt oftare förespråkar en straffprocessrättslig lagstiftning med stränga och inskränkande åtgärder för effektiv brottsbekämpning. Att införa en möjlighet för brottsbekämpande myndigheter att kunna nyttja information som annars dolts i krypterade former måste anses förenliga med den populistiska kriminalpolitiken.

Enligt Packers modeller för förståelsen av straffprocessrättens syfte och funktion indikerar det pågående utökningsmönstret av brottsutredande myndigheters befogenheter att effektivitet är det centrala fokuset i lagstiftningen. Den exponentiella tillväxten av myndigheters verktyg för att genomsöka individers elektroniska kommunikationer kan inte tolkas på annat sätt än att ständigt ge företräde åt effektivt brottsbekämpande. Debatten om brottsbekämpningens utmaningar i det tekniskt moderna samhället med ökande nätverksrelaterad kriminalitet problematiserar relationen mellan effektiv brottsbekämpning och individens skydd mot överdrivna statliga repressioner. Enligt Packers modeller betraktas förhållandet mellan effektivitet och individens rätt till skydd mot staten som en dikotomi. Detta kan tolkas återspegla verkligheten där antingen det brottsbekämpande motivet eller det individuella perspektivet tydligt dominerar den rådande synen på straffprocessrättens funktion och krav i samhället.

Området för straffprocessrätt kan därför uppfattas som pendlande när det kommer till syfte och funktion. Ibland domineras funktionen av staten som brottsbekämpande mekanism där straffprocessuell lagstiftning som begränsar möjligheterna till E2E-krypterade kommunikationsmedel anses legitima för att upprätthålla effektiv brottsbekämpning. Utifrån effektivitetsperspektivet är därför både Online Safety Bill och Chat Control-förordningens begränsningar av kryptering på marknaden en rimlig lösning för att hantera samhällets problem med kriminalitet.

Utifrån Packers defensiva modell får inte straffprocessuell rätt möjliggöra för någon form av överdriven repression eller maktmissbruk mot individen. Utifrån rådande politiska uttryck, lagförarbeten och den rättsliga utvecklingen kan konstateras att individens rättigheter ofta får anses underordnas lagar och åtgärder som anses effektiva för brottsbekämpningen. Både Online Safety Bill och de begränsande bestämmelserna i Chat Control-förordningen skulle inte ha ansetts vara rättfärdigade enligt den defensiva modellen. Det konstateras dock att dagens lagstiftning på området inte präglas av en defensiv attityd gentemot straffprocessuella regelverk.

En viktig faktor är dock Jareborgs inflik om att en offensiv kriminalpolitik och straffprocessrätt förutsätter att lagstiftning och åtgärder som vidtas enligt perspektivet i verkligheten faktiskt är effektiva. För att kunna motivera en lagstiftning som inskränker en möjlighet till krypterad kommunikation för ett brottsbekämpande syfte, måste det leda till faktiska resultat. Som diskuterades i kapitel 2 om användandet av krypterade kommunikationstjänster fastställs att nätverksrelaterad kriminalitet utnyttjar de krypterade möjligheterna till planering och genomförande av brott. Genom exempelvis dekrypteringen av tidigare krypterade kommunikationstjänster som Anom och Encrochat kan konstateras att åtkomsten av innehållet i kommunikationen var avgörande för att brottsbekämpande myndigheter effektivt kunde utföra sitt arbete. Det skulle kunna ses som en bekräftelse på att effektivitetsperspektivet faktiskt kan motivera en lagstiftning där krypterade kommunikationsmöjligheter begränsas för att straffprocessrättens funktion om effektiv brottsbekämpning ska kunna uppnås.

Likt den proportionalitetsbedömning som krävs innan tillstånd beviljas för hemliga tvångsmedel i Sverige, bör också resultatet av en åtgärd som motiveras av effektivitet anses vara tillräckligt effektivt i förhållande till den inskränkning som det medför för individen. För att ett perspektiv om effektiv brottsbekämpning ska kunna rättfärdiga inskränkande straffprocessrättslig lagstiftning krävs därför att upprepade utvärderingar bevisar ett tillräckligt effektivt resultat. En sådan kvalitativ bedömning borde vidare utforskas.

6.3 En kort reflektion om särskilt kritiska aspekter

> Integritetsintresset och behovet av hemliga tvångsmedel står mot varandra. Pendeln har svängt fram och tillbaka. Just nu vill alla ha mer tvångsmedel men var vi befinner oss om tio år har jag inte en aning om.[226]

Citatet av Gunnel Lindberg[227] kan anses karaktärisera dagens föränderliga politik och svängande inställning till straffprocessuella tvångsmedel och brottsbekämpande lagstiftning. Just nu är det så stort fokus på att öka brottsbekämpande myndigheters möjligheter att hantera kriminaliteten att jag får en uppfattning om att få stannar upp för att se vart lagstiftningen är på väg. Direktiv går om varandra, utredningar staplas på hög och propositioner med olika straffprocessuella lagförslag återanvänder varandras granskningar om effektivitet och rättssäkerhet. Uppsatsens resonemang landar i en slutsats om att rationella tankemönster, underbyggda juridiska resonemang och ideologiska argumentationer tar allt mindre plats i lagstiftningsprocessen.

Det kan argumenteras för att dagens politiker oftare anpassar sig efter rådande opinion och framför frågor och idéer för rättssystemets utveckling i enlighet med det som anses passande i stunden. I en demokratisk kontext är det medborgarnas vilja och åsikter som styr den politiska inriktningen. Allmänhetens värderingar påverkas och formas av flera faktorer i samhället. Till exempel kan den omfattande medierapportering om skjutvapenvåldet i Sverige vara en faktor som påverkar allmänhetens inställning till det brottsbekämpande arbetet. En annan faktor är okunskapen om vad lagtekniska och komplicerade regelverk egentligen innebär för olika samhällsaktörer. Jag tvivlar på att allmänheten förstår innebörden av en reglering som medför att alla meddelanden och bilder som skickas inom EU ska genomgå en automatisk skanning. När till och med Lagrådet uttrycker att det ”har varit svårt för Lagrådet att överblicka de mera praktiska konsekvenserna”[228] av de tekniska lösningarna i lagstiftningen, kan det konstateras att det råder

[226] Lindberg (2022b).
[227] Tidigare överåklagare, sakkunnig i Justitiedepartementet, ordförande i Säkerhets- och integritetsskyddsnämnden och författare av betydande juridisk doktrin om straffprocessuella tvångsmedel.
[228] Prop. 2021/22:136 s. 951-952.

osäkerhet kring vem som faktiskt förstår regelverket. Om det i framtiden framkommer en ny Edward Snowden, som informerar allmänheten om det nuvarande rättslägets praktiska innebörd, kommer den allmänna inställningen till den effektivt brottsbekämpande lagstiftningen troligen bli mer restriktiv.

6.4 Slutsatser

Den frågeställning uppsatsen avser att besvara är i vilken utsträckning som funktionen av den svenska straffprocessrätten kan anses rättfärdiga en lagstiftning som begränsar möjligheten till end-to-end krypterad kommunikation. Det har utretts hur funktionen och grundläggande syften med svensk straffprocessrätt är ett rörligt fenomen som utgörs av en populistisk kriminalpolitik och pendlar mellan fokus för brottsbekämpning och fokus för individuell frihet och rättssäkerhet. Det har också utretts hur svensk lagstiftning om elektronisk kommunikation i samband med straffprocessuella tvångsmedel som hemlig avlyssning och hemlig dataavläsning i dagsläget möter vissa svårigheter i genomförandet på grund av krypterade kommunikationstjänster. Det konstateras dock att regelverket är under ständig förändring, och att utökade ansvarsregleringar och medverkansskyldigheter för tjänsteleverantörer i framtiden förväntas påverka tillgängligheten av E2E-krypterade kommunikationstjänster på marknaden.

Eftersom den svenska straffprocessrätten, vars funktion och syften påverkas av skiftande kriminalpolitiska tendenser, är dynamisk kan frågeställning endast besvaras med att fastställa att straffprocessrättens grundläggande funktion får anses anpassas utefter den rådande populistiska politiken. Idag råder ett offensivt effektivitetssperspektiv för brottsbekämpande lagstiftning som underordnar en rättslig utveckling och diskussioner om individens rättigheter och friheter. Slutsatsen blir därför att lagstiftning som Chat Control och Online Safety Bill, när det gäller bestämmelser som kan förhindra möjligheter till E2E-krypterad kommunikation på marknaden, i stor utsträckning anses sammanfalla med rådande syn på straffprocessrättens samhällsfunktion för effektiv brottsbekämpning.

Käll- och litteraturförteckning

Offentligt tryck

Sverige

Propositioner

Prop. 2002/03:110 Lag om elektronisk kommunikation, m.m.

Prop. 2011/12:55 De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation.

Prop. 2013/14:237 Hemliga tvångsmedel mot allvarliga brott.

Prop. 2019/20:64 Hemlig dataavläsning.

Prop. 2021/22:136 Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation.

Utredningsbetänkanden

SOU 2012:44 Hemliga tvångsmedel mot allvarliga brott.

SOU 2017:75 Datalagring – brottsbekämpning och integritet.

SOU 2017:89 Hemlig dataavläsning - ett viktigt verktyg i kampen mot allvarlig brottslighet.

SOU 2018:61 Rättssäkerhetsgarantier och hemliga tvångsmedel.

SOU 2022:19 Utökade möjligheter att använda hemliga tvångsmedel.

SOU 2023:22 Datalagring och åtkomst till elektronisk information.

SOU 2023:60 Utökade möjligheter att använda preventiva tvångsmedel 2.

SOU 2023:78 Hemlig dataavläsning - utvärdering och permanent lagstiftning.

Övrigt

Regeringskansliet Faktapromemoria 2020/21:FPM6.

Skriftlig fråga 2022/23:526 av Niels Paarup-Petersen (C).

Svar på skriftlig fråga JU202 3/00879, 2022/23:526.

Europeiska unionen

Europeiska kommissionens Förslag till Europaparlamentets och rådets förordning om fastställande av regler för att förebygga och bekämpa sexuella övergrepp mot barn, COM(2022) 209 final. [cit. Chat Control-förordningen]

EPRS. Proposal for a regulation laying down the rules to prevent and combat child sexual abuse, Complementary impact assessment, 2023-04. [cit. EPRS, Complementary impact assessment 04/2023]

EDPB-EDPS. Joint opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, 2022-07-28. [cit. EDPB-EDPS, Joint opinion 04/2022]

Storbritannien

Government UK. *Online Safety Act 2023*. (26 oktober 2023). Tillgänglig på: <https://www.legislation.gov.uk/ukpga/2023/50/enacted> (besökt 2024-01-02). [cit. Online Safety Act 2023]

Government UK. *Consultation outcome: Online Harms White Paper*. (15 december 2020). Tillgängligt på: <https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper> (besökt 2024-01-02). [cit. DCMS (2022) *Online Harms White Paper*]

Government UK. *Policy paper: Overview of expected impact of changes to the Online Safety Bill.* (18 januari 2023). Tillgänglig på: <https://www.gov.uk/government/ publications/online-safety-bill-supporting-documents/overview-of-expected-impact-of-changes-to-the-online-safety-bill> (besökt 2024-01-02). [cit. DCMS (2023) *Overview of expected impact of changes to the Online Safety Bill*]

Litteratur och tidskrifter

Tryckt litteratur

Anttila, I & Törnudd, P. (1973). *Kriminologi - i kriminalpolitiskt perspektiv. En lärobok.* Norstedts.

Ekelöf, P. O., Andersson, S., Bylund, T., m.fl. (2018). *Rättegång - Tredje häftet.* Åttonde upplagan. Norstedts juridik.

Ermoshina, K., & Musiani, F. (2019). "Standardising by running code": The Signal protocol and de facto standardisation in end-to-end encrypted messaging. *Internet Histories, 3*(3–4), 343–363.

Ermoshina, K., Musiani, F., & Halpin, H. (2016). End-to-End Encrypted Messaging Protocols: An Overview. *Third International Conference, INSCI2016 - Internet Science,* 244 – 254.

Denning, D. E. (1996). 'The future of cryptography' i Ludlow, P (red.). (1996). *Crypto Anarchy, Cyberstates, and Pirate Utopias*. MIT Press.

Diffie, W., & Landau, S. E. (1998). *Privacy on the Line: The Politics of Wiretapping and Encryption*. MIT Press.

Häthén, C. (1990). *Straffrättsvetenskap och kriminalpolitik: De europeiska straffteorierna och deras betydelse för svensk strafflagstiftning 1906-1931: tre studier*. Lund University Press.

Jareborg, N. (1995). 'Vilken sorts straffrätt vill vi ha? Om defensiv och offensiv straffrättspolitik' i Victor, D (red.). (1995). *Varning för straff. Om vådan av den nyttiga straffrätten*. Fritzes Förlag.

Jareborg, N. (2001). *Allmän kriminalrätt.* Istus Förlag.

Kerr, O. S., & Schneier, B. (2017). Encryption workarounds. *106 Georgetown Law Journal 989.*

Le-Khac, N-A., & Raymond Choo, K-K. (2022). *A Practical Hands-on Approach to Database Forensics.* Springer International Publishing.

Lindberg, G. (2022). *Straffprocessuella tvångsmedel - när och hur får de användas?*. Femte upplagan. Karnov Group. [cit. Lindberg (2022a)]

Ludlow, P. (1996). *Crypto Anarchy, Cyberstates, and Pirate Utopias*. MIT Press.

Meinrath, S. D., & Vitka, S. (2014). Crypto war II. *Critical Studies in Media Communication, 31*(2), 123–128.

Monsees, L. (2022). 'Crypto-politics' i Ceron, A (red.). (2022). *Elgar Encyclopedia of Technology and Politics.* Edward Elgar Publishing.

Packer, H. (1964). Two models of the criminal process. *University of Pennsylvania Law Review, 113*(1).

Packer, H. (1968). *The limits of the criminal sanction*. Stanford University Press.

Polismyndigheten. (2 juni 2023). *Myndighetsgemensam lägesbild – organiserad brottslighet 2023.* Polismyndighetens tryckeri.

Polismyndigheten. (19 oktober 2021). *Myndighetsgemensam lägesbild – organiserad brottslighet 2021*. Polismyndighetens tryckeri.

Pomerantz, J. (2015). *Metadata.* The MIT Press.

Sandgren, C. (2021). *Rättsvetenskap för uppsatsförfattare: Ämne, material, metod och argumentation.* Fjärde upplagan. Norstedts juridik.

Singh, S. (2000). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Anchor Books.

Svensson, E. (2016). *Gärningsmannaskap vid fleras deltagande i brott.* Iustus Förlag.

Tham, H. (1995). ’Från behandling till straffvärde. Kriminalpolitik i en förändrad välfärdsstat’ i Victor, D (red.). (1995). *Varning för straff. Om vådan av den nyttiga straffrätten*. Fritzes Förlag.

Tham, H. (2022). *Brott och straff i Sverige sedan 1965.* Norstedts Juridik.

Trengove, M., Kazim, E., Almeida, D., m.fl. (2022). A critical review of the Online Safety Bill. *Patterns, 3*(8).

Träskman, P. O. (2008). Vem är kriminalpolitikens nyckelperson: brottslingen, brottsoffret eller ”jag” själv?. *Juridisk Tidskrift,* 497-515.

Ulväng, M. (2009). ’Om straffrätt och principer’ i Asp, P., Lernestedt, C., & Ulväng, M. (2009). *Katedralen - Tre texter om straffrätt*. Iustus Förlag.

Victor, D. (1995). ’Politik och straffsystem - ett drama under utveckling’ i (1995). *Varning för straff. Om vådan av den nyttiga straffrätten*. Fritzes Förlag.

Övriga elektroniska källor

Apple. (7 december 2022*). Apple advances user security with powerful new data protections.* Tillgänglig på: <https://www.apple.com/newsroom/2022/12/apple-advances-user-security-with-powerful-new-data-protections> (besökt 2024-01-02).

Brå. Rapport 2023:13. *Barn och unga i kriminella nätverk. En studie av inträde, brott, villkor och utträde.* [Brå, Rapport 2023:13]

Cantwell, O. (31 mars 2023). *Bedrövligt av regeringen att säga ja till chat control.* Aftonbladet. Tillgänglig på: <https://www.aftonbladet.se/nyheter/kolumnister/a/76xrr4/chat-control-bedrovligt-att-regeringen-sager-ja> (besökt 2023-12-12).

Cleris, J. (26 augusti 2013). *Darknet bistår brott och demokrati*. Dagens Nyheter. Tillgänglig på: <https://www.dn.se/nyheter/sverige/darknet-bistar-brott-och-demokrati/> (besökt 2023-12-12).

Fors, E. (16 juni 2021). *Ungern förbjuder ”främjande” av homosexualitet.* SVT Nyheter. Tillgänglig på: <https://www.svt.se/nyheter/utrikes/ungern-forbjuder-framjande-av-homosexualitet> (besökt 2023-12-26).

Greenberg, A. (2014). *Hacker Lexicon: What Is End-to-End Encryption?*. Wired. Tillgänglig på: <https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/> (besökt 2024-01-02).

Heed, J., & Jörnmark, D. (11 juni 2021). *Operation Trojan Shield och FBI-fällan - P3 Nyheter Dokumentär*. Sveriges Radio. Tillgänglig på: <https://sverigesradio.se/avsnitt/operation-trojan-shield-och-fbi-fallan-p3-nyheter-dokumentar> (besökt 2023-12-04).

Hyllert, U., & Wiman Snäll, E. (9 april 2023). *”EU:s nya massövervakning får inte förstöra källskyddet”*. Dagens Nyheter. Tillgänglig på: <https://www.dn.se/debatt/eus-nya-massovervakning-far-inte-forstora-kallskyddet/> (besökt 2023-12-12).

Karlung, J. (3 april 2023). *”Chat control är en demokratisk katastrof”*. Svenska Dagbladet. Tillgänglig på <https://www.svd.se/a/xgVxrX/jon-karlung-bahnhof-chat-control-ar-en-demokratisk-katastrof> (besökt 2023-12-12).

Larsson, L. (21 oktober 2023). *Vapnet mot gängen - polisen hackar hundratals mobiler*. Dagens Nyheter. Tillgänglig på:

<https://www.dn.se/sverige/vapnet-mot-gangen-polisen-hackar-hundratals-mobiler/> (besökt 2023-12-16).

Lindberg, G. (11 november 2022). *”Jag blir rädd när politiker säger att polisen ska få alla verktyg på önskelistan”.* Dagens Juridik. Tillgänglig på: <https://www.dagensjuridik.se/nyheter/jag-blir-radd-nar-politiker-sager-att-polisen-ska-fa-alla-verktyg-pa-onskelistan/> (besökt 2023-12-28). [cit. Lindberg (2022b)]

Lodding, M., & Öhrstedt, B. (23 mars 2021). *Det här är Vårbynätverket på 60 sekunder*. SVT Nyheter. Tillgänglig på: <https://www.svt.se/nyheter/lokalt/stockholm/det-har-ar-varbynatverket-pa-60-sekunder> (besökt 2023-12-04).

IMY. (8 juni 2023). *CSAM-förordningen (Chat Control 2.0) och ett tryggt informations-samhälle.* Tillgänglig på: <https://www.imy.se/blogg/csam-forordningen-chat-control-2.0-och-ett-tryggt-informationssamhalle/> (besökt 2024-01-02).

Informationsmaterial från Arbetsmarknadsdepartementet. (2 november 2022). *En strategi för lika rättigheter och möjligheter oavsett sexuell läggning, könsidentitet eller könsuttryck.* Tillgänglig på: <https://www.regeringen.se/contentassets/a9e6f17695204d5380edee25b1f069a8/en-strategi-for-lika-rattigheter.pdf> (besökt 2024-01-02). [cit. Arbetsmarknadsdepartementet (2022)]

Internet Watch Foundation. (2022). *Internet Watch Foundation annual report 2020 - face the facts*. Tillgänglig på: <https://www.iwf.org.uk/about-us/who-we-are/annual-report/(2020)> (besökt 2023-12-03).

IT-ord.idg.se. *Chat Control.* Tillgänglig på: <https://it-ord.idg.se/ord/chat-control/> (besökt 2024-01-02). [cit. IT-ord.idg.se.]

Macdonald, J. (2022). *Shut the Back Door: Protecting Encryption From the Online Safety Bill.* Adam Smith Institute. Tillgänglig på: <https://policycommons.net/artifacts/2679408/shut-the-back-door/3702704/ on 19 Oct 2023. CID: 20.500.12592/jtv3jz> (besökt 2023-12-03).

Melchior, S. (9 november 2023). *EU-parlamentet tar strid mot den kontroversiella chat control-lagen.* Dagens Nyheter, Tillgänglig på: <https://www.dn.se/varlden/eu-parlamentet-tar-strid-mot-den-kontroversiella-chat-control-lagen/> (besökt 2023-12-12).

Mosesson, M. (22 oktober 2023). *Så byggde Rawa Majid maktpyramiden som gjort barn till mördare.* Tillgänglig på: <https://www.dn.se/sverige/sa-byggde-rawa-majid-maktpyramiden-som-gjort-barn-till-mordare/> (besökt 2023-12-03).

Myndigheten för samhällsskydd och beredskap. (2023). *Säkra kryptografiska funktioner*. Tillgänglig på: <https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/sakra-kommunikationer/sakra-kryptografiska-funktioner/> (besökt 2024-01-02). [cit. MSB (2023)]

Nadeem, S. M. (2023*). End-to-End Encryption. What Is It and How Does It Work?*. Mailfence. Tillgänglig på: <https://blog.mailfence.com/end-to-end-encryption/> (besökt 2024-01-02).

Polisen. *Sprängningar och skjutningar - Polisens arbete.* Tillgänglig på: <https://polisen.se/ompolisen/polisens-arbete/sprangningar-och-skjutningar/> (besökt 2023-11-30). [cit. Polisen, *Sprängningar och skjutningar - Polisens arbete*)]

Schwartz Wiman, S., & Wiklund, M. (28 september 2023). *Tre döda på tolv timmar – dödligaste månaden hittills*. SVT Nyheter. Tillgänglig på: <https://www.svt.se/nyheter/inrikes/efter-kvallens-skjutning-dodligaste-manaden-pa-fyra-ar> (besökt 2023-12-17).

Tucker, I. (11 juni 2023). *Signal's Meredith Whittaker: 'These are the people who could actually pause AI if they wanted to'.* The Guardian. Tillgänglig på: <https://www.theguardian.com/technology/2023/jun/11/signals-meredith-whittaker-these-are-the-people-who-could-actually-pause-ai-if-they-wanted-to> (besökt 2023-11-30).

Vallace, C. (24 februari 2023).*" Signal would 'walk' from UK if Online Safety Bill undermined encryption".* BBC News. Tillgänglig på: <https://www.bbc.co.uk/news/technology-64584001> (besökt 2023-12-04). [cit. Vallace (2023a)]

Vallace, C. (27 juni 2023). *"Apple joins opposition to encrypted message app scanning."* BBC News. Tillgänglig på: <https://www.bbc.com/news/technology-66028773> (besökt 2023-12-04). [cit. Vallace (2023b)]

Voge, C & Wilton, R. (2022). *Internet Impact Brief: End-to-end Encryption under the UK's draft Online Safety Bill.* Internet Society. Tillgänglig på:

<https://www.internetsociety.org/resources/doc/2022/iib-encryption-uk-online-safety-bill/> (besökt 2023-12-04).

Woodhouse, J., Conway, L., & Lipscombe, S. (31 oktober 2023). *Research Briefing: Online Safety Bill: progress of the Bill.* House of Commons Library. Tillgänglig på: <https://commonslibrary.parliament.uk/research-briefings/cbp-9579/> (besökt 2023-12-04). [cit. Woodhouse m.fl. (2023) *Research Briefing*]

Woodhouse, J. (8 april 2022). *Analysis of the Online Safety Bill*. House of Commons Library. Tillgänglig på: <https://researchbriefings.files.parliament.uk/documents/CBP-9506/CBP-9506.pdf> (besökt 2023-12-04). [cit. Woodhouse (2022) *Analysis of the Online Safety Bill*]

Wright, T. (20 september 2023). *Signal hints at leaving UK market following passage of Online Safety Bill*. Cointelegraph.com. Tillgänglig på: <https://cointelegraph.com/news/signal-hints-leaving-uk-following-online-safety-bill> (besökt 2023-12-04).

Yen, A. (27 oktober 2023). *The Online Safety Act doesn't protect encryption, but Ofcom can.* Proton news. Tillgänglig på: <https://proton.me/blog/online-safety-act> (besökt 2023-12-04).

Rättsfallsförteckning

Hovrätten för Västra Sverige, dom 2022-04-08, mål nr B 6938–21.

Svea hovrätt, dom 2022-04-21, mål nr B 1462–22.

Svea hovrätt, dom 2021-05-21, mål nr B 2251-21.

Svea hovrätt, dom 2021-05-07, mål nr B 3203-21.

Svea hovrätt, dom 2022-02-18, mål nr B 9407-21 och B 3900-21.

Attunda tingsrätt, dom 2023-04-05, mål nr B 5322-21 och B 5369-22.

Attunda tingsrätt, dom 2021-02-22, mål nr B 10010–20.

Eskilstuna tingsrätt, dom 2021-02-26, mål nr B 210–21.

Göteborgs tingsrätt, dom 2021-12-17, mål B 9647–21.

Solna tingsrätt, dom 2022-03-16, mål nr B 10459-20.

Södertörns tingsrätt, deldom 2021-03-04, mål nr B 11907-20.

Södertörns tingsrätt, dom 2021-07-14, mål nr B 3712-21, B 11907-20 och B 5660-21.