JURIDISKA FAKULTETEN
vid Lunds universitet

Laurita Krisciunaite

Inhämtning av digital bevisning vid sexualbrott mot barn via internet

Avvägningen mellan effektivitet och personlig integritet

JURM02 Examensarbete

Examensarbete på juristprogrammet
30 högskolepoäng

Handledare: Ulrika Andersson

Termin för examen: Period 1 HT2019

Innehåll

Summary

The increasing use of internet and the development of technology has led to the transfer of traditional crimes into the digital environment. The internet enables communication to a different extent than before and greater opportunities for sexual offenders to contact children with the aim of exposing them to sexual abuse. Digital evidence is a crucial element in all investigations of such crimes. The purpose of the thesis is to identify the possibilities the police have in order to obtain information regarding electronic communication that can constitute digital evidence in cases regarding sexual offences against children via the internet. The purpose also includes presenting legislative proposals on government hacking as well as adaptation of the rules of house searches and seizures to the digital environment. In addition, the thesis aims to problematize and discuss the balance of interests, between effective law enforcement and personal integrity, made in the legislative context regarding the law enforcement authorities' investigative measures, in the light of the interest of legal security.

The study shows that digital evidence can be obtained in a variety of ways, through house searches, seizures, covert interception and covert surveillance of electronic communication, the Electronic Communications Act and by obtaining information based on agreements from service providers. At the same time, the study shows deficiencies with all of them, which means that the regulation should be reviewed in order to provide effective investigative measures for investigating digital sexual offences against children. All investigative measures described entail a breach of personal integrity. The regulation on electronic communication entails an obligation for operators and internet and telecom providers to store information about users' communication. The purpose of combating internet-related crimes against children has also led providers of services, such as social media and chat sites, to disclose information about communications to law enforcement authorities. The study shows that the interest of effective law enforcement is given priority over personal integrity. However, the conclusion of the study is that the infringement of integrity is legitimate because personal integrity is not an absolute right and the opposing interest of law enforcement is a heavier-weighted public interest. In addition, there are several control and security mechanisms and monitoring bodies that ensure that the regulation does not result in an excessive infringement of integrity or, at least, that the infringement is compensated.

Personal integrity is an important opposing interest and should be discussed more often in order to ensure that the legislation does not go beyond what is necessary for the purpose of crime investigation. In addition, the development of law and society indicates that the powers of law enforcement authorities will need to be adapted further. Discussions on efficiency and personal integrity are thus important in order to maintain legal security.

Sammanfattning

Den ökande internetanvändningen och teknikutvecklingen har lett till en förflyttning av traditionella brott till den digitala miljön. Internet möjliggör kommunikation i en annan utsträckning än tidigare och större möjligheter för sexualförbrytare att kontakta barn i syfte att utsätta dessa för sexuella övergrepp. Digital bevisning avseende elektronisk kommunikation blir ett avgörande inslag i samtliga utredningar av sådan brottslighet. Syftet med uppsatsen är att kartlägga polisens möjligheter att säkra information om och innehåll i elektronisk kommunikation som kan utgöra digital bevisning vid sexualbrott mot barn via internet. I syftet innefattas även att presentera lagförslag om hemlig dataavläsning samt anpassning av reglerna om husrannsakan och beslag till den digitala miljön. Därutöver syftar uppsatsen till att i ljuset av rättssäkerhetsintresset problematisera och diskutera den intresseavvägning som görs i lagstiftningssammanhang av brottsbekämpande myndigheters utredningsmöjligheter, mellan effektiv brottsbekämpning och personlig integritet.

Studien visar att digital bevisning kan inhämtas på flera olika sätt, genom husrannsakan, beslag, hemlig avlyssning och hemlig övervakning av elektronisk kommunikation, lagen om elektronisk kommunikation samt på basis av avtal med tjänsteleverantörer. Samtidigt visar studien brister med samtliga som medför att regleringen bör ses över i syfte att tillförsäkra tillräckligt effektiva utredningsåtgärder vid utredning av sexualbrott mot barn. Samtliga utredningsåtgärder som polisen har till sitt förfogande medför intrång i den personliga integriteten. Regleringen om elektronisk kommunikation medför en skyldighet för operatörer och internet- och teleleverantörer att lagra information om användarnas kommunikation. Ändamålet att bekämpa internetrelaterad brottslighet mot barn har även lett till att leverantörer av tjänster såsom sociala medier och nätforum utlämnar information om kommunikation till brottsbekämpande myndigheter. Studien visar på att effektiv brottsbekämpning ges företräde framför personlig integritet. Samtidigt är intrånget legitimt med hänsyn till att personlig integritet inte är en absolut rättighet och det motstående intresset om brottsbekämpning är ett tungt vägande allmänt intresse. Därutöver finns flera kontroll- och säkerhetsmekanismer samt övervakningsorgan som ser till att regleringen inte medför ett för stort integritetsintrång eller att intrånget åtminstone kompenseras.

Personlig integritet är ett viktigt motstående intresse och bör lyftas upp oftare i lagstiftningssammanhang i syfte att säkerställa att lagstiftningen inte går utöver det som är nödvändigt för utredning av brott. Dessutom talar rätts- och samhällsutvecklingen för att brottsbekämpande myndigheters befogenheter i utredningssammanhang avseende elektronisk information kommer att behöva anpassas. Diskussioner om effektivitet och personlig integritet är därmed viktiga i syfte att upprätthålla rättssäkerhet.

Förkortningar

BrB	Brottsbalken (1962:700)
BRU	Beredningen för rättsväsendets utveckling
Brå	Brottsförebyggande rådet
Ds	Departementsserien
EKMR	Europeiska konventionen om de mänskliga rättigheterna och grundläggande friheterna
FN	Förenta nationerna
HD	Högsta domstolen
IP	Internet Protocol
IT	Informationsteknik
LEK	Lag (2003:389) om elektronisk kommunikation
Libr	Lag (2000:562) om internationell rättslig hjälp i brottmål
NCMEC	National Center for Missing and Exploited Children
NJA	Nytt juridiskt arkiv
Prop.	Proposition
PTS	Post- och telestyrelsen
RB	Rättegångsbalken (1942:740)
RF	Regeringsformen (1974:152)
Rättighetsstadga	Europeiska unionens stadga om de grundläggande rättigheterna
SOU	Statens offentliga utredningar

1 Inledning

1.1 Ämnesbeskrivning

Sexuella övergrepp mot barn som begås på distans har fått ökad uppmärksamhet under de senaste åren. Dessa brott begås nästan uteslutande via olika kommunikationskanaler som använder sig av internet. Övergreppen omskrivs och diskuteras i media till följd av domar där barn förmåtts genomföra sexuella handlingar på sig själva, exempelvis i webbkamera, som dokumenterats av gärningspersonen. Barnpornografi som kan dokumentera det egna övergreppet mot barnet handlar numera nästa uteslutande om digitalt bild- och filmmaterial.[1] Ämnet är högst aktuellt med hänsyn till barn och ungdomars omfattande internetanvändning. Den tekniska och digitala utvecklingen har lett till att användning av internet och medier har blivit en normal del av barnens vardagliga liv.[2] Nästintill alla barn i åldrarna 9-16 år har tillgång till internet i hemmet och använder sig av det dagligen. Majoriteten av barnen i 9-12 års åldern och nästintill alla över tolv år har en egen smartphone.[3]

Samtidigt presenteras siffror på att barns utsatthet för sexuella brott via internet ökar. *Friends*[4] presenterade år 2017 att vart tionde barn i åldrarna 10-16 år utsatts för sexuella trakasserier under de senaste tolv månaderna.[5] Brottsförebyggande rådet (Brå) har i sin undersökning från år 2017 presenterat siffror på årskurs nio elevernas utsatthet på internet. Av de tillfrågade ungdomarna angav 18 %, vilket är en ökning på 3 % sedan år 2015, att de utsatts för sexualbrott under de senaste tolv månaderna.[6] Enligt *Friends* ligger siffrorna i underkant. Beteenden såsom sexuella trakasserier är normaliserade och inget som uppfattas som förbjudet.[7] Det är därmed troligt att fler barn än vad som presenterats i undersökningen utsätts. Det är dock svårt att ge en exakt bild eftersom det inte förs någon kriminalstatistik avseende sexuella övergrepp mot barn via internet. Ett skäl till detta kan vara att dessa brott varken har en egen brottsrubricering eller brottskod hos de brottsbekämpande myndigheterna.

Trots att antalet anmälningar för sexualbrott mot barn ökar är lagföringen av de misstänkta inte särskilt hög.[8] Förra året fick Sverige 10 000 tips från National

[1] Kronqvist, s. 21f, 162-165.
[2] Ungar & medier, 2019, s. 7f.
[3] Ibid, s. 15, 24, 45.
[4] Friends är en politiskt oberoende organisation som genom forskning, utbildning och rådgivning arbetar för att stoppa mobbning.
[5] Friends nätrapport, s. 14.
[6] Brå, 2017, s. 23f, 31.
[7] Friends nätrapport, s. 14.
[8] *Jmf.* Diesen & Diesen, s. 146-156; Sutorius, s. 237f.

Center for Missing and Exploited Children (NCMEC[9]) angående misstanke om sexualbrott mot barn via internet. Ungefär två procent av de inkomna tipsen ledde till förundersökning. År 2019 förväntades polisen få in närmare 20 000 tips.[10] Det låga antalet anmälningar som leder till förundersökning handlar i många fall om brister i bevisningen. Enligt Sutorius är det sällan man konstaterar att ett övergrepp inte har skett. Brottsutredningen läggs oftast ned eftersom det inte går att utreda när, var eller hur övergreppet har skett.[11] Sexualbrott i allmänheten är brott som associeras med stora bevissvårigheter då ord står mot ord.[12] För brott som begås via internet finns i inledningsstadiet oftast endast tillgång till någon form av digital bevisning. Denna kan bestå av dokumenterat övergreppsmaterial men även information om kommunikation mellan gärningspersonen och barnet i form av skärmdumpar[13] på konversationer, trafik-, lokalisering- och abonnemangsuppgifter.[14]

Digital bevisning är flyktigt och oberoende av landsgränser. Bevisning kan finnas i ett annat land än där utredningen genomförs och hos en leverantör som inte lyder under svenska lagar. Vid misstanke om brott måste polisen ha effektiva medel till hands för att säkra tidskänslig information. Dessa medel regleras främst av nationell lagstiftning men inte utan inverkan av EU och annan internationell reglering. Vissa bevissäkringsåtgärder innebär tvång och är hemliga för individen. Åtgärderna går ut på att information om individens beteenden och personliga förhållanden röjs i syfte att utreda ett brott vilket motiveras med behovet av effektiva utredningsåtgärder i syfte att bekämpa brott. Vissa utredningsåtgärder kan endast företas mot en misstänkt person men det finns även åtgärder som kan företas i ett tidigare skede. Alla dessa utredningsåtgärder kan utgöra en inskränkning i det grundlagsstadgade skyddet för den personliga integriteten. Lagstiftaren och rättstillämparen måste beakta dessa motstående intressen vid införande och tillämpning av åtgärder som möjliggör inhämtning av information om och innehåll i elektronisk kommunikation (digital bevisning). I många fall motiveras behovet av tillgång till digital bevisning genom att uppgifterna är nödvändiga för att kunna utreda särskilt allvarliga brott mot rikets säkerhet såsom spioneri och terrorism. Sexualbrott mot barn nämns endast i förbifarten. Med utgångspunkt i den ovan beskrivna problematiken med ökande internetanvändning och barns utsatthet är fokus för denna uppsats sexualbrott mot barn.

[9] Ideell organisation i USA vars uppgift är att hjälpa hitta försvunna barn samt minska sexuellt utnyttjande av barn.
[10] Larsson, telefonintervju; Jerrstedt; *jmf.* Europol, IOCTA, s. 30.
[11] Sutorius, s. 207.
[12] *Jmf.* Diesen & Diesen, s. 146-149.
[13] Nationalencyklopedin definierar *skärmdump* som en bild som visar innehållet på en bild-skärm eller delar av den vid ett givet tillfälle.
[14] *Jmf.* tingsrättens dom i mål nr. B 11206-18.

1.2 Syfte och frågeställningar

En konsekvens av digitaliseringen och den tekniska utvecklingen är att brottsligheten har fått en ny plattform. Barn är i hög grad aktiva i den digitala miljön och riskerar att utsättas för sexuella övergrepp. Det allmänna har en absolut skyldighet att skydda barn från att utsättas för brott.[15] Eftersom barn saknar det konsekvenstänk och slutledningsförmåga som vuxna har är de särskilt skyddsvärda. En fördel med dagens teknik är att all form av aktivitet i den digitala miljön lämnar spår. Dessa spår kan vara avgörande för en brottsutredning där barn utsatts för sexualbrott via internet. Denna uppsats ämnar undersöka två övergripande frågor. I första hand avser uppsatsen att kartlägga de rättsliga möjligheter som polisen har för att inhämta information om och innehåll i elektronisk kommunikation som kan utgöra digital bevisning vid utredning av sexualbrott mot barn via internet. I syftet innefattas även att presentera lagförslag på nya sätt att inhämta sådan information. I andra hand avser uppsatsen i ljuset av rättssäkerhetsintresset problematisera och diskutera den intresseavvägning som görs i lagstiftningssammanhang mellan effektiv brottsbekämpning och personlig integritet. I denna del syftar uppsatsen inte till att diskutera huruvida de enskilda bedömningarna är rättssäkra eller materiellt riktiga utan att undersöka synen på personlig integritet, effektivitet och rättssäkerhet mer principiellt utifrån teorier och argument om dessa.

I avsikt att uppnå uppsatsens syfte kommer följande frågeställningar undersökas och besvaras:

1) Vilka rättsliga möjligheter finns för polisen att inhämta information om och innehåll i elektronisk kommunikation i syfte att utreda sexualbrott mot barn via internet?
2) Hur sker lagstiftarens avvägning mellan intresset att bedriva effektiv brottsbekämpning och intresset att skydda enskildas personliga integritet vid lagstiftning av utredningsåtgärder som avser inhämtning av elektronisk kommunikation, och vilka konsekvenser medför avvägningen för rättssäkerheten?

För att besvara ovannämnda frågeställningar ska även följande frågor undersökas och redogöras för:

1) Vilka sexualbrott mot barn kan begås via internet?
2) Vilken funktion har digital bevisning i en brottsutredning och i den efterföljande rättsprocessen?

[15] *Se* avsnitt 3.2.

1.3 Avgränsning

Sexualbrott mot barn via internet betraktas inte som rena IT-brott men datorteknik används som ett hjälpmedel för att begå ett traditionellt sexualbrott.[16] Digitaliseringen av brottsligheten innebär att det kan förekomma många olika sorters digital bevisning som kan vara av nytta i en brottsutredning. Eftersom kommunikation mellan gärningspersonen och barnet är en förutsättning för ett digitalt övergrepp, kommer fokus för uppsatsen vara digital bevisning som hänför sig till sådan kommunikation. Framställningen har avgränsats till att inledningsvis behandla beslag och husrannsakan i den mån det har betydelse för inhämtning av information om och innehåll i elektronisk kommunikation. Därefter läggs fokus på hemlig avlyssning och hemlig övervakning av elektronisk kommunikation, inhämtning av information enligt lagen (2003:389) om elektronisk kommunikation (LEK) samt informations-inhämtning från tjänsteleverantörer[17]. Avgränsningen till dessa medel har skett utifrån att de bedömts som mest relevanta för den brottslighet som undersöks i denna framställning. De nya lagförslagen som presenteras är omfattande, presentationen kommer begränsas till de mest relevanta delarna för uppsatsens syfte.

Polisens arbete i underrättelseverksamhet kommer inte att behandlas eftersom det bedöms som mindre relevant. Det finns ett antal speciallagar om inhämtning av elektronisk kommunikation i underrättelseverksamhet men dessa är nästintill oanvändbara vid sexualbrott mot barn via internet på grund av de höga straffvärdeskraven.[18]

Sexualbrott mot barn regleras främst i sjätte kapitlet men även i 16 kap. 10a § BrB som reglerar barnpornografibrottet. Det är inte helt ovanligt att en brottsutredning avser undersöka gärningar från hela brottskatalogen. Då uppsatsen syftar till att undersöka hur informationsinhämtning sker vid sådan brottslighet har bedömningen gjorts att ingen fullständig redogörelse av den gällande rätten avseende sexualbrotten behövs. En övergripande beskrivning görs avseende vilka sexualbrott mot barn som kan begås via internet samt deras straffvärden i syfte att sätta uppsatsens frågeställning i sitt sammanhang samt ge läsaren nödvändig kunskap för den fortsatta framställningen.

Den internationella och EU-rättsliga aspekten av uppsatsämnet har begränsats till reglering som avser elektronisk kommunikation. Syftet är inte att analysera

[16] *Jmf.* Interpol, Cybercrime; Brå, 2000, s. 12.
[17] *Se* avsnitt 1.5.2.
[18] *Se* Lag (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott och lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

tillkomsten av sådan reglering utan dess konsekvenser för den nationella rättsutvecklingen.

1.4 Metod och material

Vid författande av juridiska akademiska texter är ett naturligt val av metod den rättsdogmatiska metoden.[19] Eftersom delade meningar råder avseende metodens innehåll är det inte helt enkelt att beskriva på vilket sätt metoden används. Den traditionella bestämningen av rättsdogmatik kan anses innefatta fastställande av gällande rätt och rekonstruktion av rättssystemet. Gemensamt för dessa är att uppgiften utgår från de allmänt accepterade rättskällorna som består av lagtext, lagförarbeten, rättspraxis och doktrin.[20]

Det förekommer olika uppfattningar huruvida värderingar och argument utanför den gällande rätten ingår i rättsdogmatiken. Enligt Jareborg hindrar rättsdogmatiken inte att perspektiv vidgas och går utöver den gällande rätten eftersom rättsdogmatikern ska söka efter ideala lösningar.[21] Trots att Kleineman är en förespråkare av den striktare rättsdogmatiska metoden anser han att rättsdogmatiken inte är skild från värderingar och rättsreglernas tillämpning i praktiken. Kritik genom omvärldsiakttagelser behövs och kan ge ledning för hur gällande rätt borde vara. Detta är dock inte samma sak som uppgiften att faktiskt fastställa gällande rätt menar han.[22] Enligt Sandgren är den rättsdogmatiska metoden i traditionell mening begränsad på så sätt att den inte tillåter uttalanden om effekterna av gällande rätt.[23] Samtidigt framför han argument för att värderingar, normer och fri argumentation i praktiken ingår i diskussionen om gällande rätt.[24] Sandgren ifrågasätter benämningen av metoden som dogmatisk och anser att analytisk skulle vara en mer realistisk och klargörande benämning.[25]

I denna uppsats kommer den strikta rättsdogmatiska metoden användas i syfte att fastställa gällande rätt avseende sexualbrott mot barn via internet samt de brottsbekämpande myndigheternas möjligheter att inhämta digital bevisning. Då uppsatsens ämne har en internationell och EU-rättslig aspekt kommer även sådant material att presenteras. Många rättsakter som antagits inom EU är bindande för Sverige och vid konflikt ska dessa ha företräde framför svensk lag. Principer och uttalanden som EU-domstolen gör ska tillämpas på nationell

[19] *Jmf.* Sandgren, 2016, s. 722.
[20] Sandgren, 2018, s. 48f; Jareborg, 2004, s. 4, 8; Kleineman, s. 21.
[21] Jareborg, 2004, s. 4.
[22] Kleineman, s. 24.
[23] Sandgren, 2018, s. 50.
[24] Sandgren, 2005, s. 652f.
[25] Ibid, s. 656; 2016, s. 724f.

nivå.[26] EU-rättsligt material kommer därmed presenteras i syfte att fastställa gällande rätt och ge regleringen ett sammanhang. Detta gäller främst vid beskrivning av reglerna om elektronisk kommunikation.

Vidare syftar uppsatsen till att gå utöver den gällande rätten. Enligt Sandgren kan rättsanalytisk metod användas om en framställning avser att analysera rätten. Metoden är friare, tillåter en fri argumentation och användning av alla former av material. Därutöver är metoden mer öppen för att ge värderingar spelrum, exempelvis genom att analysera gällande rätt utifrån grundläggande värderingar såsom rättssäkerhet i relation till effektivitet.[27] Uppsatsen avser att undersöka och diskutera hur olika rättsintressen förhåller sig till varandra. Utöver fastställandet av den gällande rätten avser arbetet att öka kunskapen på en mer abstrakt och generell plan vilket motiverar valet av en bredare metod. Rättsanalytisk metod kommer därmed användas genomgående i uppsatsen. Enligt Sandgren kan materialet dock medföra urvalsproblem.[28]

För det första har urval skett utifrån de rättsliga intressen som kommer att undersökas i uppsatsen. Intressena definieras och ges innehåll genom uttalanden i lagförarbeten samt litteratur av auktoritativa författare. De teoretiska utgångspunkterna och argumenten som presenteras kommer att tjäna som underlag för diskussion och analys av lagstiftarens motivering gällande intresseavvägningen vid lagstiftning av polisens möjligheter till inhämtning av digital bevisning. Avseende intresset effektiv brottsbekämpning har material avgränsats till relevanta lagförarbeten och doktrin som behandlar eller är applicerbara på sexualbrott mot barn via internet. Det omvända gäller för personlig integritet. Uppsatsen syftar till att bedöma huruvida allmänhetens personliga integritet kränks, oavsett om individen är utomstående, misstänkt eller offer. Därav kommer allmänna uttalanden angående konsekvenser för den personliga integriteten presenterats. För det andra har materialurvalet avgränsats i tid. I vissa delar, exempelvis vid sexualbrottslighetens utveckling och användning av tvångsmedel, har äldre material beaktats. Den gällande rätten grundas på äldre lagstiftning och värderingar. Internetrelaterad brottslighet och digital bevisning är relativt nya ämnen och har i vissa fall föranlett ett urval av nyare lagförarbeten, litteratur, undersökningar med mera.

Svensk praxis har använts i syfte att påvisa gällande rätt samt för att exemplifiera ett praktiskt fall där digital bevisning haft en framträdande roll. Praxis presenteras endast i för uppsatsen relevanta delar. Således kommer diskussioner som främst avser gränsdragningen mellan olika brott samt

[26] Reichel, s. 111f, 116f; Hettne & Otken, s. 173-175.
[27] Sandgren, 2018, s. 50f.
[28] Ibid, s. 51.

rekvisitens innebörd inte presenteras i detalj. Syftet är istället att presentera hur domstolen resonerat avseende brott som kan begås på distans.

De lagförarbeten som har använts är främst propositioner och statliga utredningar avseende svensk sexualbrottslagstiftning och lagstiftning som på olika sätt reglerar polisens befogenheter att inhämta digital bevisning. Enligt Kleineman kan uttalanden som förekommer i exempelvis propositioner inte ensamt utgöra gällande rätt om de går emot en normalspråkig tolkning av lagtexten som aldrig slagits fast av den lagstiftande församlingen. Uppfattningen är dock att lagförarbeten är accepterade som rättskällor eftersom regeringsmakten har stöd i den lagstiftande församlingen.[29] I denna framställning har lagförarbeten använts som ett hjälpmedel för att utröna gällande rätt samt i syfte att undersöka lagstiftarens syn på effektivitet och personlig integritet. Försiktighet har vidtagits vid val av uttalanden i förarbeten som presenterats som uttryck för gällande rätt. Lagförarbeten har även använts i deskriptivt syfte för att sätta rättsutvecklingen i dess sammanhang och ge en bakgrund till rättsreglernas utveckling.

Användning av doktrin som uttryck för gällande rätt är också omdiskuterat. Doktrin kan tillmätas stor betydelse då de har skrivits av auktoriteter inom akademin. Dess ställning som rättskälla kan även avgöras genom dess starka logiska struktur eller analysens inre logik.[30] I denna framställning används doktrin främst i syfte att få en sammanfattande och heltäckande bild av rättsnormerna och vad dessa säger i vissa frågor. Urvalet av författare har skett utifrån kunskap på de relevanta områdena, det vill säga författare som är professorer eller forskare eller har specialkompetens eller praktisk erfarenhet inom de relevanta rättsområdena.

För att ge ett bredare perspektiv på ämnet används även icke-juridiskt material såsom rapporter, empiriska och statistiska undersökningar, tidningsartiklar och radioprogram. Vidare har enstaka verk från andra akademiska områden såsom kriminologi och informationsteknik använts. Polisens metoder vid inhämtning av bevisning är inte omskrivna utan består huvudsakligen av myndighetens praktiska arbete, särskilt avseende myndighetens möjlighet att inhämta information från tjänsteleverantörer. I syfte att få insyn i detta arbete har telefonintervju genomförts med Lena Larsson, gruppchef för IT-relaterade sexualbrott mot barn på Nationellt IT-brottscentrum SC3 på Nationella Operativa Avdelningen. Av förklarliga skäl kan uppsatsen inte presentera en heltäckande bild av de metoder som polisen använder sig av vid inhämtning av digital bevisning. Intresset att utreda brott motiverar att denna del hålls hemlig.

[29] Kleineman, s. 28f.
[30] Ibid, s. 28f, 33.

1.5 Terminologi

1.5.1 Allmänna begrepp

Barn definieras som varje människa under 18 år.[31] I brottsbalken görs en distinktion mellan barn under femton och barn som fyllt femton men inte arton år. Barn som är under femton år har ett absolut skydd mot sexuella övergrepp då de inte har någon sexuell självbestämmanderätt. I denna framställning används begreppet *barn* i avseende på personer som inte fyllt femton år.

När det kommer till misstanke för sexualbrott är män klart överrepresenterade i kriminalbrottsstatistiken. 97 % av de misstänkta år 2018 var män.[32] Trots detta kommer pronomen *hen* och begreppet *gärningsperson* användas genomgående i uppsatsen för att upprätthålla ett mer könsneutralt språk.

Det finns ingen enhetlig definition för vad som avses med *sexuella övergrepp* mot barn. De olika definitionerna har det gemensamt att en vuxen utnyttjar den minderåriges oförstånd eller okunskap om de sexuella handlingarna samt brist på förståelse för handlingarnas kortsiktiga och långsiktiga konsekvenser för barnet. Svedin definierar sexuella övergrepp mot barn som ”handlingar eller situationer med sexuell innebörd där en vuxen utnyttjar en minderårig”.[33] FN:s barnrättskommitté anser att sexuella övergrepp och sexuellt utnyttjande innefattar bland annat att ”förmå eller tvinga ett barn att delta i någon olaglig eller psykiskt skadlig sexuell aktivitet”.[34] Alla sexuella handlingar som en vuxen företar mot ett barn som är straffbelagda är förbjudna.[35] Sexuella övergrepp som begrepp kan dessutom innefatta flera olika övergrepp.[36] I svensk rätt finns ett särskilt lagstadgat brott som betecknas som sexuellt övergrepp mot barn (6 kap. 6 § BrB). I denna framställning används begreppet som ett samlingsbegrepp, synonymt med begreppet *sexualbrott mot barn*.

Uppsatsen avser endast undersöka polisens rättsliga möjligheter att inhämta digital bevisning. Brottsbekämpande myndigheter används dock som ett övergripande begrepp som innefattar polisens verksamhet eftersom begreppet används genomgående i lagförarbeten och doktrin.

[31] Art. 1 barnkonventionen.
[32] Brå, statistik.
[33] Svedin & Banck, s. 58f.
[34] FN, allmän kommentar, s. 12.
[35] Ibid.
[36] *Jmf.* Sutorius, s. 150f.

1.5.2 Tekniska begrepp

Digital bevisning som begrepp är odefinierat i juridisk litteratur utan avser allt material som härrör från digitala miljöer såsom datorer, mobiltelefoner och andra system som styrs av och innehåller datateknik. Det finns därmed olika sorters uppgifter som kan innefattas i begreppet digital bevisning.[37] Digital bevisning kan delvis bestå av information om information, så kallad *metadata*, men även av innehåll i en viss information, exempelvis innehåll i ett SMS eller en bild.[38] Digital bevisning i ärenden om sexualbrott mot barn via internet kan utgöras av information om elektronisk kommunikation eftersom brottsligheten förutsätter att kommunikation förekommit mellan gärningspersonen och offret. Fokus för uppsatsen är därmed att undersöka tillgång till innehåll i och information om elektronisk kommunikation som i denna uppsats betecknas som *digital bevisning*.

Elektronisk kommunikation innebär överföring av signaler i elektronisk form. Signalerna bygger på data i analog eller digital form som överförs via elektromagnetiska svängningar.[39] Begreppet *digital* avser data som presenteras med hjälp av två siffror, ettor och nollor. Majoriteten av dagens teknik är digital och innefattar bland annat telefoni och datakommunikation. Den tekniska utvecklingen och digitaliseringen har medfört att de olika formerna för överföring av information har konvergerat. Konvergensutvecklingen innebär att olika information kan representeras på samma sätt och att tidigare avskilda nät numera kan användas för att förmedla samma typer av tjänster. Mobiltelefoner kan exempelvis användas för att titta på TV, datorer för att ringa varandra och TV för att surfa på internet.[40] Den tekniska definitionen av *data* är ”fakta, idéer eller liknande i en form lämpad för överföring, tolkning eller bearbetning av människor eller av automatiska hjälpmedel”.[41] Innehållet i data på området elektronisk kommunikation kan innefatta text, ljud och bild.[42] I denna framställning används begreppet *data* synonymt med begreppet *information*.

Informationsbärare används som ett allmänt begrepp och avser fysiska föremål där data kan lämna spår eller presentera informationsinnehåll. Exempel på informationsbärare är hårddisk, mobiltelefon och SIM-kort. Dessa kan kategoriseras olika utifrån deras olika fysiska egenskaper men i denna uppsats görs ingen differentiering.[43] Digital bevisning består därmed av data om elektronisk kommunikation som kan vara digital och som överförs, lagras eller

[37] Kronqvist, s. 19.
[38] Kävrestad, s. 23f.
[39] Prop. 2002/03:110, s. 58.
[40] Ibid, s. 58.
[41] SIS, 2015, s. 7.
[42] Prop. 2002/03:110, s. 58.
[43] Läs mer om detta i Ekfeldts avhandling *Om informationstekniskt bevis*, avsnitt 1.3.3.

på annat sätt behandlas med hjälp av en digital och/eller elektronisk informationsbärare.

Svensk rätt reglerar operatörers och leverantörers skyldigheter vid misstanke om brott i LEK. En *operatör* är den som innehar eller på annat sätt råder över ett allmänt kommunikationsnät eller tillhörande installation, det vill säga den som tillhandahåller direkt anknytning till nätet. I internetsammanhang definieras *leverantör* som ett företag som tillhandahåller tillgång till internet och som en person kan teckna abonnemang hos. Däremot har internetleverantören ingen direkt anslutning till nätet utan måste köpa transit av en operatör. Operatörer kan samtidigt vara internetleverantörer, exempelvis Telia och Tele2.[44] Uppsatsen undersöker även skyldigheten att utlämna digital bevisning som andra leverantörer än operatörer och internetleverantörer har. Leverantörer av webbsidor, sociala medier och andra applikationer kan också inneha betydelsefull information för en brottsutredning. Dessa kommer att betecknas *tjänsteleverantörer*.

1.6 Forskningsläge

Internetrelaterad brottslighet är som nämnt ett ganska nytt fenomen. Särskilt sexualbrott mot barn via internet är ett ganska snävt omskrivet ämne. Det finns ett antal studier utförda i USA och Storbritannien avseende sexualbrott mot barn via internet men svensk forskning är begränsad. Sexualbrott mot barn är omskrivet av bland annat Svedin och Banck i *Sexuella övergrepp mot flickor och pojkar* samt Diesen och Diesen i *Övergrepp mot kvinnor och barn – den rättsliga hanteringen*. Det finns däremot inga svenska doktrin avseende de internetrelaterade brotten. Ämnet är omskrivet i nationell skönlitteratur men främst i internationell litteratur[45]. Den internationella litteraturen fokuserar oftast på det egna landets lagstiftning. Då uppsatsen inte har ett komparativt syfte har relevansen av sådan litteratur varit begränsad. I SOU 2016:60 utreddes huruvida lagstiftningen tillförsäkrade ett tillräckligt skydd för barn mot sexuella övergrepp via internet. Därutöver omnämns sexualbrott mot barn via internet som hastigast i lagförarbeten till tvångsmedelslagstiftningen samt LEK. Ämnet är något mer omskrivet i examensuppsatser i juridik.

Bevisrätten är ett ämne som har en långtgående praxisutveckling och som är generöst omskrivet i doktrin. Däremot finns lite material avseende digital

[44] 1 kap. 7 § LEK; SOU 2000:50, s. 161f.

[45] *Se* exempelvis Davidson, Julia & Gottschalk, Peter (red.), *Internet child abuse: current research and policy*, Routledge, Abingdon, 2011; Martellozzo, Elena, *Online child sexual abuse: grooming, policing and child protection in a multi-media world*, Routledge, Abingdon, 2012; Ost, Suzanne, *Child pornography and sexual grooming: legal and societal responses*, Cambridge University Press, New York, 2009.

bevisning och dess roll i brottsutredningen och rättsprocessen samt avseende elektronisk kommunikation. Digital bevisning är mer allmänt omskrivet ur ett tekniskt perspektiv av Kronqvist i *Brott och digitala bevis: en handledning* och Kävrestad i *Fundamentals of Digital Forensics Theory, Methods, and Real-Life Applications* och mer grundlig ur ett juridisk perspektiv av Ekfeldt i *Om informationstekniskt bevis*. Lindberg har i sin handbok *Straffprocessuella tvångsmedel: när och hur får de användas?* på ett omfattande sätt beskrivit användning av straffprocessuella tvångsmedel och tillämpning av LEK med inslag av diskussion om den digitala bevisningens ställning i svensk rätt. Bring, Diesen och Andersson har också fört en kortare redogörelse av digital bevisning i *Förundersökning*. Ämnet är högst relevant och har föranlett att ett antal examensuppsatser i ämnet har skrivits på senare år.

Personlig integritet omskrivs generöst i litteratur och lagförarbeten. Effektiv brottsbekämpning i relation till personlig integritet omskrivs på en grundläggande plan av Flyghed i *Brottsbekämpning - mellan effektivitet och integritet: kriminologiska perspektiv på polismetoder och personlig integritet*. För en djupare utredning och diskussion om personlig integritet i förhållande till inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet hänvisas till Naarttijärvis doktorsavhandling i samhällsvetenskap *För din och andras säkerhet: konstitutionella proportionalitetskrav och Säkerhetspolisens preventiva tvångsmedel*. Därutöver är ämnet ofta återkommande och djupgående behandlat i lagförarbeten[46] som avser brottsbekämpande myndigheters användning av straffprocessuella tvångsmedel och inhämtning av elektronisk kommunikation. Fokus i dessa ligger främst på verksamhet som avser att bekämpa brott mot rikets säkerhet. Barnpornografibrottet lyfts mer frekvent upp som ett IT-brott på grund av att dess distribution nästan uteslutande sker via internet. Som ett resultat av flera nätpedofilhärvor på senare år har dock även vuxnas kontakter med och utnyttjande av barn i sexuella syften via internet lyfts fram som exempel på brottslighet som kräver effektiva brottsbekämpningsmetoder.[47]

1.7 Disposition

Uppsatsen inleds med detta inledande kapitel som presenterar ämnet, uppsatsens syfte och frågeställningar, metod och inledande terminologiska frågor. Följande avsnitt (kapitel 2) beskriver den teoretiska bakgrunden till intressekollisionen mellan effektiv brottsbekämpning och personlig integritet. I nästföljande avsnitt (kapitel 3) ges en övergripande redogörelse för gällande rätt avseende

[46] *Se* exempelvis SOU 2005:38.
[47] *Se* exempelvis prop. 2011/12:55.

sexualbrott mot barn via internet. Avsnittet avslutas med en presentation av ett exemplifierande fall som belyser betydelsen och nödvändigheten av digital bevisning i sexualbrottmål. Uppsatsen övergår därefter (kapitel 4) till ämnet digital bevisning som utgör uppsatsens huvudsakliga del. Avsnittet inleds med en allmän beskrivning av bevisning i sexualbrottmål och övergår till en beskrivning av nödvändiga terminologiska utgångspunkter för den fortsatta framställningen. Vidare presenterar avsnittet olika rättsliga möjligheter för polisen att inhämta digital bevisning samt lagstiftarens diskussioner kring intressena effektivitet och personlig integritet. Avsnittet övergår till att beskriva inhämtning av information från tjänsteleverantörer samt förslag på ett nytt tvångsmedel – hemlig dataavläsning. Framställningen avslutas (kapitel 5) med en sammanställning och analys av vad som framkommit i uppsatsen som avser att besvara uppsatsens frågeställningar.

2 Intressekollisionen

2.1 Inledning

Att leva i en kollektiv sammanslutning – en stat – innebär att den enskilda individen måste ge upp en del av sin frihet. Frihetsinskränkningen motiveras av att staten ska minska risken för hot från individer mot kollektivet. Allmänhetens förtroende för staten är beroende av att samhället klarar av att förebygga, utreda och lagföra brott. Frihetsinskränkningen som allmänheten upplever måste uppvägas av vinsten för att betraktas som legitim.[48] Det finns två poler i denna diskussion, de som anser att polisens effektivitet ska prioriteras och de som anser att enskildas integritet ska prioriteras.[49] Konflikten mellan polisär effektivitet och medborgerlig integritet är aktuellt i demokratiska samhällen som garanterar medborgarna frihet och garanterar att det allmänna inte ska kunna tillgripa vilka medel som helst för att kontrollera oönskade beteenden. För mycket kontroll kan leda till att medborgarnas förtroende för statsmakten minskar medan ökad effektivitet riskerar att försvaga rättsordningens legitimitet vilket kan leda till samhällelig instabilitet. Det är en balansgång som innebär att staten inte kan utöva för mycket kontroll på bekostnad av de enskildas integritet eftersom demokratin riskerar att urholkas. Övervakning av medborgarna i preventivt syfte är ett steg över gränsen för vad som kan anses vara en godtagbar inskränkning i medborgarnas integritet.[50]

I denna uppsats ska lagstiftningen som reglerar polisens rättsliga möjligheter att inhämta digital bevisning undersökas i ljuset av dessa två intressen. Å ena sidan intresset att bedriva effektiv brottsbekämpning och å andra sidan intresset att skyddas från ingrepp i den personliga integriteten. Lagstiftningen möjliggör en generell övervakning som innebär att samtliga individer övervakas oavsett om individen är misstänkt eller inte. Frågan som uppstår är om allmänheten ska avstå en del av sin rätt till den personliga integriteten till förmån för det kollektiva intresset att effektivt utreda sexualbrott mot barn via internet. I detta avsnitt ges en teoretisk och principiell beskrivning av begreppen rättssäkerhet, effektivitet och personlig integritet.

[48] Flyghed, 2000, s. 11f; SOU 2017:100, s. 28.
[49] Flyghed, 2000, s. 14f.
[50] Ibid, s. 20f; Jareborg, 1992, s. 91f. *Jmf.* Ulväng, s. 13f; Abrahamsson, s. 429f avseende övervakningssamhälle.

2.2 Rättssäkerhet

Rättsprinciperna som staten och lagstiftningen bygger på utgår från ett idealtypsresonemang som grundas i olika teorier om hur saker och ting är eller borde vara.[51] Syftet med uppsatsen är inte att ifrågasätta hur rättigheterna har uppkommit eller vad dess rätta innebörd är eller borde vara utan att definiera dessa i uppsatsens kontext. I en demokratisk rättsstat ska straffsystemet vara uppbyggt på ett sätt som tillförsäkrar den enskilde rättssäkerhet. Det finns ingen entydig definition av rättssäkerhet trots att det används generöst i rättsliga sammanhang. I flera försök till att definiera begreppet finns dock inslag av krav på förutsebarhet och skydd för den enskilda mot godtycklig rättstillämpning.[52]

År 2006 sammanställdes Justitiekanslerns tillsynsprojekt som innefattade en översyn av rättstillämpningens användning av begreppet rättssäkerhet. Där konstaterades att rättssäkerhet ofta förknippas med rättigheter som den enskilde erhåller i förhållande till statens tvångsmedelsanvändning.[53] Begreppet har i den rättspolitiska debatten delats upp mellan materiell och formell rättssäkerhet. Den formella rättssäkerheten kännetecknas av förutsebarhet och likabehandling inför lagen medan materiell rättssäkerhet kännetecknas av materiellt rättvisa resultat i konkreta rättstillämpningsfall.[54] Ett annat sätt att definiera formell och materiell rättssäkerhet är att den materiella rättssäkerheten är ett resultat av en avvägning mellan förutsebarhet och andra etiska värden i konkreta beslutssituationer. Enligt Peczenik handlar diskussionen om skyddet för fri- och rättigheter på en abstrakt nivå om skydd för etiska värden. Förutsebarhet är i sammanhanget ett formellt etiskt värde. Materiell rättssäkerhet är därmed resultatet av sammanvägningen av dessa värden.[55]

Enligt Jareborg finns det ingen anledning att dela upp rättssäkerhet i formell och materiell. Den formella rättssäkerheten skyddar samma värden som den materiella. Bristande förutsebarhet avseende huruvida individen kommer att utsättas för offentlig maktutövning innebär i praktiken samma inskränkning som att utsättas för brott och förlora någon av de medborgerliga fri- och rättigheterna.[56] Jareborg är kritisk till Peczeniks definition av begreppet rättssäkerhet och menar på att vad som är etiskt godtagbart, som ett kriterium för rättssäkerhet, är för oprecist.[57]

[51] Ribbing & Sandgren i Flyghed, 2000, s. 24f.
[52] Ibid, s. 30.
[53] *Felaktigt dömda*, rapport, s. 22.
[54] Ibid, s. 24f.
[55] Peczenik, s. 92, 94f.
[56] Jareborg, 1992, s. 87f.
[57] Ibid, s. 90.

Frändberg definierar rättssäkerhet som ett skydd mot överhetens godtycke som är ett resultat av brist på rättslig reglering. Tre villkor måste vara uppfyllda för att rättssäkerheten ska råda, det ska finnas klara och adekvata regler, reglerna ska vara lättillgängliga för allmänheten och allmänheten ska kunna lita på reglernas innehåll.[58] Ramberg utgår från en liknande formulering om skydd från statens maktmissbruk av rättsordningen. Rättsordningen ska inte kunna missbrukas och användas som en ursäkt för att åsidosätta mänskliga rättigheter. Förutsebarhet innebär inte per automatik att ett rättssystem är rättssäkert. Ett exempel på detta anses vara lagar som är förutsebara med samtidigt kränker mänskliga rättigheter.[59]

Då uppsatsen avser att undersöka tvångsmedel som kan användas vid misstanke om brott är det lämpligt att ansluta sig till den beskrivning av rättssäkerhet som presenteras i rapporten från Justitiekanslerns rättssäkerhetsprojekt men även Jareborgs definition. Lagstiftning som reglerar polisens befogenheter vid inhämtning av digital bevisning ska diskuteras med utgångspunkt i kravet på förutsebarhet och respekt för mänskliga rättigheter. Rättssäkerhet används som ett måttstock för lagstiftningens legitimitet.

2.3 Personlig integritet

Skyddet för den personliga integriteten är en grundlagsstadgad medborgerlig rättighet. Var och en är gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om intrånget sker utan samtycke från den enskilde och innebär en övervakning eller kartläggning av den enskildes personliga förhållanden.[60] Rättigheten är relativ och kan begränsas genom lag för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Därutöver ska inskränkningen vara proportionerlig, får inte innebära ett hot mot den fria åsiktsbildningen och får inte göras på grund av politisk, religiös, kulturell eller annan sådan åskådning.[61] Rätten till personlig integritet kan inskränkas under förutsättning att det uppfyller kraven på legalitet, ändamål, behov och proportionalitet.[62]

Innehållet i begreppet personlig integritet är inte klart definierat och syftet med denna uppsats är inte att finna en ”rätt” definition. Syftet är istället att presentera olika förståelser av begreppet och därigenom precisera användningen av det i uppsatsen. Integritetsskyddet har inte utvecklats utifrån ett definierat begrepp utan genom olika skyddsregler och ställningstaganden i dessa. Skyddet har

[58] Frändberg, s. 274f.
[59] Ramberg, s. 154; Frändberg, s. 271f.
[60] 2 kap. 6 § andra stycket RF.
[61] 2 kap. 20-21 §§ RF; *jmf.* art. 8.2 EKMR.
[62] Bring, m.fl., s. 284f.

utvecklats genom att olika åtgärder, exempelvis straffprocessuella tvångsmedel, i enskilda fall inte ansetts försvarbara med hänsyn till den skada de skulle ha medfört för den enskildas integritet. Det går därmed inte att definiera begreppet utan att beakta motstående intressen såsom brottsbekämpning.[63] Naarttijärvi anförde i sin doktorsavhandling att skyddet för den personliga integriteten härstammar från specifika skyddsbestämmelser i lagstiftningen och inte från grundlagen. Det konkreta skyddet består av processuella krav som ställs inför inhämtning och utlämning av uppgifter i de regelverk som ger mandat till sådan inhämtning och utlämning. Regler som finns i exempelvis rättegångsbalken och andra tvångsmedelslagar som medger undantag från skyddet för den personliga integriteten ger de brottsbekämpande myndigheterna mandat att inhämta information om den enskilda och utgör det konkreta utflödet av regeringsformens skydd. Lagstiftarens ställningstaganden till integritetskränkande åtgärder och dess legitimitet kan utläsas av lagstiftarens redovisning av proportionalitetsbedömningen.[64]

Skyddet för den personliga integriteten har därutöver utvecklats genom olika internationella förpliktelser som Sverige åtagit sig såsom Europeiska unionens stadga om de grundläggande rättigheterna (EKMR). I artikel 8 EKMR stadgas skyddet för privat- och familjeliv, hem och korrespondens och innefattar skydd för den personliga integriteten. Enligt Europadomstolen innefattas i skyddet för privatliv och korrespondens skydd mot olovlig avlyssning och övervakning av telekommunikation. Europadomstolen menar att sådan övervakning utgör ett hot mot integriteten. Inhämtning av viss information, exempelvis om uppringda nummer, kan innebära ett intrång i privatlivet även om intrånget inte anses vara lika allvarligt som vid inhämtning av uppgifter genom hemlig avlyssning. Skyddet gäller redan vid registrering av uppgifter om kommunikation. Även lokaliseringsuppgifter och abonnemangsuppgifter såsom IP-adresser omfattas av skyddet[65]. Intrånget kan dock vara legitimt om det genomförs med stöd av lag.[66] Därutöver är Sverige bunden av EU:s rättighetsstadga samt andra EU-dokument som kontinuerligt utvecklar skyddet för den personliga integriteten genom skyddslagstiftning för personuppgifter, däribland Datalagringsdirektivet[67].[68]

---

[63] SOU 2007:22 del I, s. 52.
[64] Naarttijärvi, s. 209f, 217, *se även* s. 40, 43-66.
[65] *Se* avsnitt 4.4 för begreppsförklaring.
[66] Prop. 2011/12:55, s. 54f; Naarttijärvi, s. 192-196.
[67] Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG, OJ L 105, 13.04.2006.
[68] *Se* exempelvis Europaparlamentets och rådet förordning 2016/679/EU av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG, OJ L 119, 04.05.2016.

Även om det inte finns en enhetlig definition för vad som avses med personlig integritet eller vad som utgör en inskränkning i denna finns det vissa typer av handlingar som anses utgöra en sådan inskränkning. Rätten till skydd för den personliga integriteten har diskuterats i lagstiftningssammanhang långt innan den grundlagsstadgades. I flera lagförarbeten hänvisar utredare till Tvångsmedelskommitténs och Stig Strömholms försök till att definiera begreppet.[69] Strömholm identifierade tre kategorier av inskränkningar i den personliga integriteten med därtill underliggande kränkande handlingar. Dessa kategorier utgörs av intrång i individens privata sfär (fysiska eller andra), insamlande av uppgifter om individens privata förhållanden och offentliggörande eller annat utnyttjande av material om individens privata förhållanden.[70] Tvångsmedelskommittén delade upp integritet i kategorierna den rumsliga, materiella, kroppsliga, personliga i fysisk mening och personliga i ideell mening. Kommittén ansåg att ett tvångsmedel som används mot en person alltid innebär ett ingrepp i någon av dessa slag av integritet.[71]

Skyddet för den personliga integriteten har därutöver granskats vid en översyn av regeringsformen. Regeringen anförde att kränkningar av den personliga integriteten utgör ”intrång i den fredade sfären som den enskilde bör vara tillförsäkrad och där intrång bör kunna avvisas.”[72] Integritetsskyddskommittén sammanfattade det som att den enskilde har ett intresse av att skydda information om sina personliga förhållanden. Behovet av att förankra skyddet för den personliga integriteten i grundlagen motiverades med behovet av att stärka individens rätt att själv bestämma över information som rör hens personliga förhållanden. Med detta avses information som kan knytas till den enskildes person.[73] Skyddet i grundlagen ska säkerställa att enskilda har rätt att inte vara föremål för kartläggning eller övervakning. Som exempel ges polisens insamling av information genom användning av olika tvångsmedel.[74]

Åsikterna kring huruvida övervakning av enskilda individer utgör en integritetskränkning skiljer sig åt. Ett gammalt argument som förekommer än idag i den digitala miljön är ’har du inget att dölja behöver du inte oroa dig för övervakning’. Enligt Abrahamsson är argumentet oförenligt med både svensk grundlag och EKMR eftersom utgångspunkten är att var och en är tillförsäkrad skydd för privatliv oavsett om man har något att dölja eller inte.[75] Enligt Ulväng utgör lagring av information, såsom registrering av samtals- och e-posttrafik,

[69] *Se* exempelvis SOU 2007:22 del I, s. 55-58, 60-61; prop. 2005/06:173, s. 14; prop. 2009/10:80, s. 175.
[70] Strömholm, s. 698f.
[71] SOU 1984:54 s. 42.
[72] Prop. 2009/10:80, s. 175.
[73] Ibid, s. 175-177.
[74] Ibid, s. 180f.
[75] Abrahamsson, 2009 s. 421, 424; *jmf.* Naarttijärvi, s. 238.

inte i sig en integritetskränkning. Det är vad som händer med informationen, vem som har tillgång till den och syftet med insamlingen som kan medföra en sådan kränkning. Ulväng menar att man ska tala om risker för en integritetskränkning, det vill säga risken för spridning, otillbörligt utnyttjande, missbruk med mera.[76] Som presenterats ovan har Europadomstolen gått längre än Ulväng. Enligt domstolen utgör inhämtning och lagring av sådana uppgifter om den enskilde ett intrång i privatlivet i strid med artikel 8 EKMR oavsett om eller hur dessa uppgifter kan komma att användas mot den enskilde.[77] Naarttijärvi framför att argumentet ’inget att dölja’ utgår från en priviligierad utgångspunkt tillhörande en etnisk, kulturell, religiös eller politisk majoritet. Uppoffringen av en rättighet anses befogad för att det i verkligheten oftast är någon annans rättigheter som offras för den egna säkerheten. Dessutom bygger argumentet på uppfattningen att myndighetspersonal som hämtar in och behandlar uppgifterna aldrig begår misstag. Det tredje argumentet som Naarttijärvi framför är att uppgifter som verkar harmlösa idag kan ha en annan effekt imorgon vilket exemplifieras av historien om bland annat judeförföljelsen under andra världskriget.[78]

Med utgångspunkt i det ovan sagda kan begreppet sammanfattas som en rätt för den enskilde till en privat sfär som är skyddat från fysiska och psykiska intrång. I denna uppsats kommer begreppet personlig integritet användas i ideell bemärkelse.[79] Här avses därmed inte fysisk eller kroppslig integritet utan främst insamling och utnyttjande av immateriell information om den enskilde och dennes personliga förhållanden utan dennes samtycke.

2.4 Effektvitet

Begreppet effektivitet har, i likhet med de intressen som nämnts ovan, en relativ innebörd och måste sättas i relation till något. Enligt Ulväng kan effektivitet förstås genom att sättas i relation till ett mål eller ett medel. Målet kan vara brottsprevention, fler fällande domar eller ökad handläggning. Målsättningen kan senare motiveras med att lagstiftaren vidtar olika åtgärder för att öka effektiviteten. Som medel kan effektivitet ses som en möjlighet att utreda brott, exempelvis genom införande av nya tvångsmedel. Effektiviteten mäts här utifrån kostnads- och arbetsbesparande kriterier. Effektivitet som diskuteras i relation till brottsbekämpning kan hamna i konflikt med intressen såsom integritet och rättssäkerhet.[80]

[76] Ulväng, 2007 s. 1, 12f.
[77] Naarttijärvi, s. 196f.
[78] Ibid, s. 240f.
[79] *Jmf.* SOU 2007:22 del I, s. 63.
[80] Ulväng, 2007 s. 1, 8f.

Utöver effektivitet i den nationella brottsbekämpningen har Sverige internationella åtaganden som måste beaktas. Av EKMR och EU:s rättighetsstadga följer att var och en som vistas i Sverige har rätt att göra anspråk på att staten vidtar effektiva åtgärder för att tillvarata individens säkerhet. Staten har en skyldighet att skapa och upprätthålla ett tillräckligt rättsligt skydd genom att förebygga och utreda brott samt lagföra gärningspersoner. Staten ska skydda individer från intrång i deras privatliv och personliga integritet. Underlåtenhet att upprätthålla ett effektivt rättsligt skydd kan medföra statligt ansvar för brott mot EKMR. En förutsättning för välfungerande brottsbekämpning är effektiva utredningsåtgärder i den fysiska såväl som i den digitala miljön.[81] Europadomstolen har i ett fall uttalat att konfidentialitet för elektronisk kommunikation och yttrandefrihet ibland måste få ge vika för att skydda andra legitima intressen såsom brottsbekämpning och skydd för andras fri- och rättigheter. Domstolen anförde att det inte får ställas oproportionerliga krav på lagstiftaren att tillförsäkra vissa rättigheter på bekostnad av andra rättigheter och rättssäkerhetsintresset.[82]

I utredningssammanhang av nya tvångsmedel eller justering av befintliga sådana förs en diskussion avseende dess effektivitet. Diskussionen utgår främst från redovisning av brottsbekämpande myndigheters användning och betydelse av tvångsmedel i specifika fall vilket enligt Flyghed är ett vagt kriterium och enligt Ramberg ofta dåligt underbyggt.[83] Därutöver menar Ramberg att intresseavvägningen kan utfalla olika vid olika tidpunkter med hänsyn till bland annat befintliga behov.[84]

Enligt Ramberg hävdar vissa att det största integritetsintrånget är att utsättas för brott och att staten har en absolut skyldighet att tillförsäkra skydd för individerna att inte bli utsatta för brott.[85] Detta exemplifieras av uttalanden i delbetänkandet från Beredningen för rättsväsendets utveckling (BRU). Enligt BRU är den integritetskränkning som tvångsmedel kan medföra blygsam i jämförelse med den kränkning som ett brottsoffer utsätts för. I utredningen anfördes att desto mer svårutredd brottsligheten blir, desto mer omfattande tvångsåtgärder bör tillåtas.[86] Ramberg anser att låg brottslighet inte per automatik innebär ett samhälle som är önskvärd att leva i vilket exemplifieras med det tyska östblocket under andra världskriget. Det pris det kostar att bo i ett sådant samhälle motsvarar inte värdet av att brottsligheten är låg. En rättsstats uppgift är i stället att med hänsyn till mänskliga rättigheter förhindra, lösa och beivra brott och garantera invånarna skydd mot övergrepp och kriminalitet. Om

[81] Prop. 2018/19:86, s. 27f.
[82] K.U. mot Finland, p. 48-49.
[83] Flyghed, 2007, s. 62; Ramberg, s. 156f.
[84] Ramberg, s. 155; *jmf.* Flyghed, 2007, s. 64.
[85] Ramberg, s. 169f.
[86] SOU 2005:38, s. 135.

brottsbekämpningsintresset tillåts väga för tungt kommer effektiviteten att bli hög på bekostnad av grundläggande mänskliga rättigheter.[87]

Enligt Ekelöf kan otydlig reglering tillämpas olika i olika situationer vilket främjar effektiviteten eftersom polisen kan agera mer fritt. Konsekvensen av detta är dock oförutsebar rättstillämpning vilket utgör ett hot mot rättssäkerheten. Det faktum att tvångsmedel används i större utsträckning idag och intresset att bekämpa brott tillmäts större vikt på bekostnad av enskildas integritet behöver inte innebära att Sverige har blivit ett mindre rättssäkert land. Frågan huruvida regleringen är rättssäker beror istället på hur tvångsmedlen regleras och tillämpas.[88]

I denna uppsats används begreppet effektivitet i relation till målet att genomföra bättre utredningar av sexualbrott mot barn via internet. Med bättre utredningar avses bättre förutsättningar att säkra digital bevisning i syfte att fler tips och anmälningar ska leda till förundersökning och därefter till åtal. Denna målsättning ska uppnås genom införande av effektiva utredningsåtgärder i brottsbekämpningssammanhang. Uppsatsen ska i detta sammanhang ta ställning till befintliga utredningsåtgärders effektivitet vid framtagning av digital bevisning i relation till det integritetsintrång som åtgärderna medför.

[87] Ramberg, s. 169f; *jmf.* Jareborg, 1992, s. 92.
[88] Ekelöf, 2018, s. 42f.

3 Sexualbrott mot barn via internet

3.1 Inledning

En av samhällets främsta uppgifter är att skydda barn mot sexuella övergrepp. Att utsätta ett barn för ett sexuellt övergrepp är ett stort ingrepp i barnets integritet och kan medföra förödande fysiska samt psykiska konsekvenser för barnet.[89] Teknikutvecklingen och internetanvändningen har lett till att gärningspersoner på enklare sätt kan utnyttja barn sexuellt, utan att ett fysiskt möte kommit till stånd. Med några få knapptryckningar kan gärningspersonen nå ett stort antal barn, inte sällan genom att utge sig för att vara en annan person. Därutöver möjliggör internetutvecklingen obegränsad rörlighet av barnpornografiskt material. Effektiv brottsbekämpning av sådana brott förutsätter ett gott nationellt och internationellt straffrättsligt skydd.[90]

Det är inte möjligt att ur lagens ordalydelse utläsa om sexuella övergrepp mot barn som begås på distans är kriminaliserade. Detta avsnitt avser att kort presentera de sexualbrott mot barn som gärningspersonen kan dömas för och därtill hörande straffskalorna. Därefter beskrivs utvecklingen av den gällande rätten till att omfatta handlingar som genomförs på distans.

3.2 De straffbelagda gärningarna

Sexualbrott mot barn regleras i sjätte kapitlet brottsbalken och har omarbetats i flera omgångar i syfte att stärka skyddet för barnen. Skyddet för barn är ovillkorligt vilket innebär att gärningspersonen kan dömas till ansvar oavsett om den sexuella handlingen utförts frivilligt från barnets sida. Svensk sexualbrottslagstiftning bygger på synsättet att barn under femton år saknar självbestämmanderätt i sexuella sammanhang vilket innebär att barn under femton år har ett absolut skydd mot sexuella övergrepp.[91]

Den som genomför samlag med barn under femton år eller annan sexuell handling som med hänsyn till kränkningens allvar är jämförlig med samlag, döms enligt 6 kap. 4 § första stycket BrB för våldtäkt mot barn till fängelse i lägst två och högt sex år. Våldtäktsbestämmelsen omfattar vaginala, orala och anala samlag. Därutöver omfattas handlingar som att stoppa fingrar eller

[89] Prop. 1994/95:2, s. 8.
[90] Ds 2007:13, s. 21f; prop. 2004/05:45, s. 94f.
[91] Prop. 1994/95:2, s. 9; prop. 2004/05:45, s. 21f, 67.

föremål i barnets underliv eller anus.[92] Det avgörande vid bedömningen om en sexuell handling är jämförbar med samlag är kränkningen som följer av handlingen, det vill säga huruvida kränkningen är lika allvarlig som den kränkning som följer av ett påtvingat samlag.[93] Sedan omarbetningen av sjätte kapitlet brottsbalken år 2005 ställs inte längre något krav på att den sexuella handlingen ska innefatta fysisk och varaktig kroppslig beröring för att den ska kunna bedömas som en sexuell handling. Det avgörande är huruvida handlingen haft en påtaglig sexuell prägel samt varit ägnad att tydligt kränka barnets sexuella integritet.[94]

Våldtäktsbestämmelsen är avsedd att omfatta de mest allvarliga sexualbrotten. Om våldtäkten med hänsyn till omständigheterna är att anse som mindre allvarlig kan gärningspersonen istället dömas för sexuellt utnyttjande av barn till fängelse i högst fyra år enligt 6 kap. 5 § BrB. Bestämmelsen ska dock användas restriktivt och omfattar situationer när en person har samlag med ett barn som är strax under femton år som bygger på frivillighet och ömsesidighet.[95] Om gärningspersonen genomför en annan sexuell handling, som inte är tillräckligt kvalificerad än vad som avses i 4-5 §§, ska hen enligt 6 kap. 6 § första stycket BrB dömas för sexuellt övergrepp mot barn till fängelse i högst två år. Det avgörande för brottets rubricering är arten och graden av den kränkning som barnet utsätts för och inte handlingens tekniska karaktär. Som exempel anges då gärningspersonen förmår barnet att onanera på sig själv.[96] Enligt lagförarbeten bör utgångspunkten vara att det alltid medför en kränkning att utsätta ett barn för alla former av sexuella handlingar.[97]

Därutöver kan gärningspersonen enligt 6 kap. 8 § BrB dömas för utnyttjande av barn för sexuell posering till böter eller fängelse i högst två år om hen främjar eller utnyttjar barnet för sådan posering. Bestämmelsen innefattar ett absolut skydd för barn under femton år att medverka i posering och avser att skydda barn från utnyttjanden för framställning av pornografiskt material.[98] Detta gäller även posering genom exempelvis en webbkamera.[99] Samtidigt kan gärningspersonen enligt 16 kap. 10a § BrB dömas för barnpornografibrott till fängelse i högst två år. Poserings- och barnpornografibrotten har olika skyddsintressen, därmed kan gärningspersonen dömas för utnyttjande av barn för sexuell posering och barnpornografibrott i konkurrens.[100] Barnpornografiskt material kan skildra sexuella övergrepp mot barn enligt sjätte kapitel

[92] Prop. 2004/05:45, s. 33f, 136.
[93] Ibid, s. 36, 46.
[94] Ibid, 32-34.
[95] Ibid, s. 76f.
[96] Ibid, s. 79f.
[97] Ibid, s. 22.
[98] Ibid, s. 98f.
[99] *Jmf.* hovrättens dom i mål nr. B 1293-17 och B 5801-15.
[100] Prop. 2004/05:45, s. 147.

brottsbalken men barnpornografibrottet kriminaliserar handlingar utöver det sexuella övergreppet.[101] För barnpornografibrott döms den som har befattning med material som skildrar barn i pornografisk bild. All befattning med sådant material, från framställning till spridning, är kriminaliserat.[102] Bestämmelsen har dock en annan definition av barn än brottsbalkens sjätte kapitel. Barn definieras som en person under arton år eller en person vars pubertetsutveckling inte är fullbordad.[103]

Gärningspersonen kan enligt 6 kap. 9 BrB även dömas för köp av sexuell handling av barn till böter eller fängelse i högst två år. Bestämmelsen avser främst att skydda barn från att dras in i prostitution men avser även andra situationer såsom när en gärningsperson mot ersättning utnyttjar barnet i sexuellt syfte.[104] Den som förmår barnet att företa eller medverka i en handling som till sin karaktär inte är tillräckligt kvalificerad för att betraktas som sexuell handling men har en sexuell innebörd döms enligt 6 kap. 10 § BrB för sexuellt ofredande till böter eller fängelse i högst två år. Detsamma gäller den som blottar sig för barnet på ett sätt som är ägnat att väcka obehag eller annars genom ord eller handlingar ofredar barnet på ett sätt som är ägnat att kränka dess sexuella integritet. Bestämmelsen omfattar även sexuella kontakter på distans.[105] Att skicka oönskade nakenbilder på sitt könsorgan till en person är ett exempel på sexuellt ofredande.[106]

I flera fall föregås sexualbrotten av en process där gärningspersonen försöker vinna barnets förtroende i syfte att vid ett senare tillfälle utnyttja barnet sexuellt. Denna process betecknas som grooming och är enligt 6 kap. 10a § BrB kriminaliserat som kontakt för att träffa ett barn i sexuellt syfte. Processen utgör ett förstadium till sexualbrott och går ut på att skapa en kontakt med barnet i syfte att ”förbereda” barnet för såväl fysiska som digitala sexuella övergrepp.[107] De medel som gärningspersonen använder sig av är bland annat smicker, uppskattning, tröst, förståelse och presenter. Grooming är en manipulations-process som bryter ner barnets motstånd och skapar situationer där sexuella övergrepp kan begås, samtidigt som distans mellan barnet och föräldrarna skapas och risken för att barnet berättar minskar.[108] Groomingbrottet är ett resultat av den tekniska utvecklingen och dess konsekvenser för barns utsatthet för sexualbrott via internet.[109]

---

[101] Prop. 1997/98:43, s. 77.
[102] 16 kap. 10a § BrB.
[103] Prop. 1997/98:43, s. 161, se s. 81-87 avseende lagstiftarens motivering angående pubertetsutveckling som åldersrekvisit.
[104] Prop. 2004/05:45, s. 92.
[105] Ibid, s. 149.
[106] Hovrättens dom i mål nr. B 4763-14, s. 3.
[107] Prop. 2008/09:149, s. 16; Davidson & Gottchalk, s. 10; *jmf.* Ds 2007:13, s. 31f.
[108] Shannon, s. 22; Ds 2007:13, s. 32.
[109] Prop. 2008/09:149, s. 5f.

Gärningspersonen ska enligt 6 kap 14 § BrB inte dömas till ansvar om åldersskillnaden mellan hen och barnet är ringa, det är uppenbart att något övergrepp mot barnet inte skett och det inte förekommit tvångs- eller våldsinslag. Bestämmelsen träffar situationer där sexuellt umgänge mellan två tonåringar förekommit och skillnaden i ålder och mognadsutvecklingen mellan dem är obetydlig samt omständigheterna i övrigt, såsom deras relation till varandra, inte talar för en annan slutsats. Bestämmelsen innebär en möjlighet för åklagaren att underlåta att väcka åtal och möjliggör för domstolen att ogilla åtalet på den grunden att gärningen inte bör föranleda ansvar i det fall åklagaren väckt åtal. Den ska tillämpas med stor försiktighet.[110]

Bestämmelserna om våldtäkt mot barn, sexuellt övergrepp mot barn, utnyttjande av barn för sexuell posering samt barnpornografi föreskriver även straffansvar för grovt brott och medför strängare straffskalor. Samtliga brott förutom sexuellt ofredande och kontakt för att träffa ett barn i sexuellt syfte är kriminaliserade på försöksstadiet.[111]

3.3 Utvecklingen i praxis

Sexualbrott har tidigare betraktats vara egenhändiga brott, det vill säga att det för fällande dom krävdes att gärningspersonen själv utfört den straffbelagda sexuella handlingen. Genom omarbetning av bestämmelserna och dess tolkning i domstol har detta tankesätt övergetts.[112] I NJA 2015 s. 501 prövades frågan om en gärningsperson kunde dömas till ansvar genom att förmå ett barn att utföra sexuella handlingar på sig själv via internet. Gärningspersonen hade genom Skype förmått två målsäganden under femton år att visa sig nakna inför hen. Målsäganden B förmåddes även, under hot om spridning av nakenbilder på henne, smeka sig över bröstet och onanera inför gärningspersonen samtidigt som gärningspersonen onanerat inför målsäganden. En av de rättsliga frågorna som försökte klargöras genom instanserna var huruvida den sexuella handlingen via Skype skulle rubriceras som sexuellt övergrepp mot barn eller som utnyttjande av barn för sexuell posering.[113]

HD framförde att utgångspunkten i lagförarbetena numera är att det inte krävs någon varaktig fysisk beröring för att en handling ska kvalificeras som en sexuell handling. Omarbetningen av sjätte kapitlet brottsbalken innebär en utökning av det straffbara handlandet som innefattas i rekvisitet sexuell handling. Domstolen var kritisk mot terminologin som användes i sjätte kapitlet vid tidpunkten för brottet. I vissa bestämmelser angavs uttrycket ”förmår en

[110] Prop. 2004/05:45, s. 115f, 152.
[111] 6 kap. 15 §; 16 kap. 17 § BrB.
[112] SOU 2016:60, s. 228-236; SOU 2010:71, s. 192-195.
[113] NJA 2015 s. 501.

person…” medan i andra, däribland bestämmelsen om sexuella övergrepp mot barn, angavs ”genomför en sexuell handling med”. Domstolen ansåg att det av lagmotiven inte gick att utläsa i vad mån de olika formuleringarna innebar en skillnad avseende det straffbara handlandet. Ett exempel på sexuell handling är enligt lagförarbetena att en person förmår barnet att onanera på sig själv. HD anförde att det genom lagmotiven stod klart att sådant agerande – att förmå ett barn att genomföra sexuella handlingar på sig själv – ska innefattas i rekvisitet sexuell handling och därmed omfattas av 6 kap. 6 § BrB.[114] Trots vissa terminologiska brister ansåg domstolen att den aktuella gärningen ”får anses vara omfattad av det normala betydelseområdet för uttrycket att genomföra en sexuell handling med en annan person”[115] och därmed inte i strid med legalitetsprincipen.[116] Domstolen ansåg därmed att gärningspersonens agerande innefattade ett straffbart handlande enligt 6 kap. 6 § BrB.

Sexualbrottskommittén fick år 2014 i uppgift att se över huruvida lagstiftningen tillförsäkrade barn ett tillräckligt skydd i den digitala miljön. Domen i NJA 2015 s. 501 hann falla innan kommitténs betänkande hade redovisats. Trots utfallet i avgörandet ansåg kommittén att det fortfarande fanns behov av att i lagstiftningen tydliggöra vilka brott som kunde begås på distans eftersom HD endast hade prövat tillämpningsområdet av bestämmelsen sexuellt övergrepp mot barn.[117] Regeringen var dock av annan uppfattning och ansåg att HD:s uttalande klargjorde frågan huruvida gärningsmannaskap vid sexualbrott kräver fysisk delaktighet. Regeringen ansåg att det till följd av domen inte förelåg behov av att i lagtext införa att bestämmelserna om våldtäkt mot barn, sexuellt utnyttjande samt sexuellt övergrepp mot barn innefattar sexuella handlingar som sker på distans. I syfte att uppnå enhetlighet i språkligt hänseende ändrades samtliga bestämmelser till att innehålla rekvisitet ”genomför en sexuell handling med”.[118] Bestämmelsernas tillämplighet på övergrepp som begås via internet är därmed numera fastställt i lagförarbetena.

I ett senare refererat hovrättsavgörande dömdes en gärningsperson till våldtäkt mot barn som begåtts via internet. Gärningen bestod i att gärningspersonen, via chatt, förmått målsägande A att utföra oralsex på målsägande B. Målsägande A filmade handlingen och skickade denna till gärningspersonen som sparade filmen. Både målsägandena var tolv år gamla. Med hänsyn till att gärningspersonen genom hot och tjat förmått målsägandena utföra de sexuella handlingarna, att dessa varit förnedrande och förödmjukande för målsäganden A, att gärningspersonen via internet aktivt dirigerat hur den sexuella handlingen

[114] Ibid, skäl 2-6.
[115] Ibid, skäl 9.
[116] Ibid.
[117] SOU 2016:60, s. 234.
[118] Prop. 2017/18:177, s. 43f.

skulle genomföras och handlingen pågått under en längre tid dömdes gärningspersonen för våldtäkt mot barn.[119]

I NJA 2018 s. 1103 prövades huruvida ett sexuellt övergrepp som i de olika delarna begåtts vid olika tidpunkter omfattades av bestämmelsen sexuellt övergrepp mot barn. Gärningspersonen hade förmått ett barn att onanera i ensamhet, filma detta och sedan skicka filmen till gärningspersonen. Den tidsmässiga uppdelningen innebar att den sexuella handlingen genomförts vid ett annat tillfälle än när gärningspersonen tagit del av handlingen, det vill säga inte *inför* gärningspersonen. Med utgångspunkt i legalitetsprincipen ansåg HD att bestämmelsens ordalydelse innefattar ett krav på att gärningspersonen måste vara närvarande under den del av händelseförloppet som innefattar den sexuella handlingen. Ett sådant handlande som var aktuellt i detta fallet innebar inte att gärningspersonen *genomfört* en sexuell handling med barnet.[120]

3.4 Husbymålet

Det finns ett antal uppmärksammade mål om sexuella övergrepp mot barn via internet, däribland kan nämnas Alexandra-, Kumla- och Husbymålen. Nedan kommer Husbymålet som är ett av de första och mest omfattande sexualbrottmålen mot barn via internet att presenterats för att ge läsaren insyn i omfattningen och vikten av digital bevisning i sådana mål.

I Husbymålet inledde gärningspersonen kontakt med ett sextiotal olika målsäganden genom nätforumet Kamrat som sedan övergick till andra kommunikationsprogram. Där övertalades och hotades målsägandena till att posera och genomföra sexuella handlingar på sig själva i webbkamera vilket dokumenterades av gärningspersonen.[121] De handlingar som målsägandena utsattes för kunde även utläsas av chattarna som upphittades i målsägandenas datorer och mobiltelefoner.[122]

De första anmälningarna i fallet inkom 2012 som polisen genom IP-spårning kunde knyta till en misstänkt person. Vid ett förhör påtalades för den misstänkta att hen blivit identifierad genom IP-spårning. Den misstänkta nekade och i brist på bevisning lades utredningen ned. Som en konsekvens av detta installerade personen säkerhetsprogram på sin dator som gjorde att det var omöjlig att spåra datorn.[123] År 2013 inkom ytterligare anmälningar från flickor i tolv till arton års åldern som utsatts för grova sexuella övergrepp på internet. Utredningen utgick

[119] RH 2018:6.
[120] NJA 2018 s. 1103, skäl 14-18.
[121] Tingsrättens dom i mål nr. B 8098-13, s. 18
[122] P3, 2019.
[123] Mål nr. B 8098-13, s. 18; P3, 2019.

från en användarlista som Kamrat hade sammanställt med registrerade användarnamn som kunde knytas till en och samma person. Genom användning av samma lösenord, IP-adress samt köp på forumet genom samma mobil och kontantkort hittades ett samband mellan kontona som kunde kopplas till en misstänkt person. Utredningen ledde till en husrannsakan och efterföljande beslag av datorer, mobiltelefoner med mera hos gärningspersonen.[124]

Gärningspersonen hade stor IT-kompetens och använde sig av både anonymiseringstjänster och kryptering[125]. Vid tidpunkten för husrannsakan var en av datorerna påslagen men inte inloggad. Teknikerna gjorde en spegelkopia av datorn som sedan tjänade som viktig stödbevisning. Då gärningspersonen vägrade samarbeta genom utlämning av lösenord medförde krypteringen svårigheter att ta del av innehållet i datorn. Viss material kunde dock säkras. Mappar med flicknamn och miniatyrbilder på dessa, en film som visade hur en flicka hotats och förnedrats under två timmar i webbkamera samt sökningar på flickors adresser och Facebook-konton påträffades.[126]

Tingsrätten och hovrätten ansåg att det gick att knyta en och samma gärningsperson till de olika gärningarna genom den tekniska bevisningen. Delvis fanns en mängd fynd i gärningspersonens dator med kopplingar till målsäganden men även kopplingar mellan olika e-postadresser och konton på Kamrat, Skype, Kik och Facebook som gärningspersonen använt sig av samt köp som kunde knytas till gärningspersonen.[127] Gärningspersonen dömdes för diverse sexualbrott mot barn till sju år och nio månaders fängelse.[128]

[124] Ibid, s. 18-20.
[125] Kryptering går ut på att omvandla läsbar data till icke-läsbar data, så kallad kryptotext, med hjälp av en nyckel. Texten kan endast göras läsbar genom dekryptering som kräver nyckeln. *Se* SOU 2017:89, s. 160f.
[126] P3, 2019.
[127] Mål nr. B 8098-13, s. 30-53; hovrättens dom i mål nr. B 5801-15, s. 40-42.
[128] Mål nr. B 5801-15, s. 92f.

4 Tillgång till digital bevisning

4.1 Inledning

Brottsbekämpande myndigheter kan inhämta digital bevisning på olika sätt och vid olika tidpunkter. Avsnittet avser att kartlägga olika rättsliga möjligheter för polisen att inhämta digital bevisning som hänför sig till elektronisk kommunikation. Vidare presenteras lagstiftarens diskussioner och avvägningar mellan effektiv brottsbekämpning och personlig integritet vid reglering av de olika möjligheterna till inhämtning av digital bevisning.

4.2 Allmänt om bevisning i sexualbrottmål

Svensk bevisrätt bygger på principen om fri bevisföring vilket innebär att alla bevismedel av relevans är tillåtna.[129] Sexualbrottmål i allmänhet grundar sig oftast på uppgifter från målsäganden vars utsaga utgör huvudbevisning i rättegången. Utsagan tillmäts beviskraft i förhållande till målsägandens tillförlitlighet men i ord-mot-ord-situationer krävs någon form av stödbevisning.[130] Sexualbrottmål avseende barn är förenade med ytterligare svårigheter ur bevissynpunkt. Barn hörs oftast inte inför domstol utan deras utsaga åberopas som bevisning genom uppspelning av barnförhör under förundersökningen.[131] Enligt Sutorius kan HD:s praxis tolkas som att video-förhör ska tillmätas lägre bevisvärde till skillnad från domstolsförhör och att det därmed krävs mer stödbevisning än vanligt.[132] Stödbevisning förekommer alltid i någon form i övergreppsmål men styrkan i bevisningen varierar.[133]

I föregående avsnitt exemplifierades hur digital bevisning kan användas i utredningar och efterföljande rättegångsprocesser vid sexualbrott mot barn.[134] Enligt Larsson utgör digital bevisning ett komplement till en målsägandeutsaga genom att antingen styrka eller förkasta utsagan.[135] Digital bevisning som bevismedel är inte helt oproblematisk. En riskfaktor med att presentera digital bevisning är att den lättare kan manipuleras och därmed svårare för domstolen att fastställa dess äkthet. Det kan till följd därav krävas mer information om den digitala bevisningen (metadata[136]) än innehållet i informationen vilket kan

[129] 35 kap. 1 § RB.
[130] Leijonhufvud, s. 41.
[131] Sutorius, s. 163-165.
[132] Ibid, s. 177, 182-183; NJA 1993 s. 616.
[133] Sutorius, s. 294, 333-336.
[134] *Se* avsnitt 3.4.
[135] Larsson, telefonintervju.
[136] *Se* avsnitt 1.5.2.

utgöras av information om avsändare, tidsstämplar och lokaliseringsuppgifter. Av sådan kringliggande information kan framgå huruvida den datalagrade informationen har ändrats i förhållande till dess ursprungliga form vilket har betydelse vid bevisvärderingen i rättegången.[137]

4.3 Från tips till förundersökning

Polisen får kännedom om sexuella övergrepp mot barn på flera olika sätt. Ett stort antal av tipsen kommer från NCMEC. Organisationen får in rapporter om misstänkta barnpornografibrott från amerikanska leverantörer av elektroniska tjänster, undersöker materialet och skickar tipset till det land som IP-adressen spåras till. Larsson beskriver att materialet inledningsvis undersöks för att se om det är olagligt i Sverige. Om så inte är fallet läggs undersökningen ner. När det går att fastställa att materialet är olagligt skrivs en anmälan genom vilken en förundersökning inleds.[138]

Syftet med en förundersökning är att utreda ett misstänkt brott, vem gärningspersonen är samt säkra bevisning. Syftet är även att fria misstänkta personer från misstanke.[139] Förundersökningen utgör underlag för åklagarens åtalsbeslut och bereder målet för framställning i huvudförhandling. Förundersökningsprocessen regleras av principer för att säkerställa att den genomförs på rätt sätt och inte inskränker brottsoffrets integritet eller medför grundlösa frihetsberövanden av misstänkta.[140] Under förundersökningen kan även vissa tvångsmedel företas i syfte att eftersöka information som kan vara av betydelse för utredningen.[141] För tvångsmedelsanvändning krävs normalt att någon skäligen kan misstänkas för ett brott men vissa åtgärder kan även företas när så inte är fallet vilket kommer presenteras nedan.[142]

4.4 Terminologi

Nedan kommer en mer djupgående presentation ske av elektronisk information som kan tjäna som digital bevisning. På detta område förekommer en del tekniska termer. I syfte att undvika otydligheter och begreppsförvirring ska de mest etablerade och viktiga termerna förklaras.

[137] Ekelöf, 2009, s. 255-258; *se* även Kronqvist, s. 120-122.
[138] Larsson, telefonintervju.
[139] 23 kap. 1-2 § RB; Larsson, telefonintervju; *jmf.* Sutorius, s. 204.
[140] Bring m.fl., s. 63-68; Sutorius, s. 205f.
[141] 23 kap. 16 § RB.
[142] *Jmf.* 24 kap. 1 §, 25 kap. 1 §, 26 kap. 1 §, 27 kap. 20 §, 28 kap. 1 § RB; *se* avsnitt 4.5.2-4.5.3, 4.6.2, 4.7.

På teleområdet finns en gemensam terminologi för olika typer av information. *Trafikuppgifter* utgörs av information om skickade och mottagna meddelanden som förs över eller har förts över till och från en viss adress. Uppgifterna innefattar information om var meddelandet kommer ifrån och vart det ska skickas, datum och tid för kommunikationen, meddelandets storlek och varaktighet. Med *adress* avses den icke fysiska adressen som ett meddelande skickas till eller från. Exempel på icke fysiska adresser är abonnemangsuppgifter, telefonnummer, e-postadress, IP-adress eller någon annan identifieringsmetod.[143] Med *meddelanden* avses information som överförs eller har överförts till eller från en adress mellan ett begränsat antal parter i ett elektroniskt kommunikationsnät. Meddelanden innefattar ljud, text, bild eller data som överförs genom bland annat telefoni, datorkommunikation, elektronisk post och annan elektronisk kommunikationsutrustning.[144]

Med *abonnemangsuppgifter* avses uppgifter som identifierar en abonnent, exempelvis abonnentens nummer, namn, adress och titel. Uppgifter om typ av abonnemang, avtal, fakturering och vissa tekniska uppgifter om utrustningen räknas också in i abonnemangsuppgifter. Utredningen om datalagring och EU-rätten ifrågasatte huruvida vissa i lagförarbetena angivna uppgifter skulle räknas som abonnemangsuppgifter. Utredningen ansåg att definieringen borde göras utifrån syftet med uppgifterna och inte dess tekniska karaktär. Trots detta ingår de omdiskuterade uppgifterna IMSI-nummer[145] och IP-adress i begreppet abonnemangsuppgifter.[146]

En *IP-adress* består av en tolvsiffrig nummerkombination som är uppdelat i olika segment. IP-adressen är nödvändig för att informationen som skickas över internet ska hitta fram. Det finns fasta och dynamiska IP-adresser. De fasta innebär att det alltid är samma nummerserie som skickar och mottar meddelanden på internet. De dynamiska IP-adresserna innebär att varje meddelande som skickas tilldelas ett för tillfället unik IP-adress som sedan kan återanvändas för ett annat meddelande. Det är därmed lättare att identifiera en avsändare eller mottagare som har en fast IP-adress. För att identifiera en person som har en dynamisk IP-adress måste adressen knytas till en tidsstämpel och ett skickat meddelandet. Denna koppling kan endast göras med hjälp av operatören eller internetleverantören som tillhandahåller telenätet. Anonymiseringstjänster kan användas i syfte att dölja sin identitet och aktivitet på internet.[147]

[143] SOU 2005:38, s. 164f.
[144] 27 kap. 18-19 §§ RB; prop. 2011/12:55, s. 58f; *jmf.* SOU 2005:38, s. 154-157.
[145] International Mobile Subscriber Identity är ett nummer som är kopplat till abonnentens SIM-kort och därmed telefonnummer.
[146] Prop. 2018/19:86, s. 93; SOU 2017:75, s. 98; *se* avsnitt 4.6.2.
[147] Prop. 2018/19:86, s. 93; Kronqvist, s. 72-74.

Lokaliseringsuppgifter utgörs av information om platsen för en viss elektronisk kommunikationsutrustning eller tvärt om av information avseende vilka elektroniska kommunikationsutrustningar som har funnits i ett visst geografiskt område vid en given tidpunkt.[148]

4.5 Straffprocessuella tvångsmedel

4.5.1 Inledning

Tvångsmedel kan endast användas under en pågående förundersökning, i annat fall anses förundersökningen inledd genom tillgripande av tvångsmedel.[149] Undantag från denna regel gäller användning av tvångsmedel i underrättelseverksamhet. Med tvångsmedel avses ”direkta ingripanden mot person eller egendom som företas i myndighetsutövning och som utgör någon form av intrång i en persons rättssfär”.[150] Därutöver ska åtgärden syfta till att åstadkomma ett konkret resultat och medföra synbara och kännbara verkningar för den enskilde. Användning av tvångsmedel behöver inte innefatta inslag av tvång utan det som kännetecknar en sådan åtgärd är att den mot vilken åtgärden företas skulle motsätta sig åtgärden om hen kände till den. Hemlig avlyssning och hemlig övervakning av elektronisk kommunikation är exempel på detta.[151]

Användning av tvångsmedel är den mest ingripande åtgärden som det allmänna rätteligen kan företa mot den enskilda. Avvägningen mellan bakomliggande rättsliga intressen, effektiv brottsbekämpning och personlig integritet, görs främst av lagstiftaren vid införande av nya tvångsmedel men även av rättstillämparen som ska förhålla sig till olika principer vid beslut om tvångsmedelsanvändning.[152] Förutom legalitetsprincipen ska lagstiftaren och rättstillämparen ta hänsyn till tre allmänna principer. Tvångsmedel får endast införas och användas för att uppnå det ändamål för vilket tvångsmedlet har beslutats för (ändamålsprincipen). Vidare får tvångsmedlet endast införas och användas om det föreligger ett påtagligt behov och om det avsedda resultatet inte kan uppnås med andra, mindre ingripande medel (behovsprincipen). Slutligen ska tvångsmedlet och den kränkning som det medför för den enskilda stå i rimlig proportion till det önskade målet (proportionalitetsprincipen). Tvångsmedlet får därmed endast användas om skälen för åtgärden uppväger den skada som åtgärden innebär för den misstänkta eller för något annat intresse.[153] Konflikter mellan rättsliga intressen såsom personlig integritet och effektivitet löses genom användning av, enligt Naarttijärvi, en bredare definition av

[148] SOU 2009:1, s. 61.
[149] 23 kap. 16 § RB; SOU 1995:47, s. 137.
[150] SOU 1995:47, s. 137.
[151] Ibid, s. 137-140; Bring, m.fl., s. 292-295.
[152] Lindberg, 2018, s. 14-17.
[153] 27 kap. 1 § RB; prop. 1988/89:124, s. 26; Bring, m.fl., 285-287.

proportionalitetsprincipen. Enligt Naarttijärvi används proportionalitet som en metod att begränsa eller ogiltigförklara intrång som är för omfattande i förhållande till det syfte som lagstiftaren försöker uppnå genom intrånget. Styrkan med en proportionalitetsbedömning är att ett intrång kan motiveras med tydliga motstående intressen och legitima ändamål. Den breda definitionen av proportionalitet innefatta fyra byggstenar, nämligen legalitet, ändamål, behov och nödvändighet och proportionalitet i strikt mening.[154]

Ramberg är kritisk till lagstiftarens motiveringar avseende behovet, effektiviteten och proportionaliteten av tvångsmedel. Enligt Ramberg överskuggas dessa överväganden av generella och dåligt underbyggda argument och påståenden om ”rent mjöl i påsen” och ”att det bara är grova brottslingar som riskerar att bli utsatta för tvångsmedel”.[155] Bevisbördan för nödvändigheten av tvångsmedel ligger på dem som anför att sådana ska införas och inte på dem som ifrågasätter detta menar hon.[156]

Enligt Qvarnström är användning av straffprocessuella tvångsmedel, inte minst hemliga sådana, en förutsättning för att utreda och lagföra brott. Qvarnströms uppfattning är att tvångsmedlen i främsta hand för utredningen framåt och frambringar bevis om brott. Larsson och Qvarnström, som båda representerar brottsbekämpande myndigheter, menar att integritetsdebatten hamnat snett. Integritetsförespråkare motsätter sig integritetskränkande brottsbekämpnings-åtgärder men har sällan egna förslag på utredningsåtgärder som skulle kunna ersätta tvångsmedlen som är föremål för diskussion.[157]

4.5.2 Husrannsakan och beslag

Bevissäkring under förundersökning sker oftast genom en husrannsakan som gör det möjligt att beslagta fysiska informationsbärare som kan innehålla bevisning. Husrannsakan bereder polisen tillgång till utrymmen som de annars inte skulle ha haft tillgång till i syfte att söka efter egendom (reell husrannsakan) eller person (personell husrannsakan).[158] Undersökningen kan avse såväl fysiska som andra utrymmen. Reglerna om husrannsakan omfattar därmed även undersökning av innehåll i datorer och andra informationsbärare.[159]

Husrannsakan kan endast företas om det finns anledning att anta att ett brott har förövats på vilket fängelse kan följa och tvångsmedlet ämnar söka efter föremål som kan tas i beslag eller i förvar eller annars kan utröna omständigheter som

[154] Naarttijärvi, s. 40, 43-66.
[155] Ramberg, s. 157.
[156] Ibid, s. 156f.
[157] Qvarnström, s. 136f; Larsson, telefonintervju.
[158] Lindberg, 2018, s. 604.
[159] Ibid, s. 621.

kan vara av betydelse för utredningen.[160] Därutöver krävs att den mot vilken husrannsakan företas skäligen kan misstänkas för brottet eller att det föreligger andra kvalificerade omständigheter. Misstankegraden förutsätter att det finns konkreta omständigheter av viss styrka som pekar på att den misstänkta har begått brottet. Den ska grundas på fakta och inte på allmänna utpekanden av en viss person, icke verifierade andrahandsuppgifter eller andra omständigheter som saknar relevans för misstanken. Misstanken ska ha en viss substans och bevisningen som misstanken grundar sig på viss styrka. En husrannsakan kan i vissa fall även företas hos annan än den som skäligen misstänkts för brottet.[161]

Föremål som skäligen kan antas ha betydelse för utredningen om brott, genom att det kan utgöra bevisning eller ge ledtrådar i utredningen, får tas i beslag. Däremot ställs inget krav på brottets svårhetsgrad. Det som sägs om föremål gäller även skriftliga handlingar som inte omfattas av beslagsförbudet[162].[163] Skriftlig handling definieras inte i lag men med hänsyn till den tekniska utvecklingen har det även ansetts omfatta datalagrad information.[164]

Endast lösa, fysiska och tillgängliga föremål kan beslagtas.[165] Undersökning av beslagtagna informationsbärare i syfte att erhålla tillgång till information är i övrigt ett oreglerat område. Enligt Ekelöf är dagens reglering inte anpassad till teknikutvecklingen.[166] Det som gäller idag får antas ha utvecklats genom polisens praktiska arbete som bekräftas i statliga utredningar. Det verkar råda delade meningar huruvida information som lagras i informationsbärare bör få undersökas med stöd av reglerna om beslag och husrannsakan. I utredningssammanhang har argument framförts att elektroniskt lagrad information bör åtnjuta samma skydd som slutna förvaringsställen i enlighet med rättighetsskyddet i RF och EKMR. Följaktligen skulle ett särskilt beslut om husrannsakan krävas för undersökning av exempelvis en dators hårddisk. Detta skulle medföra ett starkare skydd för elektronisk information eftersom strängare krav gäller för husrannsakan. Denna uppfattning speglar dock inte verkligheten och uppfattningen hos de brottsbekämpande myndigheterna. Enligt Beslagsutredningen krävs det inget särskilt beslut för att kunna genomsöka datorer, mobiltelefoner eller andra elektroniska informationsbärare vilket även bekräftas av Larsson. Såväl beslags- som husrannsakansbeslut innefattar en möjlighet för polisen att undersöka informationsbärare i syfte att få tillgång till

[160] 28 kap. 1 § RB.
[161] Lindberg, 2018, s. 611-615; Bring m.fl., s. 168-171.
[162] Om en skriftlig handling kan antas innehålla uppgifter om en befattningshavare eller någon annan som avses i 36 kap. 5 § RB eller omfattas av tystnadsplikt får det inte beslagtas. Detta gäller exempelvis kommunikation mellan advokat och dess klient. Motsvarande gäller i vissa fall avseende kommunikation mellan närstående. Se 27 kap. 2 § RB; prop. 2015/16:68, s. 55f.
[163] 27 kap. 1 § RB; Bring m.fl., s. 403.
[164] Lindberg, 2018, s. 406; *jmf.* Ekelöf, 2009, s. 255.
[165] Lindberg, 2018, s. 403-405.
[166] Ekelöf, 2018, s. 83; *jmf.* Bring, m.fl., s. 423.

information som finns lagrad i föremålen oavsett om det krävs ett lösenord för att komma åt innehållet i informationsbäraren.[167]

Det förs en diskussion huruvida elektronisk information i sig ska kunna beslagtas. Eftersom beslagsbestämmelsen innebär en besittningsrubbning som fråntar ägaren av föremålet möjlighet att disponera över det anses uppfattningen vara att information som är en immateriell handling inte kan beslagtas. Informationen blir dock beslagtagen i samband med att informationsbäraren blir beslagtagen.[168]

Därutöver uppstår frågor om vilka åtgärder som får vidtas för att öppna en dator eller en mobiltelefon eller om polisen får öppna mobila applikationer för att avläsa information som lagras där. Elektronisk kommunikation kan endast undersökas med stöd av ett husrannsakans- eller beslagsbeslut om informationen är lagrad på en informationsbärare. Detta gäller exempelvis e-postprogram på datorn som kontinuerligt hämtar och lagrar e-postmeddelanden på datorns hårddisk (exempelvis imap[169]).[170] Endast information som inkommit och lagras på informationsbäraren vid tidpunkten för beslaget eller husrannsakan kan undersökas. Inkommande information efter beslagstidpunkten eller husrannsakan kan inte undersökas med stöd av respektive beslut eftersom det skulle innebära kringgående av reglerna om hemliga tvångsmedel.[171] Det är därmed heller inte tillåtet att hålla igång en mobiltelefon eller en dator för att invänta inkommande meddelanden.[172] Information som lagras externt, det vill säga meddelanden som ännu inte har nått mottagaren och som lagras hos operatören kan endast undersökas med stöd av beslut om hemlig avlyssning och övervakning av elektronisk kommunikation och LEK.[173] Inhämtning av information från tjänsteleverantörer omfattas dock inte av denna reglering och kommer att presenteras i avsnitt 4.7.

Reglerna om beslag och husrannsakan har överlevt teknikutvecklingen och bevisskiftningen på grund av dess teknikneutrala karaktär. Det faktum att reglerna inte har anpassats till teknikutvecklingen lagtekniskt börjar hysa tvivel om dess tillämpningsområde i den digitala miljön och gränsdragnings-problematik.[174] Enligt Flyghed medför bristfälligt underbyggda argument för nyttan och effekterna av tvångsmedelsanvändning att sådana medel

[167] Ds 2005:6, s. 281; SOU 2017:100, s. 266f; Beslagshandboken, s. 32f; Bring, m.fl., s. 424f; Lindberg, 2018, s. 621; Larsson, telefonintervju.
[168] SOU 2017:100, s. 172-175, 177-179; Lindberg, 2018, s. 407; Bring, m.fl., s. 404.
[169] Internet Message Access Protocol.
[170] Ds 2005:6, s. 283; SOU 2017:100, s. 181f; Larsson, telefonintervju.
[171] Prop. 2002/03:74, s. 45f; SOU 2017:100, s. 181; Bring m.fl., s. 423; *se* avsnitt 4.5.3.
[172] Beslagshandboken, s. 34; SOU 2017:100, s. 174.
[173] Beslagshandboken, s. 14f, 30.
[174] Lindberg, 2007, s. 55f.

normaliseras. Trots att flera tvångsmedel används för allvarlig brottslighet glider de ofta ut till att tillämpas även på lindrigare brottslighet.[175]

Kritiken har föranlett en översyn och förslag på anpassning av regleringen för den digitala miljön. Beslagsutredningen har delvis föreslagit reglering av kopiering av beslagtaget material men även av undersökning på distans av elektroniskt lagrad information som kan nås med hjälp av informationsbärare som undersöks under en husrannsakan eller som har beslagtagits (utvidgad undersökning). Detta gäller lagrings- och kommunikationstjänster som lagras i molnet[176]. De brottsbekämpande myndigheterna föreslås kunna få åtkomst till elektroniskt lagrad information genom användning av egen utrustning för att via ett elektroniskt kommunikationsnät bereda sig tillgång till informationen. Detta ska ske antingen via inloggning genom användning av den misstänktas användaruppgifter eller genom installation av program- eller maskinvara vilket inte är möjligt i dagsläget. Förslaget gäller informationsbärare som kan användas för kommunikation men även användarkonton av exempelvis en kommunikations- eller lagringstjänst.[177] Syftet med förslaget är endast att anpassa reglerna om husrannsakan och beslag till modern teknik och inte att skapa nya möjligheter till realtidsövervakning. Enligt utredningen är integritetsintrånget som uppstår vid en utvidgad undersökning proportionerlig. Tvångsmedlet medför inte ett större integritetsintrång än undersökning av lokalt lagrad information i en informationsbärare med stöd av ett husrannsakansbeslut. Informationen som myndigheten får del av är densamma. Det som skiljer sig åt är sättet att bereda sig tillgång till informationen. Därutöver gjorde utredningen bedömningen att utvidgad undersökning kommer att vara av stor nytta i de fall den får användning. Undersökning via kommunikationsnät genom installation av program- eller maskinvara ansågs dock medföra tillgång till samma information som förslaget om hemlig dataavläsning. Därmed ansåg utredning att det inte föreligger behov av en sådan metod.[178] I skrivande stund har förslaget remissbehandlats och bereds i Regeringskansliet.

4.5.3 Hemliga tvångsmedel

Hemliga tvångsmedel skiljer sig från ovan nämnda tvångsmedel genom att den som blir föremål för tvångsmedlet inte har vetskap om detta. Tvångsmedlen måste användas i hemlighet för att få den åsyftade verkan. Det finns ett antal kontrollmekanismer i syfte att säkerställa att tvångsmedlen inte används på ett

[175] Flyghed, 2007, s. 63f.
[176] En molntjänst används för att lagra information externt, i utomstående servrar istället för i den egna datorn, mobiltelefonen eller liknande.
[177] SOU 2017:100, s. 36, 300f, 311, 313; *jmf.* avsnitt 4.3.3 och 4.5.
[178] Ibid, s. 303-310, 314-316, 319-324.

felaktigt sätt och inskränker den enskildas integritet mer långtgående än nödvändigt.[179]

Hemliga tvångsmedel får endast användas om någon skäligen är misstänkt för ett brott och åtgärden är av synnerlig vikt för utredningen.[180] Här avses samma som för övriga tvångsmedel, det vill säga att misstanken ska vara underbyggd av objektiva omständigheter som talar för att en viss person begått brottet. När det gäller åtgärdens betydelse för utredningen ska i första hand andra, mindre integritetskränkande, metoder användas. Om bedömningen däremot utmynnar i att utredningen inte kan föras vidare med hjälp av andra medel och det finns skäl att anta att hemliga medel kan få verklig effekt, anses åtgärden av synnerlig vikt. Samma gäller om de mindre ingripande medlen kräver orimliga resurser.[181]

Ansökan om hemliga tvångsmedel framställs av åklagaren inför rätten. Åklagaren kan dock fatta interimistiskt beslut avseende tillstånd till hemlig avlyssning och övervakning av elektronisk kommunikation. Beslut kan fattas i avvaktan på domstolsprövning om ett inhämtande av domstolens tillstånd skulle medföra en tidsutdräkt eller annan olägenhet av väsentlig betydelse för utredningen.[182]

4.5.3.1 Hemlig avlyssning av elektronisk kommunikation

Hemlig avlyssning är ett mycket allvarligt ingrepp i den personliga integriteten eftersom innehåll i samtal och meddelanden kan avlyssnas utan den enskildes medgivande eller vetskap. Historiska meddelanden såväl som meddelanden i realtid kan avlyssnas.[183] Utgångspunkten är att den som olovligen avlyssnar kommunikationen kan dömas för olovlig avlyssning. Avlyssning kan medföra misstro och skapa otrygghet för medborgarna. I ett välfungerande samhälle kan avlyssning endast tillåtas för de ändamål som medborgarna är villiga att offra sitt skydd för.[184]

Hemlig avlyssning av elektronisk kommunikation innebär att meddelanden som överförs eller har överförts i ett elektroniskt kommunikationsnät, till eller från en adress, avlyssnas i hemlighet.[185] Lagstiftningen är teknikneutral, såväl datorkommunikation som telefoni kan avlyssnas i samma utsträckning. Avlysningen avser innehåll i exempelvis telefonsamtal, SMS och e-

[179] Lindberg, 2018, s. 487; *se* avsnitt 4.5.5.
[180] 27 kap. 20 § första stycket RB.
[181] Prop. 1988/89:124, s. 44f.
[182] 27 kap. 21 § första och andra styckena och 21a § RB; prop. 2011/12:55, s. 78f.
[183] SOU 2009:1, s. 60.
[184] 4 kap. 9a § BrB; prop. 1988/89:124, s. 36f; prop. 2002/03:74, s. 20f.
[185] 27 kap. 18 § RB.

postmeddelanden.[186] Tillstånd till hemlig avlyssning ger även rätt till övervakningsuppgifter[187] vilket motiveras med effektivitetsvinster samt att det inte medför ett större integritetsingrepp eftersom avlyssning är betydligt mer ingripande. Därutöver sker tillståndsprövningen på domstol och ett offentligt ombud deltar vid prövningen i syfte att värna om den enskildes integritet.[188]

Flera adresser[189] kan avlyssnas om de har en anknytning till den misstänkta. Antingen genom att den misstänkta innehar eller har innehaft en viss adress eller det kan antas att hen kommer att använda en viss adress. Exempel på detta är adresser som tillhör en partner eller personer i samma hushåll, arbetsplatser samt skola. Även adress som den misstänkte har kontaktat eller kan komma att kontakta kan avlyssnas om det finns synnerlig anledning att anta att den misstänkta kommer att ta kontakt med den adressen. Det ska kunna påvisas konkreta omständigheter som tyder på att kontakt kommer att ske eller har skett.[190]

Tvångsmedlet får endast användas för brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år, särskilt allvarliga brott som avses i 27 kap. 2 § andra stycket 2-7 RB eller vid försök, förberedelse eller stämpling till sådana brott. Hemlig avlyssning kan även användas för brott med lägre straffminimum om det kan antas att brottets straffvärde överstiger fängelse i två år.[191] Straffvärdesventilen infördes i syfte att effektivt kunna utreda brott med straffskalor som har höga straffmaximum men låga straffminimum.[192]

Enligt de brottsbekämpande myndigheterna är nyttan av hemlig avlyssning framträdande i det inledande stadiet av utredningen.[193] Det har förekommit diskussioner att misstankegraden för användning av tvångsmedlet bör sänkas eftersom tvångsmedlet ofta används för att nå ett bevisläge mot en viss person för att kunna tillgripa andra tvångsmedel. Med hänsyn till den integritetskränkning som avlyssning medför ansågs dock en sänkning av beviskravet obefogad.[194]

[186] SOU 2009:1, s. 60.
[187] *Se* avsnitt 4.5.3.2.
[188] 27 kap. 21 § första stycket RB; prop. 2011/12:55, s. 69f; SOU 2005:38, s. 220-222, *se* avsnitt 4.5.4.
[189] *Se* avsnitt 4.4.
[190] 27 kap. 20 § RB; prop. 1988/89:124, s. 45f; prop. 2002/03:74, s. 37-39; Lindberg, 2018, s. 512f.
[191] 27 kap. 18 § RB; prop. 2013/14:237, s. 44.
[192] Prop. 2013/14:237, s. 32-34.
[193] Lindberg, 2018, s. 506f.
[194] Prop. 1988/89:124, s. 43f.

4.5.3.2 Hemlig övervakning av elektronisk kommunikation

Hemlig övervakning avser inhämtning av information om meddelanden som förs eller har förts över i ett elektroniskt kommunikationsnät samt den geografiska positionen av elektroniska kommunikationsutrustningar (trafik- och lokaliseringsuppgifter).[195] Precis som hemlig avlyssning är bestämmelsen teknikneutral och avser kommunikation via all teknik som förs över i ett elektroniskt kommunikationsnät.

Syftet med hemlig övervakning är att kartlägga den misstänktas kontakter. Tvångsmedlet möjliggör tillgång till information om kommunikation som förekommit mellan olika adresser men inte innehållet i dessa.[196] Övervakningen ska avse en viss adress som har sådan anknytning till den misstänkta som presenterats ovan.[197] Genom övervakning kan polisen få information om exempelvis vilka telefonnummer samtal förs över till och vilka telefonnummer som ringt upp det övervakade numret, tidpunkt och längd för samtal, vilka hemsidor en abonnent har besökt och mellan vilka e-postadresser kommunikation har skett.[198] Dessa uppgifter kommer från operatörer som är skyldiga att spara uppgifterna enligt LEK.[199]

Lokaliseringsuppgifter om en viss elektronisk kommunikationsutrustning avser främst spårning av den misstänktas fysiska förehavanden.[200] Eftersom uppsatsen syftar till att undersöka digital brottslighet kommer detta inte beröras närmare.

Hemlig övervakning anses inte vara lika ingripande i den personliga integriteten. Av denna anledning kan tvångsmedlet användas vid brott för vilka det inte är föreskrivet lindrigare straff än fängelse i sex månader eller för vissa i bestämmelsen specificerade brott, däribland barnpornografibrott som inte är att anse som ringa samt för brott enligt 27 kap. 2 § andra stycket 2-7 RB. Därutöver kan tvångsmedlet användas vid försök, förberedelse och stämpling till sådana brott. I lagförarbetena poängterades dock att sådan övervakning kan innebära en kartläggning av den övervakade personen och den person som den övervakade kommunicerar med.[201] Enligt Lindberg kan dessutom en kombination av olika tvångsmedel användas för att skapa sig en bild av individens personliga förhållanden.[202] Naarttijärvi menar att trafikuppgifter är

[195] 27 kap. 19 § RB.
[196] Ibid.
[197] Prop. 2013/14:237, s. 92; *se* avsnitt 4.5.3.1.
[198] Prop. 2011/12:55, s. 48.
[199] Lindberg, 2018, s. 539; *se* avsnitt 4.6.
[200] *Jmf.* prop. 2011/12:55, s. 128.
[201] 27 kap. 19 § tredje stycket RB; prop. 1988/89:124, s. 49; *jmf.* Qvarnström, s. 139.
[202] Lindberg, 2007, s. 56.

minst lika integritetskränkande eftersom de gör det möjligt att kartlägga kommunikationsnätverk och skapa sociogram som visar på hur individer och grupper hänger samman och kommunicerar.[203]

Hemlig övervakning av historiska uppgifter kan även ske utan att det finns en skäligen misstänkt person. En förutsättning för sådan övervakning är att brottsmisstanken gäller ett brott som kan leda till beslut om hemlig avlyssning av elektronisk kommunikation.[204] I praktiken innebär det att övervakning av historiska uppgifter utan skäligen misstänkt person endast kan ske vid misstanke om våldtäkt mot barn eller då omständigheterna vid brottet är sådana att straffvärdet för ett annat sexualbrott[205] mot barn överstiger fängelse två år. I inledningsskedet av utredningen finns dock sällan misstanke om brott med minimistraff sex månader.[206]

4.5.4 Rättssäkerhetsgarantier

I syfte att skydda enskilda från missbruk av tvångsmedelsanvändning finns ett antal skydds- och kontrollmekanismer. Den enskilda ska underrättas när denne blir utsatt för tvångsmedel, såsom husrannsakan eller beslag. När det gäller hemliga tvångsmedel ska underrättelse ske i efterhand för att tvångsmedlet inte ska förlora sitt syfte. Om åtal väcks mot den misstänka kommer denna att få ta del av de tvångsmedel som använts gentemot hen, oavsett om medlen varit hemliga eller inte. Detta följer av rätten till partsinsyn.[207] Den mot vilken åtal inte har väckts ska underrättas om personen varit misstänkt för brottet. En innehavare av en avlyssnad eller övervakad adress ska också underrättas. Andra personer som blivit avlyssnade ska inte underrättas om underrättelsen kräver ytterligare identifieringsåtgärder. Underrättelsen ska ske senast en månad efter avslutad förundersökning om inte sekretess gäller för uppgifterna.[208]

Offentligt ombud utses och ska närvara i domstol vid beslut om bland annat hemlig avlyssning för att övervaka den enskildas integritetsintresse. Endast den som är eller var varit advokat eller ordinarie domare kan förordnas som offentligt ombud. Ombudets roll är att säkerställa att domstolens beslut är förenligt med lag och att tillståndet till tvångsmedelsanvändning utformas på ett

[203] Naarttijärvi, s. 271.
[204] 27 kap. 19 § fjärde stycket och 20 § andra stycket RB.
[205] Grovt barnpornografibrott, sexuellt utnyttjande av barn, sexuellt övergrepp mot barn, utnyttjande av barn för sexuell posering, köp av sexuell handling av barn, kontankt för att träffa ett barn i sexuellt syfte och sexuellt ofredande.
[206] RättsPM, 2016, s. 8.
[207] Prop. 2006/07:133, s. 27.
[208] 27 kap. 31 och 33 §§ RB; prop. 2006/07:133, s. 36-40.

sätt som inte kränker de enskildas integritet i onödan. Ombudet har även möjlighet att överklaga ett tillståndsbeslut.[209]

Därutöver sker en löpande parlamentarisk kontroll av tvångsmedels-användningen. Vissa myndigheter samt Justitieombudsmannen och Justitiekanslern utövar tillsyn och efterhandskontroller över användning av hemliga tvångsmedel och ska genom skrivelser redovisa resultaten till riksdagen. Regeringen ska ta fram en årlig skrivelse till riksdagen över tillämpningen av samtliga tvångsmedel.[210] Lindberg anför att det är viktigt att uppgifter om användning av tvångsmedel redovisas. Bristande redovisning kan leda till antingen överskattning eller underskattning av behovet och effekterna av tvångsmedlen.[211]

År 2008 inrättades en Säkerhets- och integritetsskyddsnämnd som genom eget initiativ utövar tillsyn genom inspektioner och undersökningar över de brottsbekämpande myndigheternas användning av hemliga tvångsmedel. En enskild som blir underrättad om att hen varit föremål för hemlig tvångs-medelsanvändning kan vända sig till nämnden för att få prövat huruvida tvångsmedelsanvändningen varit felaktig.[212] Nämnden kan vidare lämna underrättelser till de brottsbekämpande myndigheterna om behov av verksamhetsförändringar samt uttalanden till regeringen om behov av lagförändringar.[213]

4.6 Reglering av elektronisk kommunikation

4.6.1 ePrivacy-direktivet[214]

I syfte att tillförsäkra EU-medborgare skydd för behandling av deras personuppgifter inom sektorn för elektronisk kommunikation infördes ett antal EU-rättsliga direktiv och beslut på området kommunikation, media och IT.[215] I syfte att öka skyddet för medborgarnas integritet genom att harmonisera medlemsstaternas lagstiftning infördes bland annat ePrivacy-direktivet. Enligt direktivet ska de enskilda skyddas från olovlig avlyssning och lagring av

[209] 27 kap. 26-28 §§ RB; prop. 2002/03:74, s. 22-25; prop. 2006/07:133, s. 33f.
[210] Prop. 2006/07:133, s. 28.
[211] Lindberg, 2007, 53f.
[212] Prop. 2006/07:133, s. 31, 66.
[213] Ibid, s. 69.
[214] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation, OJ L 201, 31.07.2002.
[215] Prop. 2002/03:110, s. 111f.

kommunikation mellan abonnenter utan deras samtycke. Lagring av trafikuppgifter är endast tillåten i syfte att förmedla kommunikationstjänster. Trafikuppgifter om abonnenten ska raderas eller avidentifieras när de inte längre behövs för exempelvis fakturering.[216] Direktivet föreskriver att operatörer som tillhandahåller allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster ska säkerställa konfidentialitet.[217] Enligt direktivet har medlemsländerna rätt att föreskriva undantag från denna skyldighet, exempelvis för brottsbekämpande ändamål.[218] På vilket sätt sådana undantag ska genomföras och vilka krav dessa ska vara förenade med har utvecklats i praxis. Behovet av tillgång till uppgifter i brottsbekämpande sammanhang måste vara faktisk och strikt begränsad till de fall då tillgång krävs. Därutöver ska tillgången stå i rimlig proportion till ingreppet i den personliga integriteten. Lagstiftningen ska föreskriva klara och precisa regler avseende vilka säkerhetsmekanismer som operatörerna ska företa i syfte att skydda uppgifterna. Lagstiftningen ska ange materiella och formella villkor som bygger på objektiva kriterier enligt vilka myndigheterna ska få tillgång till uppgifterna.[219]

Direktivet är endast bindande i fråga om det resultat som ska uppnås. Det är därmed upp till varje medlemsstat att välja den form och metod som anses bäst för den egna staten i syfte att uppnå det angivna resultatet. LEK är ett resultat av EU-regleringen på området elektronisk kommunikation.[220] Kapitel 6 i LEK är ett resultat av ePrivacy-direktivet och avser behandling av trafikuppgifter samt integritetsskydd.

4.6.2 Lag om elektronisk kommunikation

LEK reglerar enskildas och myndigheternas tillgång till elektroniska kommunikationsnät och kommunikationstjänster. Med elektroniska kommunikationsnät avses system för överföring och utrustning för koppling eller dirigering av signaler medan kommunikationstjänster avser tjänster som tillhandahålls mot ersättning och som utgörs av överföring av signaler i elektroniska kommunikationsnät.[221] Rena innehålls- och lagringstjänster omfattas inte. Kommunikationstjänster som inte möjliggör överföring av signaler faller också utanför lagens tillämpningsområde. Det avgörande är därmed huruvida leverantören av en viss tjänst har inflytande över överföring av signaler som innehåller informationen. Skype Classic är ett exempel på sådana tjänster eftersom de möjliggör kommunikation över en redan

[216] Ibid, s. 69f, 249.
[217] ePrivacy-direktivet, art. 5.
[218] Ibid, art. 15.1.
[219] Tele2 Sverige, p. 115-121; *jmf.* prop. 2018/19:86, s. 62f.
[220] Prop. 2002/03:110, s. 110-112.
[221] 1 kap. 1, 4 och 7 §§ LEK; prop. 2011/12:55, s. 60.

föreliggande kommunikationstjänst. Kommunikationen sker via abonnentens befintliga internettjänst. Internetleverantören är den som har rådighet över överföringen av signalerna och inte tjänsteleverantören.[222] Även om operatören sköter överföringen av signaler som innefattar kommunikation kan kommunikationen inte utläsas då dess innehåll är osynligt för operatören.[223] Innehållet kan endast avläsas av avsändaren eller mottagaren och i vissa fall av tjänsteleverantören.

Anmälningspliktiga operatörer och internetleverantörer som tillhandahåller elektroniska kommunikationsnät och kommunikationstjänster ska följa LEK och därmed upprätthålla konfidentialitet vid kommunikation.[224] Enligt huvudregeln är verksamheterna skyldiga att avidentifiera och radera trafikuppgifter som förekommer i deras verksamhet och som inte längre behövs för överföring av kommunikation. Trafikuppgifter är ofta men inte alltid personuppgifter och avser alla uppgifter om abonnenter som behandlas i syfte att överföra ett elektroniskt meddelande eller för att fakturera meddelandet.[225] Lagen föreskriver dock vissa undantag från raderingsskyldigheten. Uppgifter som omfattas av beslut om hemlig avlyssning eller övervakning av elektronisk kommunikation ska inte raderas.[226]

LEK föreskriver en anpassningsskyldighet för verksamheter som tillhandahåller elektroniska kommunikationsnät och kommunikationstjänster. Skyldigheten innebär att verksamheten ska anpassas så att de brottsbekämpande myndigheterna ska kunna verkställa beslut om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation.[227] Operatörer och internetleverantörer som får tillgång till uppgifter om abonnemang samt innehåll i och information om elektroniska meddelanden i sin verksamhet har en tystnadsplikt avseende sådana uppgifter. Tystnadsplikten gäller dock inte när en brottsbekämpande myndighet begär att få tillgång till uppgifterna.[228]

Sedan år 2006 ska operatörer och internetleverantörer lagra historiska trafikuppgifter för brottsbekämpande ändamål. Lagändringen är ett resultat av Datalagringsdirektivet som syftade till att harmonisera lagstiftningen och säkerställa lagring av trafikuppgifter för utredning, avslöjande och åtal avseende allvarlig brottslighet.[229] Innan ändringen var det inte möjligt för myndigheterna

[222] 1 kap. 4 § andra stycket LEK; PTS, s. 13f, 21f.
[223] Naarttijärvi, s. 247f.
[224] 2 kap. 1 § LEK; prop. 2002/03:110, s. 253.
[225] 6 kap. 5-6 §§ LEK; prop. 2002/03:110, s. 257; SOU 2007:76, s. 48.
[226] 6 kap. 8 § LEK.
[227] 6 kap. 19 § LEK; *jmf*. prop. 2002/03:110, s. 268-270.
[228] 6 kap. 22 § LEK
[229] Prop. 2010/11:46, s. 12; SOU 2007:76, s. 43.

att få tillgång till sådana uppgifter, förutom de uppgifter som operatören eller internetleverantören lagrade för egen del för exempelvis fakturering. Endast realtidsuppgifter samlades in efter beslut om hemliga tvångsmedel.[230] Lagringsskyldigheten innebär att bland annat abonnemangsuppgifter som är nödvändiga för att spåra och identifiera kommunikationskällan, slutmålet med, datum, tidpunkt, varaktighet och typ av kommunikation, kommunikationsutrustning samt lokalisering av kommunikationsutrustning ska lagras.[231] Lagändringen motiverades med behovet av historiska trafikuppgifter vid utredning av allvarlig brottslighet, inbegripet barnpornografibrott. Inte minst för att kunna länka samman målsäganden och gärningspersoner men även för att det kan vara de enda uppgifterna av betydelse eftersom teknik såsom kryptering medför att innehåll i meddelanden inte kan avlyssnas. BRU anförde i sitt delbetänkande att det är svårt att uppskatta betydelsen av uppgifterna som bevisning i domstol. Trafikuppgifterna utgör oftast grundläggande vägledning för polisen, för utredningsarbetet framåt och kan leda till att annan bevisning kan tas fram som sedan åberopas i rättegången.[232]

Lagringsskyldigheten medförde att ett mycket stort antal trafikuppgifter om enskildas personliga förhållanden och korrespondens lagrades. Trafikuppgiftsutredningen påtalade att redan lagringen och tillgången till uppgifterna medför en integritetskränkning oavsett om uppgifterna sedan används i brottsbekämpande syfte eller inte. Integritetskränkningen består av att uppgifter om samtliga medborgare lagras och möjliggör insyn i förhållanden av privat natur som enskilda inte vill att andra ska få insyn i. Därutöver är risken för läckage ett allvarligt bekymmer och regleringen medför en psykologisk verkan som innebär att medborgarna blir misstänksamma gentemot det allmänna.[233] I svensk rätt balanserades integritetsintrånget genom bland annat öppen och transparant reglering, begränsad lagringstid på ett år samt skydds- och kontrollmekanismer.[234]

Datalagringsdirektivet och den svenska regleringen om lagring av trafikuppgifter ogiltigförklarades några år senare av EU-domstolen med motiveringen att de överskridit de gränser som proportionalitetsprincipen uppställer. Regleringen ansågs vara för omfattande och generell samt säkerhetsgarantierna alltför bristfälliga. EU-domstolen konstaterade att ingreppet som direktivet medförde i de enskildas integritet var långtgående och

[230] SOU 2005:38, s. 312.
[231] 6 kap. 16a § LEK. *Se* 39-40 §§ förordning (2003:396) om elektronisk kommunikation avseende de uppgifter som ska lagras och som kan utlämnas.
[232] SOU 2005:38, s. 322-325.
[233] SOU 2007:76, s. 110-112.
[234] SOU 2007:76, s. 233-238; prop. 2010/11:46, s. 20.

synnerligen allvarligt utan att vara noggrant avgränsat. Även syftet att bekämpa grov brottslighet kunde inte ensamt motivera en sådan odifferentierad lagring av samtliga uppgifter avseende samtliga abonnenter och samtliga kommunikationsutrustningar.[235] Till följd av EU-domstolens uttalanden har den svenska regleringen avseende lagring av trafikuppgifter omarbetats. Regleringen trädde ikraft den 1 oktober 2019. Att lagra sådana uppgifter ansågs vara en nödvändighet för avslöjande av allvarlig brottslighet som begås i den digitala miljön.[236] Lagringsskyldigheten har avgränsats till vissa uppgifter och en differentierad lagringstid har införts. Lagringsskyldigheten avser numera lagring av uppgifter som genereras eller behandlas vid telefonitjänst, meddelandehantering samt internetåtkomst.[237]

I normalfallet ska den som bedriver anmälningspliktig verksamhet utlämna information när beslut om ett hemligt tvångsmedel har fattats. LEK föreskriver dock en möjlighet för de brottsbekämpande myndigheterna att inhämta abonnemangsuppgifter[238], även kallade kataloguppgifter, utan prövning av domstol och utan några krav på misstänkt person eller straffvärde för det misstänkta brottet.[239] Abonnemangsuppgifter kan vara avgörande vid utredning av internetrelaterade brott. Vid en översyn av brottsbekämpande myndigheters tillgång till uppgifter om elektronisk kommunikation anförde regeringen att den tekniska utvecklingen lett till att ”mindre allvarliga” brott som har fängelse i straffskalan ofta leder till bötesbrott. Som exempel gavs nätmobbning och vuxnas sexuella kontakter med barn. Utan undantaget i LEK om utlämning av abonnemangsuppgifter skulle inhämtning av sådana uppgifter vara omöjlig. Vid analysen av det integritetsintrång som utlämningen skulle medföra anförde regeringen att utlämning av sådana uppgifter utgör ett visst intrång i den personliga integriteten eftersom abonnentens identitet röjs. Diskussionen avsåg främst utlämning av IP-adresser. Huvudargumentet som regeringen anförde var att privatpersoner ofta använder dynamiska IP-adresser som inte kan övervakas och kartläggas i samma utsträckning eftersom adressen byts ut. Därutöver avser utlämningen ett begränsat antal identitetsuppgifter. Regeringens slutsats var därmed att polisens behov av tillgång till abonnemangsuppgifter i syfte att utreda brott som begås på internet väger klart tyngre än enskildas motsvarande intresse av integritetsskydd.[240]

[235] *Se* Digital Rights och Tele2 Sverige.
[236] Prop. 2018/19:86, s. 26f.
[237] Prop. 2018/19:86, s. 35, 39-41, 46, 50-51.
[238] *Se* avsnitt 4.4.
[239] 6 kap. 22 § första stycket 2 och 20 § första stycket 1 LEK; SOU 2009:1, s. 69f; *se* även 6 kap. 16c § LEK.
[240] Prop. 2011/12:55, s. 101-103; *jmf*. prop. 2002/03:74, s. 16.

Ställningstagandet att dynamiska IP-adresser utgör kataloguppgifter har problematiserats av bland annat Naarttijärvi. Gränsdragningsproblematiken avseende vilka uppgifter som ska betraktas om abonnemangsuppgifter uppstår i diskussionen om vilka uppgifter som är kopplade till ett visst kommunikationstillfälle (trafikuppgifter) och vilka uppgifter som kan bidra till att identifiera en abonnent (abonnemangsuppgifter).[241] I Justitiedepartementets promemoria avseende Sveriges tillträde till cyberkonventionen[242] framfördes följande. En fast IP-adress avser ett permanent förhållande mellan kunden och företaget medan en dynamisk IP-adress är en tillfällig uppgift som krävs för att identifiera ett visst kommunikationstillfälle. Uppgifter om enskilda kommunikationstillfällen är typiskt sett att hänföra till trafikuppgifter. Dynamiska IP-adresser borde anses vara uppgifter om meddelanden och inte om abonnemanget.[243] Utredarens definition har dock inte fått någon praktisk genomslag. Utgångspunkten att dynamiska IP-adresser utgör abonnemangsuppgifter är gällande. Diskussionen är dock viktig eftersom den avgör vilka uppgifter som de brottsbekämpande myndigheterna kan få tillgång till.[244]

4.7 Inhämtning av digital bevisning från tjänsteleverantörer

4.7.1 Inledning

Utöver de ovan presenterade möjligheterna att inhämta information som kan utgöra digital bevisning kan betydelsefull information även inhämtas från leverantörer av webbsidor, sociala medier och applikationer som verkar på internet. Enligt Larsson har 1 533 förfrågningar år 2019 (fram till 19 december 2019) skickats till leverantörer vars verksamhet inte omfattas av LEK varav 80 % av dessa har besvarats.[245] Inhämtning av uppgifter från tjänsteleverantörer är därmed en betydande åtgärd vid utredningar om sexualbrott mot barn. Inhämtning av sådan information kan utgöra ett förstadium till en förundersökning och användning av andra tvångsmedel.[246] Internet är globalt vilket innebär att informationen kan lagras var som helst i världen vilket kan medföra att inhämtningen blir förenad med rättsliga svårigheter.[247] Det finns ett antal EU och internationella samarbeten som reglerar inhämtning och utlämning

[241] Naarttijärvi, s. 283.
[242] Europarådets konvention om IT-relaterad brottslig, ETS nr. 185, Budapest 23 november 2001.
[243] Ds 2005:6, s. 325f.
[244] Naarttijärvi, s. 284-286.
[245] Larsson, e-post.
[246] Kronqvist, s. 56.
[247] Ibid, s. 55; *jmf.* Lindberg, 2007, s. 51.

av digital bevisning men det finns ingen gemensam rättslig nivå.[248] Framgången i gränsöverskridande utredningar är beroende av staternas och tjänsteleverantörernas välvilja att bidra till utredningen.

En stor del av kommunikationen sker numera genom internet via icke anmälningspliktiga tjänsteleverantörer. Exempel på detta är internetbaserade e-posttjänster såsom Hotmail, Gmail och Yahoo, som andra typer av kommunikationstjänster såsom Apple iMessage, Messenger, Skype, WhatsApp och Kik.[249] Information som lagras på internetbaserade kommunikationstjänster omfattas inte av lagringsskyldigheten i LEK.[250] Detta innebär att en omfattande del av de tjänster som vi använder oss av idag inte omfattas av någon reglering som ger polisen rätt att ta del av innehållet i dessa.

Internetbaserade tjänster fungerar på så sätt att användaren har ett användarkonto som skyddas med ett lösenord och som ger åtkomst till tjänstens innehåll. Enligt Beslagsutredningen är uppfattningen att åtkomst till sådan elektroniskt lagrad information inte är tillåten om innehållet inte är allmänt tillgängligt.[251] Viss information på internet är öppet tillgänglig för alla, även polisen. Sådan information karaktäriseras av att den som lägger ut informationen är medveten om att andra kan ta del av den. Enligt Kronqvist kan polisen genom iakttagelser och inskaffande av allmänt tillgänglig information fritt samla in bevisning från internet. Detta gäller både nationellt och internationellt.[252] Enligt Larsson är det inte förbjudet för polisen att interagera med folk på internet så länge det inte är fråga om bevis- eller brottsprovokation.[253]

Enligt Kronqvist kan digital bevisning från internet användas i två olika syften, antingen för att identifiera gärningspersonen (identifieringsbevisning) eller för att knyta gärningspersonen till den begångna gärningen (informationsbevisning).[254] I många fall kan bevisningen användas i syfte att bevisa båda vilket exemplifieras av Husbymålet.

4.7.2 Abonnemangsuppgifter

Uppgifter från tjänsteleverantörer kan delas upp i två kategorier, abonnemangsuppgifter och uppgifter om innehåll. Olika förutsättningar gäller vid inhämtning för respektive uppgiftskategori. Med abonnemangsuppgifter avses i detta sammanhang främst användarinformation som en individ angett

[248] *Se* exempelvis SÖ 2005:42.
[249] SOU 2017:75, s. 127f; SOU 2017:100, s. 182.
[250] *Se* avsnitt 4.6.2.
[251] SOU 2017:100, s. 231.
[252] Kronqvist, s. 55, 87.
[253] Larsson, telefonintervju.
[254] Kronqvist, s. 55.

vid registreringen på en viss tjänst och IP-adress. Vilken sorts uppgifter som innefattas beror på tjänsteleverantören.[255]

Många tjänsteleverantörer medverkar frivilligt till brottsutredningar och utlämnar abonnemangsuppgifter till de brottsbekämpande myndigheterna utan stöd i lag. De allra flesta stora företag vill inte ha övergreppsmaterial på barn på sina plattformar. Polisen har ett antal samarbetsavtal, främst med internationella men även nationella tjänsteleverantörer. Vissa av avtalen innefattar även utlämnande av innehållsuppgifter. Larsson anger att leverantörer som polisen samarbetar med tillförsäkrar att utlämna användar- och inloggningsuppgifter samt vissa lokaliseringsuppgifter inom två veckor.[256] Facebook är en av leverantörerna som samarbetar med polisen och utlämnar information om svenska användare och konton. Informationen möjliggör identifiering av personen bakom kontot.[257] Det finns dock ett antal tjänsteleverantörer som inte medverkar. Främst handlar det om leverantörer som har som affärsidé att dess användare ska kunna vara anonyma.[258]

De flesta tjänsteleverantörer reglerar sitt samarbete med brottsbekämpande myndigheter i sina olika policys och användarvillkor. Genom att godkänna villkoren ger användarna leverantörerna rätt att utlämna informationen. Utlämning sker främst av abonnemangsuppgifter men även innehåll kan utlämnas. Villkoren för myndighetsförfrågningar och uppgifter som kan erhållas varierar mellan leverantörerna.[259]

4.7.3 Uppgifter om innehåll

Innehållsuppgifter är svårare att erhålla och kan kräva beslut om internationell rättslig hjälp. Detta följer av den folkrättsliga territorialitetsprincipen som föreskriver att en stat inte får utöva makt inom en annan stats territorium. Sverige kan därmed inte verkställa beslut om straffprocessuella tvångsmedel i ett annat land utan måste be den aktuella staten om hjälp. Detta gäller även möjligheten att med hjälp av tekniska hjälpmedel bereda sig tillgång till utomlands lagrad elektronisk information. Externt lagrad information medför därmed en del problem i utredningssammanhang eftersom informationen kan lagras i princip var som helst i världen.[260]

[255] Larsson, telefonintervju.
[256] Ibid; *jmf.* SOU 2017:100, s. 291f; RättsPM, 2016, s. 7.
[257] Sadikovic, 2018.
[258] Larsson, telefonintervju.
[259] *Se* exempelvis Facebook, Användarvillkor; Snapchat, Law Enforcement Guide; Kik, Law Enforcement Information; WhatsApp, Law Enforcement Information.
[260] SOU 2017:100, s. 362f.

Uppgifter om innehåll anses utgöra övervakning, därmed krävs någon form av åklagar- eller domstolsbeslut för utlämning. Detta gäller information hos såväl svenska som utländska tjänsteleverantörer. När det gäller svenska leverantörer räcker det oftast med ett husrannsakansbeslut under förutsättning att uppgifterna inte kan inhämtas med stöd av beslut om hemlig avlyssning.[261] Det problematiska är när leverantören inte vill samarbeta. Polisen saknar kunskap om informationens lagringsplats vilket innebär att samtliga servrar som leverantören har måste beslagtas. Detta är en omfattande åtgärd som kan göra mycket skada. Starka proportionalitetshänsyn måste föreligga för sådana beslag. I första hand försöker polisen få leverantören att samarbeta med att utlämna informationen. Leverantörer utanför EU kräver dock begäran om internationell rättslig hjälp vilket, om man har otur, kan ta några år att få svar på.[262]

Lagen (2000:562) om internationell rättslig hjälp i brottmål (Libr) innehåller regler om åklagarens och domstolarnas internationella samarbete vid utredning och lagföring av brott. Rättslig hjälp innefattar olika åtgärder som kan vidtas vid en brottsutredning däribland husrannsakan och beslag av elektroniskt lagrad information samt hemliga tvångsmedel.[263] Lagen måste användas om exempelvis en dator eller mobiltelefon har blivit beslagtagen i Sverige men informationen lagras utomlands. Ansvarig åklagare måste ansöka om tillstånd från domstol eller myndighet i det landet för att få ut informationen.[264] Inom EU, förutom Danmark och Irland, kan tvångsmedel användas tvärs över landsgränserna med stöd av lagen (2017:1000) om europeisk utredningsorder. Beslut som har fattats i ett europeiskt land ska erkännas och verkställas i ett annat europeiskt land utan prövning av skälen för beslutet. Syftet med åtgärden ska vara att säkra bevisning.[265]

Ett första steg mot en gemensam internationell lagstiftning avseende internetrelaterad brottslighet är cyberkonventionen. Konventionen antogs 2001 och trädde i kraft år 2004. Konventionen är speciell på så sätt att även icke-medlemmar av Europarådet kan tillträda den.[266] Hittills (fram till den 3 januari 2020) har tre stater av de som antagit konventionen inte ratificerat den, Sverige är en av dem.[267] Två utredningar har tillsatts i syfte att se över vilka författningsändringar som krävs för att Sverige ska kunna tillträda konventionen men ingen av dessa har lett till lagstiftning ännu.[268] Cyberkonventionen syftar till att åstadkomma en tillnärmning av staters nationella straffrätt avseende vissa

[261] *Jmf.* avsnitt 4.4.3.1 och 4.5.2.
[262] Larsson, telefonintervju; SOU 2017:100, s. 180, 288, 292; *jmf.* avsnitt 4.4.2.
[263] 1 kap. 1-4 §§ Libr; prop. 1999/00:61, s. 46-49.
[264] Larsson, telefonintervju.
[265] 1 kap. 2-4 §§ lagen om europeisk utredningsorder.
[266] Lindberg, 2007, s. 51; Kronqvist, s. 57.
[267] Chart of signatures and ratifications of Treaty 185.
[268] Ds 2005:6 och SOU 2013:39.

brott. Därutöver ska konventionen säkerställa nationella processrättsliga bestämmelser som tillgodoser behovet att utreda och lagföra sådana brott samt behovet att tillvarata digital bevisning. Slutligen syftar konventionen till att skapa ett snabbt och effektivt internationellt samarbete vid bekämpning av IT-brott.[269] Konventionen innehåller ett frysningsinstrument som innebär att en stat kan skicka en förfrågan till en annan stat om bevarande av innehåll på en viss tjänst. Frysning innebär att all information som finns vid det aktuella tillfället bevaras under tiden som begäran om internationell rättslig hjälp upprättas och behandlas så att det finns någon information att få ut. Svenska brottsbekämpande myndigheter kan skicka en begäran om frysning till andra konventionsstater men kan själva inte erbjuda det hos svenska leverantörer då ett sådant instrument inte är reglerat i svensk lag.[270]

Enligt utredningen om IT-brottskonventionen medför frysning inget ytterligare integritetsintrång. Det är utlämnandet av uppgifterna som kan medföra integritetsintrånget. Åtgärden avser endast ett bevarandeföreläggande i avvaktan på ytterligare åtgärder från brottsbekämpande myndigheter i syfte att få tillgång till uppgifterna. Bevarandet innebär att uppgifterna under viss tid ska behållas intakta på ett sådant sätt att de inte kan förstöras, förändras eller göras oåtkomliga. Tiden för bevarandet föreslogs till 90 dagar.[271] Förslaget är fortfarande under beredning.

4.7.4 Förslag om hemlig dataavläsning

Det finns flera olika sätt att inhämta digital bevisning men dessa motsvaras inte av möjligheten att faktiskt göra så. Allt oftare är den internetbaserade kommunikationen krypterad. Facebooks Messenger och Instagram, Whatsapp, Skype, MSN, Google mail, iMessage, Twitter, Snapchat och Viber har alla inbyggda funktioner som utför kryptering. Även information som finns i datorer och mobiltelefoner krypteras allt oftare genom inbyggda krypteringstjänster. Det uppskattas att endast cirka tio procent av den avlyssnade informationen kan avläsas i klartext. Deep web och Darknet är platser som inte är allmänt tillgängliga genom vanliga sökmotorer eftersom de är lösenordskyddade eller har ett krypterat innehåll. Darknet innehåller marknadsplatser för i princip all sorts illegal verksamhet där besökaren kan köpa vapen och narkotika, utväxla barnpornografiskt material samt beställa kriminella tjänster.[272]

Kryptering och anonymisering minskar befintliga tvångsmedels effektivitet och polisens möjligheter att utreda och bekämpa brott som sker via internet. I syfte att åtgärda denna brist har förslag lagts fram om hemlig dataavläsning. Förslaget

[269] SOU 2013:39, s. 51.
[270] SOU 2017:100, s. 293; Larsson, telefonintervju; RättsPM, 2016, s. 7.
[271] SOU 2013:39, s. 256-259, 261f.
[272] SOU 2017:89, s. 162-167.

innebär att avläsning eller upptagning med ett tekniskt hjälpmedel av uppgifter avsedda för automatiserad behandling i elektronisk kommunikationsutrustning eller ett användarnamn blir tillåten. De flesta av uppgifterna som föreslås kunna inhämtas med hemlig dataavläsning kan redan inhämtas genom befintliga hemliga tvångsmedel. Däremot finns ett påtagligt behov av nya och bättre metoder för att i hemlighet komma åt uppgifterna.[273] Regeringen har gjort bedömningen att det föreligger ett påtagligt behov att även kunna inhämta uppgifter löpande i realtid i hemlighet.[274] Tvångsmedlet anses utgöra en effektiv åtgärd som överväger de negativa effekterna som förslaget får i form av integritetskränkning mot den som blir föremål för åtgärden.[275] Integritetsrisken som tvångsmedlet medför motsvarar vad som gäller vid hemlig avlyssning och hemlig kameraövervakning, därav ska samma krav ställas vid inhämtning. Avgörande för vilka brott tvångsmedlet ska kunna användas vid är vilka uppgifter det är som ska inhämtas. Avser åtgärden att exempelvis inhämta avlyssningsuppgifter ska åtgärden endast användas vid sådana brott som kan föranleda hemlig avlyssning.[276] Hemlig dataavläsning kommer främst kompensera för det effektivitetsbortfall som de befintliga tvångsmedlen haft på senare tid. Enligt regeringen kommer tvångsmedlet främst användas för samma brottstyper som vid befintliga hemliga tvångsmedel, det vill säga narkotika- och våldsbrott men även sexualbrott, grovt rån, människohandel och grovt mordbrand.[277]

[273] Prop. 2019/20:64, s. 69-71; SOU 2017:89, s. 17-21.
[274] Prop. 2019/20:64, s. 75-77.
[275] Ibid, s. 81-83, 85-88, 90-97, 208.
[276] Ibid, s. 97, 113-116.
[277] Ibid, s. 208.

5 Analys

5.1 Inledning

Uppsatsen har två syften, för det första, att undersöka polisens tillgång till digital bevisning bestående av information om och innehåll i elektronisk kommunikation vid sexualbrott mot barn via internet. För det andra att problematisera och diskutera lagstiftarens intresseavvägning mellan effektiv brottsbekämpning och personlig integritet i ljuset av rättssäkerhetsintresset. Sexualbrott mot barn via internet har ökat betydligt de senaste åren. Digital bevisning är oftast den enda bevisningen som finns att tillgå vid utredning av internetrelaterade brott. För att polisen ska kunna utreda brotten på ett effektivt sätt utarbetas, såväl nationella som internationella utredningsåtgärder som möjliggör tillgång till digital bevisning.

5.2 Sexualbrott mot barn via internet

Sexualbrottslagstiftningen har omarbetats i flera omgångar i syfte att stärka skyddet för barn mot sexuella övergrepp. Lagstiftningen har ändrat karaktär genom att kriminalisera kränkningen som sexualbrottet medför istället för det tekniska genomförandet av den sexuella handlingen. Alla handlingar, från samlag till blottning och sexuella kontakter, som har en sexuell prägel eller syftar till att tillfredsställa gärningspersonens sexuella drift är förbjudna när de företas mot ett barn.[278] De olika brotten skulle kunna delas in i tre kategorier som särskiljs genom kvalificeringen av den sexuella handlingen som barnet utsätts för. Kvalificerade sexuella handlingar som är jämförbara med samlag (våldtäkt mot barn), mindre kvalificerade sexuella handlingar som inte är jämförbara med samlag (sexuellt utnyttjande av barn och sexuellt övergrepp mot barn) samt handlingar som har en sexuell innebörd men som enligt lagförarbeten inte definieras som sexuella handlingar (utnyttjande av barn för sexuell posering, sexuellt ofredande, köp av sexuell handling av barn, kontakt för att träffa ett barn i sexuellt syfte). Bedömningen avseende handlingens sexuella karaktär samt kränkningen som den medför utmynnar i vilket brott som gärningspersonen ska dömas för. Därutöver kan gärningspersonen dömas för barnpornografibrott, i konkurrens med brotten i sjätte kapitlet brottsbalken, om hen befattar sig med barnpornografiskt material.

[278] *Se* avsnitt 3.2-3.3.

Ändringen av lagstiftningens fokus från varaktiga fysiska beröringar samt det tekniska genomförandet av den sexuella handlingen har lett till att samtliga sexuella övergrepp mot barn via internet på ett naturligt sätt inkorporerats i skyddet som lagen uppställer. Denna utveckling har skett genom lagförarbeten och praxis men kan härledas till omarbetningen av bestämmelserna och dess ändamål. Fysiskt deltagande är inte längre en förutsättning för gärnings-mannaskap vid sexualbrottslighet. Det har inte ansetts föreligga behov av att i lagstiftningen ordagrant ange att den omfattar handlingar som företas på distans eller att det för straffbarhet är tillräckligt att barnet genomfört den straffbelagda gärningen på sig själv, utan fysisk närvaro av gärningspersonen, eftersom det av lagens syfte framgår att barn har ett absolut skydd mot sexuella övergrepp. En förutsättning för ansvar avseende sexuella handlingar genomförda på distans verkar dock vara gärnignspersonens närvaro under den del av händelseförloppet som innehåller den sexuella handlingen. Här avses någon form av deltagande i realtid, exempelvis genom webbkamera eller chatt. Legalitetsprincipen begränsar tillämpningsområdet för rekvisitet *genomför en sexuell handling med* till att endast innefatta sådana handlingar som företas *inför* gärningspersonen.[279] Detta kan tyckas vara olyckligt med hänsyn till lagstiftningens syfte att hindra personer från att använda eller utnyttja en annan persons kropp som ett hjälpmedel för att bereda sig själv sexuell tillfredsställelse. Syftet med att förmå ett barn att företa en sexuell handling i ensamhet, filma denna och sedan skicka filmklippet till gärningspersonen bör enligt min mening innefattas i lagstiftningens skyddsintresse. Barnet kan utsättas för samma kvalificerade sexuella handlingar oavsett om gärningspersonen deltar i realtid eller inte. Högsta domstolens uttalanden innebär dock inte att gärningspersonen går ostraffad. Det finns flera bestämmelser som kan tillämpas för att fånga upp det klandervärda beteendet.

5.3 Inhämtning av digital bevisning vid utredning av sexualbrott mot barn via internet

Sexualbrott mot barn via internet har ökat i omfattning i takt med utvecklingen av nya kommunikationsmedier och framför allt genom utvecklingen av internet. Förutom krypterings- och anonymiseringstjänster möjliggör internet anonym kommunikation genom att användaren kan utge sig för att vara någon helt annan. Detta är särskilt problematiskt vid utredning av internetrelaterade brott. Därutöver är internet en global mötesplats som medför rättsliga gräns-överskridande svårigheter i utredningssammanhang.

[279] *Se* avsnitt 3.3.

Svensk lagstiftning föreskriver ett antal rättsliga möjligheter för inhämtning av digital bevisning. För det första kan information inhämtas genom användning av tvångsmedel. Beslut om husrannsakan och beslag kan användas i syfte att bereda sig tillgång till informationsbärare som innehåller elektroniskt lagrad information samt undersökning av informationen. Denna utveckling har skett genom polisens praktiska arbete som accepterats av såväl Justitie-ombudsmannen och Justitiekanslern som lagstiftaren. Polisen kan antingen undersöka informationsbäraren på plats under en pågående husrannsakan eller genom att beslagta denna och genomföra undersökningen vid ett senare tillfälle. Undersökningen begränsas dock till att avse historiska uppgifter som är lokalt lagrade på informationsbäraren, exempelvis datorns hårddisk eller mobiltelefonens SIM-kort. Sparade e-postmeddelanden, SMS, foton samt metadata som lagras på informationsbäraren kan undersökas. Uppfattningen avseende användning av husrannsakan och beslag är att det inte får användas för att bereda sig tillgång till externt lagrad information genom exempelvis användning av den misstänktes inloggningsuppgifter. Det finns därmed en väldigt fin gräns för vilken information som kan undersökas.

Om informationen inte lagras på den misstänktas informationsbärare finns två olika sätt att få tillgång till informationen beroende på vilken leverantör som lagrar den. När det gäller information vars överföring sköts av operatörer och internetleverantörer kan inhämtning ske med stöd av hemlig avlyssning och hemlig övervakning av elektronisk kommunikation samt LEK. Detta återkommer jag till nedan. När det däremot gäller information som lagras hos tjänsteleverantörer gäller följande. De flesta kommunikationstjänster som vi använder oss av idag, såsom Facebook, Instagram, Messenger, iMessage, Snapchat, Kik, Viber, Skype, Whatsapp är oreglerade i lag. Mycket information som kan vara av avgörande betydelse i en brottsutredningen är därmed oreglerad. De flesta tjänsteleverantörer lämnar dock ut abonnemangsuppgifter till polisen frivilligt, oavsett om de är svenska eller utländska, eftersom det finns en vilja att bekämpa sexualbrott mot barn. Polisen har avtal med flera nationella och utländska leverantörer för att effektivisera detta arbete. När det kommer till svenska tjänsteleverantörer som inte samarbetar kan polisen fatta beslut om husrannsakan hos tjänsteleverantören i syfte att eftersöka och beslagta den efterfrågade informationen. Sådana beslag medför svåra proportionalitets-bedömningar eftersom att en ofantlig mängd information beslagtas avseende många individer som inte har något med brottet att göra och måste kunna motiveras med tyngre vägande intressen än den integritetskränkning som åtgärden medför. Min uppfattning är att proportionalitetsbedömningen aldrig skulle utmynna i ett beslut om husrannsakan respektive beslag av den omfattningen vid enstaka mindre allvarliga sexualbrott mot barn.

När inhämtningen gäller innehållsuppgifter från utländska tjänsteleverantörer kan detta endast ske genom en begäran om internationell rättslig hjälp alternativt europeisk utredningsorder. Rättshjälpsbegäran kan dock ta lång tid att få svar på vilket kan äventyra utredningens framgång eftersom information på internet ändras och raderas frekvent. Frysning är ett internationellt instrument som kan nyttjas i syfte att bevara information som kan vara av betydelse för utredningen och som kan begäras gentemot konventionsstaterna till cyberkonventionen i avvaktan på beslut om internationell rättslig hjälp. På detta sätt säkerställer polisen att det faktiskt finns någon information att få ut.

Om polisen däremot vill inhämta information om och innehåll i elektronisk kommunikation från operatörer och internetleverantörer måste beslut om hemlig avlyssning respektive hemlig övervakning av elektronisk information fattas. Hemlig avlyssning reglerar exklusivt möjligheten att vid viss typ av brottslighet få uppgifter om innehållet i elektroniska meddelanden. Tillstånd till avlyssning av elektronisk kommunikation ger samtidigt rätt att övervaka meddelandena. Hemlig övervakning ger en möjlighet att ta del av information om elektronisk kommunikation. En förutsättning för hemlig övervakning och avlyssning är dock att polisen kan ange en adress som ska övervakas eller avlyssnas och att brottet för vilket beslutet fattats är av viss beskaffenhet. Här blir tjänsteleverantörernas och allmänhetens tips om misstänkta användarkonton och IP-adresser samt inhämtning av historiska abonnemangsuppgifter med stöd av LEK ett avgörande inslag i utredningen. Enligt 6 kap. 22 § första stycket 2 punkten LEK kan polisen inhämta abonnemangsuppgifter vid misstanke om brott från operatörer och internetleverantörer. Detta är den mest utnyttjade metoden för att inhämta abonnemangsuppgifter som kan underlätta för polisen att identifiera en misstänkt person eftersom bestämmelsen endast uppställer krav på misstanke om brott. Det krävs varken brottslighet av visst slag eller ett särskilt straffvärde för att kunna inhämta informationen. Anledningen till detta är att inhämtning av abonnemangsuppgifter inte anses utgöra ett tvångsmedel.

Även om det finns ett antal utredningsåtgärder som ger polisen tillgång till digital bevisning är de alla förknippade med brister. Hemliga tvångsmedel kan sällan användas vid sexualbrott mot barn via internet eftersom de föreskrivna straffskalorna inte uppnår straffvärdeskraven. Hemlig avlyssning kan användas vid utredning av våldtäkt mot barn medan hemlig övervakning av elektronisk kommunikation kan användas vid utredning av våldtäkt mot barn, grovt sexuellt övergrepp mot barn, grovt utnyttjande av barn för sexuell posering samt barnpornografibrott som inte är ringa. Hemlig avlyssning skulle även kunna användas vid utredning av sexuellt utnyttjande av barn, grovt sexuellt övergrepp mot barn, grovt utnyttjande av barn för sexuell posering samt grovt barnpornografibrott om det med hänsyn till omständigheterna kunde antas att brottets straffvärde överstiger fängelse två år. Detta förutsätter att utredaren

utifrån den inledande information kan göra bedömningen att det förväntade straffvärdet för brottet når upp till straffvärdeskravet vilket sällan är fallet.[280] De flesta internetrelaterade brotten som utreds är inte av det allvarliga slaget som reglerna om hemliga tvångsmedel tar sikte på.[281] Tillämpningsområdet för hemlig avlyssning och hemlig övervakning av elektronisk kommunikation är därmed snävt och kan endast användas vid utredning av ett fåtal sexualbrott mot barn via internet eller i ett senare skede av utredningen. Därutöver har hemlig avlyssning och hemlig övervakning förlorat sin effektivitet på grund av den ökande användningen av krypterings- och anonymiseringstjänster. Även om brottet, för vilket avlyssning beslutats för, skulle uppnå det höga straffvärdeskravet är det inte säkert att informationen skulle kunna avlyssnas i klartext.[282] Det finns därmed behov av anpassning av de befintliga hemliga tvångsmedlen till den digitala miljön avseende brott med lägre straffminimum. Förslaget om hemlig dataavläsning syftar till att effektivisera användning av hemliga tvångsmedel i digitala miljöer. Med hänsyn till att förslaget föreslås innehålla samma höga straffvärdeskrav är det tveksamt huruvida det nya tvångsmedlet kommer kunna användas i större utsträckning än befintliga hemliga tvångsmedel vid utredning av sexualbrott mot barn via internet.

Såväl beslag som husrannsakan kan användas som utredningsåtgärder vid misstanke om sexualbrott mot barn eftersom samtliga brott föreskriver straff på fängelsenivån.[283] Användning av husrannsakan och beslag förutsätter dock att det finns en skäligen misstänkt person och adress som den misstänkta kommunicerar från, vilket det sällan finns information om i det inledande stadiet av utredningar av internetrelaterade brott. Därutöver förekommer kritik mot att dessa tvångsmedel, såsom de är utformade idag, används i digitala miljöer. Husrannsakan och beslag infördes främst med avseende på fysiska föremål och skriftliga handlingar som kunde vara av betydelse för en brottsutredning. Idag används dessa även för undersökning av immateriell information. I syfte att anpassa regleringen av husrannsakan och beslag till den digitala miljön finns lagförslag om utvidgad undersökning.[284] Lagförslaget innebär att polisen ska kunna använda tvångsmedlen för att få tillgång till information på distans genom inloggning på internettjänster som den misstänka använder sig av vilket kan öka effektiviteten och resultera i bättre tillgång till elektronisk kommunikation i de fall det finns en misstänkt person.

Jag anser att utvecklingen av tillämpningsområdet av husrannsakan och beslag är naturlig. Brottsbekämpande myndigheters utredningsåtgärder utvecklas i takt

[280] *Se* avsnitt 4.5.3.2.
[281] SOU 2017:100, s. 296-298.
[282] *Jmf.* Ibid.
[283] *Se* avsnitt 4.5.2.
[284] Ibid.

med den övriga utvecklingen i samhället. Detta är bland annat konsekvensen av teknikneutral lagstiftning som möjliggör användning av befintliga rättsregler på nya medier. Förenklat uttryckt kan sägas att utredningsåtgärderna avser att komma åt samma sorts information, det vill säga information som kan utgöra bevisning i en brottsutredning. Skillnaden är formen som bevisningen har samt dess källa.

Sammantaget kan konstateras att det finns flera olika utredningsåtgärder som polisen kan använda sig av i syfte att få tillgång till digital bevisning. Tvångsåtgärder kan dock sällan användas vid utredningar av sexualbrott mot barn med hänsyn till föreliggande straffvärdeskrav. Utredningsåtgärderna kan komma att användas i ett senare skede av brottsutredningen men medför inga effektivitetsgarantier, delvis på grund av föreliggande tjänster såsom kryptering och anonymisering men även på grund av informationens föränderliga karaktär och internetets globala omfattning. Den mest effektiva utredningsåtgärden i inledningsstadiet av en utredning är inhämtning av abonnemangsuppgifter från operatörer, internetleverantörer och tjänsteleverantörer. Sådan informations-inhämtning är i många fall en förutsättning för framgång i en brottsutredning av sexualbrott mot barn via internet.

5.4 Avvägningen mellan effektiv brottsbekämpning och personlig integritet

Effektiv brottsbekämpning och personlig integritet är två viktiga allmänna intressen som ställs mot varandra vid diskussioner om brottsbekämpande myndigheters utredningsåtgärder. Ställningstaganden avseende dessa intressen är inte endast avgörande för brottsbekämpande myndigheters befogenheter men även de prioriteringar vi vill att staten vi lever i ska ha. Kollektiv samlevnad förutsätter att vissa enskilda intressen ger vika för kollektiva intressen såsom brottsbekämpning. I syfte att upprätthålla detta intresse måste de brotts-bekämpande myndigheterna ha effektiva utredningsåtgärder som kan medföra intrång i den personliga integriteten. Skyddet för den personliga integriteten fastställs i såväl svensk grundlag som olika internationella instrument. Den enskilda har rätt till skydd för information om dennes personliga förhållanden och rätt att inte vara föremål för övervakning och kartläggning. Integritets-skyddet är inte absolut och kan begränsas om det sker för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle i enlighet med principerna om ändamål, behov, och proportionalitet. Därutöver övervakar EU-domstolen och Europadomstolen staternas lagstiftning så att denna inte strider mot respektive institutions skydd för den personliga integriteten.

Den första frågan som man måste ta ställning till är vad som utgör en kränkning av den personliga integriteten när bedömningen avser inhämtning av information om individens personliga förhållanden. Enligt Ulväng utgör lagring av information inte en integritetskränkning. Utgångspunkten i denna uppfattning är att informationen redan finns någonstans, exempelvis hos operatörer eller leverantörer och att lagringen inte innebär att någon ny information inhämtas. Det är istället den efterföljande behandlingen av informationen som kan medföra en kränkning av den personliga integriteten.[285] Denna uppfattning har även framförts i utredningen om cyberkonventionen. Utredaren framförde att bevarande av information inte i sig medför en integritetskränkning utan det är den efterföljande ansökan om tillgång till informationen, det vill säga utlämning till en utomstående part, som kan medföra en sådan kränkning.[286] Oftast konstaterar dock lagstiftaren att lagring av information är en inskränkning av den personliga integriteten men en legitim sådan vilket även bekräftas av Europadomstolens uttalanden.[287] Grundlagsskyddet avser intrång i den personliga integriteten, därmed omfattas redan lagring av information eftersom lagring möjliggör åtkomst till informationen för utomstående och insyn i enskildas personliga förhållanden.

Den andra frågan som man måste ta ställning till är huruvida integritetskränkningen är legitim. Inledningsvis kan framhållas att det inte bör vara särskilt svårt att motivera brottsbekämpande åtgärder som innebär inhämtning av information när syftet är att bekämpa allvarlig brottslighet. Som EU-domstolen har konstaterat är dock detta intresse inte ensamt tillräckligt för att motivera omfattande lagring av information om samtliga medborgare.[288]

Användning av beslag och husrannsakan i digitala miljöer har utvecklats genom polisens praktiska arbete vilket innebär att lagstiftaren inte har tagit ställning till dess effektivitet i förhållande till dess konsekvenser för den personliga integriteten. Detta har inte varit nödvändigt eftersom lagstiftningen är teknikneutral. Så länge som inhämtningen har avsett uppgifter som kan ha betydelse för utredningen har källan och metoderna för inhämtningen inte varit nödvändiga att begränsa i lagstiftningen. Rättsutvecklingen kan problematiseras ur ett förutsebarhetsperspektiv, en komponent av legalitetsprincipen och rättssäkerhetsintresset. Jag anser att lagstiftaren bör ta ställning till konsekvenserna av användning av de öppna tvångsmedlen i den digitala miljön eftersom de har en annan karaktär och kan medföra oförutsedda konsekvenser. Den digitala miljön utgörs av en virtuell värld där den enskilda förväntas vara anonym. De flesta människor har någon uppfattning om polisens befogenheter

[285] *Se* avsnitt 2.3.
[286] *Se* avsnitt 4.7.3.
[287] *Se* avsnitt 4.5.3 och 4.6.2.
[288] *Se* avsnitt 4.6.2.

avseende fysiska åtgärder såsom gripande och kroppsvisitation medan polisens befogenheter i den digitala miljön är något mer diffust. Jag tror att många människor har en oro över att bli övervakade och förföljda på internet men hoppas på att inte utsättas för det själv. Internet innehåller omfattande mängd information om enskilda som möjliggör kombination av uppgifter på ett annat sätt än fysiska uppgifter. Det är mycket enklare att skapa sig en helhetsuppfattning om individers beteenden och intressen på internet. I syfte att upprätthålla förutsebarhet och rättssäkerhet bör lagstiftaren uttala sig om användning av tvångsmedel i nya situationer. Enligt mig används argument om rättssäkerhet och legalitet ibland i för stor utsträckning som ursäkter som utnyttjar bristerna och tidsutdräkten i lagstiftningsarbetet. Att påstå att befintliga tvångsmedel inte omfattar digitalt lagrad information och att tvångsmedelsanvändningen annars skulle vara oförutsebar är otidsenligt med hänsyn till samhällets digitalisering och lagstiftningens teknikneutrala karaktär. Legalitetsprincipen samverkar med andra intressen och andra principer. I syfte att upprätthålla effektivitet i lagstiftningen och brottsbekämpningen måste systemet tillåtas viss flexibilitet. Då brottsligheten förflyttas till den digitala miljön måste polisens utredningsåtgärder anpassas till denna miljö.

I beslagsutredningen avseende användning av beslut om husrannsakan och beslag i digitala miljöer har lagstiftaren anfört att undersökning på distans inte innebär ett större integritetsintrång eftersom inhämtning avser samma sorts information som hade kunnat inhämtas med nuvarande lagstiftning. Det enda som skiljer sig är metoden för inhämtningen.[289]

Inhämtning av abonnemangsuppgifter med stöd av LEK har motiverats med att sådana uppgifter inte utgör ett stort ingrepp i den personliga integriteten, i vart fall inte ett ingrepp som väger tyngre än nyttan av uppgifterna i syfte att beivra brott. Även om uppgifterna röjer individens identitet försvåras sådan övervakning av att individer använder sig av dynamiska IP-adresser.[290] Integritetsintrånget som utlämningen medför underskrider den nytta som uppgifterna kan få i brottsutredningssammanhang. I princip menar regeringen att det är en inskränkning som enskilda bör tåla för allmänhetens bästa. Argumentet är hållbart så länge som åtgärden används för det avsedda syftet och följer de begränsningar som finns. Till följd av regleringen om historiska trafikuppgifter innefattar abonnemangsuppgifter flera olika sorters uppgifter som skulle kunna möjliggöra övervakning och kartläggning av individers beteenden. Om det endast tillämpas med de begränsningar som finns i lagen kommer inhämtningen begränsas och därmed även risken för övervakning.

[289] *Se* avsnitt 4.5.2.
[290] *Se* avsnitt 4.6.2.

Inhämtning av information med stöd av hemliga tvångsmedel kan medföra omfattande integritetsintrång, delvis på grund av att innehåll i meddelanden kan avlyssnas men även eftersom det kan medföra omfattande övervakning och kartläggning av individer. Av denna anledning har tvångsmedelsanvändningen avgränsats till att gälla allvarlig brottslighet, i främsta hand brott mot rikets säkerhet. Sexualbrott mot barn verkar inte uppnå kraven på sådan allvarlig brottslighet som föreskriver en möjlighet att använda de hemliga tvångsmedlen även om de kan användas i vissa allvarliga fall. Denna teoretiska möjlighet motsvarar dock inte den praktiska användningen av hemliga tvångsmedel eftersom det i inledningsstadiet sällan kan konstateras att ett visst övergrepp kan leda till sex månaders fängelse. Integritetsintrånget som tvångsmedlen medför bedöms i samtliga lagförarbeten kunna kompenseras genom begränsningar i lag samt säkerhets- och kontrollmekanismer. Trots vissa otydligheter avseende vilka uppgifter som faktiskt kan inhämtas och den något oklara regleringen av historiska trafikuppgifter föreskrivs tydliga förutsättningar för inhämtning av information genom hemliga tvångsmedel vilket främjar rättssäkerhet.[291] Lagstiftarens motiveringar i intresseavvägningar påvisar att personlig integritet underordnas intresset effektiv brottsbekämpning. Det finns dock ingen anledning att ifrågasätta huruvida detta utgör en kränkning mot mänskliga rättigheter eftersom tvångsmedlen har införts lagenligt och objektivt sett träffar samtliga medborgare. I och med att staten tillåts inskränka mänskliga rättigheter för legitima ändamål och den svenska regleringen inte har ifrågasatts avseende dessa tvångsmedel får ingreppet i den personliga integriteten bedömas som legitim.

Generellt kan följande konstateras för samtliga utredningsåtgärder som innebär inhämtning av digital bevisning. Enligt lagstiftaren är inhämtning av digital bevisning med stöd av tvångsmedel och LEK effektiv. I enlighet med Flyghed och Ramberg[292] anser jag att lagstiftarens effektivitetsdiskussioner är bristande, men med hänsyn till utredningsåtgärdernas karaktär ändamålsenliga. Ansvaret avseende effektiv informationsinhämtning läggs på rättstillämparen som är fri att välja egna inhämtningsmetoder. Ett sådant exempel förekommer i regeringens effektivitetsdiskussion i förslaget om hemlig dataavläsning. Tvångsmedlet bedömdes som effektivt trots flera presenterade brister som kan inverka på effektiviteten och inga konkreta förslag på åtgärder av bristerna. Regeringen anförde att ”det får förutsättas att den brottsbekämpande myndigheten som ska verkställa åtgärden har gjort en noggrann kartläggning och analys för att säkerställa att verkställighetstekniken i det enskilda fallet ger tillgång till de uppgifter som eftersöks”.[293] Effektiviteten av ett visst medel är därmed beroende av rättstillämparens kunskaper och förutsättningar.

[291] *Se* avsnitt 4.5.
[292] *Se* avsnitt 2.4.
[293] Prop. 2019/20:64, s. 82.

Regeringens slutsats påvisar den brist som Naarttijärvi påtalade, att regeringen utgår från att myndighetspersonal aldrig gör fel.[294] Det bör dock poängteras att lagstiftaren fångar upp utredningsåtgärder som glider ut för mycket och tillämpas i andra sammanhang i syfte att upprätthålla rättssäkerhet.[295] För att upprätthålla teknikneutralitet och effektiv rättsutveckling måste viss vaghet i lagstiftningssammanhang tillåtas. Lagstiftaren kan dessutom inte förutsäga vilka olika inhämtningsmetoder som kommer krävas inom de närmsta åren med hänsyn till den snabba teknikutvecklingen. Även om teknikneutral lagstiftning utgör ett hot mot rättssäkerheten genom att den är mindre förutsebar anser jag att denna brist måste kunna tillåtas så länge som det framgår klart vad för sorts uppgifter som ska inhämtas, för vilka ändamål och under vilka förutsättningar. Att lämna frågan om lämpliga inhämtningsmetoder till de brottsbekämpande myndigheterna anser jag inte leda till en mindre rättssäker reglering.

Därutöver kan diskussionen avseende intresseavvägningen inte ske med utgångspunkt i att personlig integritet ska upprätthållas till vilket pris som helst eftersom integritetsskyddet inte är en absolut rättighet. Skyddet begränsas delvis till att avse övervakning och kartläggning och kan därutöver begränsas för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Möjligtvis skulle diskussionen ha en annan slutsats om frågan istället handlade om huruvida personlig integritet *bör* vara en absolut rättighet, denna diskussion faller dock utanför uppsatsens frågeställningar. I syfte att upprätthålla det kollektiva samhället som vi lever i och bekämpa brott måste vissa inskränkningar i vår personliga integritet tillåtas, så länge de är lagenliga och proportionerliga och värnar om våra mänskliga fri- och rättigheter. Däremot bör utredningsåtgärder inte motiveras med argument såsom ”har du inget att dölja behöver du inte oroa dig för övervakning” eller att åtgärderna endast kommer träffa brottslingar. Argumenten är provocerande och drabbar olika individer olika då de utgår från en priviligierad majoritet.[296] Alla människor har någonting att dölja, det behöver inte handla om olaglig verksamhet utan kan avse uppgifter om sexuell läggning, hälsa, religiösa eller politiska åsikter med mera, som man inte vill dela med utomstående.

Det skulle därutöver kunna argumenteras för att lagring och inhämtning av enstaka uppgifter, såsom enligt LEK, inte omfattas av skyddet i regeringsformen eftersom det inte utgör sådan övervakning och kartläggning som avses i grundlagen. Jag anser dock att diskussionen om enskilda inhämtningsåtgärder inte kan vara isolerad från övriga åtgärder. En kombination av uppgifter från samtliga operatörer, internetleverantörer och tjänsteleverantörer samt öppet tillgänglig information möjliggör teoretiskt sett identifiering av all

[294] *Se* avsnitt 2.3.
[295] *Se* avsnitt 4.5.2.
[296] *Se* avsnitt 2.3.

kommunikation och därmed omfattande kartläggning och övervakning av individer. Varje enskild inhämtning och lagring av uppgifter utgör en förutsättning för mer omfattande övervakning och ska bedömas och avvägas med stor försiktighet i dess bredare kontext. Övervakningsuppgifter som i lagstiftningssammanhang bedöms som mindre integritetsingripande kan potentiellt medföra omfattande kartläggning.[297] Jag vill påstå att vi i dagsläget inte lever i ett övervakningssamhälle eftersom det inte finns ett sådant syfte, däremot finns det förutsättningar för omfattande övervakning vilket utgör en riskfaktor. Ramberg menar att en demokratisk rättsstat med låg brottslighet inte är tillfredsställande om dess maktutövning missbrukas och därigenom fundamentalt kränker mänskliga rättigheter.[298] I syfte att motverka misstänksamhet mot staten och instabilitet är det därför viktigt att kontroll och redovisning av tvångsmedelsanvändningen sker. Problemet med dagens redovisning är att den endast utgörs av statistiska uppgifter. Det finns därmed ingen möjlighet för en utomstående att försöka skapa sig en bild av tvångsmedelsanvändning i specifika fall. Däremot genomförs kontroller av specifika fall av bland annat Justitieombudsmannen, Justitiekanslern och Säkerhets- och integritetsnämnden. Felaktig tvångsmedelsanvändning kan bringas till allmänhetens och lagstiftarens kännedom och åtgärdas.

Uppsatsen har skrivits med utgångspunkt i viss typ av brottslighet, nämligen sexualbrott mot barn via internet. Det är ett brott som till sin karaktär är avskyvärt och oförsvarligt. Problematiken med sådan brottslighet är att det numera ofta sker digitalt vilket innebär att behovet av digital bevisning är särskilt framträdande vid sådan brottslighet. Sammantaget kan konstateras att polisens utredningsåtgärder som möjliggör inhämtning av digital bevisning fungerar mindre effektivt vid utredning av sexualbrott mot barn via internet. Det är oacceptabelt att tips och anmälningar måste läggas ned på grund av bristande bevisning som i annat fall hade kunnat inhämtas genom hemliga tvångsmedel. De hemliga tvångsmedlen samt förslaget om hemlig dataavläsning har utvecklats till att omfatta internetrelaterad brottslighet, av denna anledning framstår det som mycket besvärligt att några av de mest aktuella internetbrotten som riktas mot barn inte kan utredas tillräckligt effektivt. En anledning till att sådana medel inte omfattar sexualbrott mot barn i tillräcklig utsträckning kan vara avsaknad av kunskap om sådan brottslighet och dess omfattning. Genom att införa brottsrubriceringar som avser digital brottslighet eller specifika brottskoder hos polisen skulle det vara möjligt att föra statistik över och presentera hur omfattande brottsligheten är samt hur många anmälningar och tips som läggs ner på grund av bristande bevisning. Att kunna påvisa sådan statistik och nyttan av digital bevisning verkar i diskussioner om tvångsmedels-användning i lagstiftningssammanhang vara avgörande. Problematiken med

[297] *Se* avsnitt 4.5.3.2.
[298] *Se* avsnitt 2.4.

hemliga tvångsmedel är att de inte kan tillämpas i inledningsstadiet där behovet är störst, på grund av dess påtagliga integritetskränkning.

5.5 Den digitala bevisningens funktion

Den sista frågeställningen avseende den digitala bevisningens funktion kan sammantaget besvaras på följande sätt. Digital bevisning är i de flesta fall en avgörande förutsättning för att kunna utreda och lagföra sexualbrott mot barn via internet. Bevisningen som främst består av abonnemangsuppgifter såsom användar- och inloggningsuppgifter, IP-adresser och telefonnummer har störst betydelse i inledningsstadiet av utredningen eftersom det möjliggör identifiering av en potentiell gärningsperson samt målsäganden. Identifieringen är en förutsättning för tillgripande av andra tvångsmedel och inledande av en förundersökning. Därutöver fungerar digital bevisning som viktig stödbevisning i brottmålsprocessen.

5.6 Slutsats och avslutande kommentar

Sammanfattningsvis kan konstateras att det idag finns en omfattande nationell reglering och ett utarbetat internationellt samarbete som möjliggör inhämtning av uppgifter om elektronisk kommunikation som kan utgöra viktig digital bevisning vid utredning om sexualbrott mot barn via internet. Problemet med de befintliga utredningsåtgärderna är att de sällan kan användas vid sådana utredningar. Detta är problematiskt med hänsyn till att allt yngre barn blir frekventa användare av internet och utsätts allt oftare för sexuella kränkningar. Internet har blivit en ny och mer effektiv plats för sexualförbrytare att kontakta barn i sexuella syften.

Det är svårt att bedöma och uttala sig mer konkret om effektiviteten av polisens utredningsåtgärder för inhämtning av digital bevisning eftersom det inte finns några mätbara faktorer att ta ställning till. Det man kan ta ställning till är att polisen mottar långt fler anmälningar och tips om sexualbrott mot barn och skickar långt fler förfrågningar om information till tjänsteleverantörer vid misstanke om brott än vad som faktiskt leder till åtal. En orsak till detta är brist på bevisning. Det går inte att säga helt säkert huruvida de befintliga utredningsåtgärderna är ineffektiva eftersom de i praktiken sällan kan användas vid utredning av sexualbrott mot barn. De tvångsmedel som har utarbetats i syfte att erhålla tillgång till uppgifter om elektronisk kommunikation har utarbetats i ljuset av brott mot rikets säkerhet och är därmed inte anpassade till den brottsligheten som sker mycket närmare vår vardag. Konsekvensen av detta är att utredningar av allvarliga brott med låga straffminimum, såsom sexualbrott mot barn, mister dessa utredningsåtgärder. Att sänka straffvärdeskraven är dock inte ett alternativ på grund av det integritetsintrång som tvångsåtgärderna

medför. Det bör dock framhållas att polisens möjligheter och metoder att få tillgång till digital bevisning vid sexualbrott mot barn bör få större utrymme i lagstiftningssammanhang. Det allmänna har en absolut skyldighet att skydda barn och har även förutsättningarna till att göra detta. Därmed borde denna typ av brottslighet efterforskas och utredas mer samt oftare lyftas upp i diskussioner om lagstiftning av nödvändiga utredningsåtgärder.

Teknikutvecklingen måste beaktas vid omarbetning av utredningsåtgärder, i annat fall riskerar brottsbekämpningen bli omodern och ineffektiv. Effektivitet i brottsbekämpningen verkar vara ett prioriterat argument i lagstiftnings-sammanhang och väga tyngre än rätten till personlig integritet. Skyddet för personlig integritet är ingen absolut rättighet och avser endast intrång som medför övervakning eller kartläggning av individens personliga förhållanden. Diskussioner avseende om integritetsintrånget är för omfattande bör istället ses i ljuset av frågan huruvida skyddet för den personliga integriteten bör vara mer omfattande. Integritetskränkningar som sker med stöd av lag och som kompenseras genom kontroll- och skyddsmekanismer anses som legitima vilket är en förutsättning för upprätthållande av rättssäkerhet. Tydliga regler som föreskriver polisens utredningsåtgärder som tillämpas lika i lika fall och inte medför oproportionerliga kränkningar av mänskliga rättigheter främjar rättssäkerhet. Det kan argumenteras att förutsebarheten är bristande avseende vilka uppgifter som brottsbekämpande myndigheter faktiskt kan inhämta samt hur externt lagrad information hanteras. Jag anser dock att denna brist är motiverad av intresset att kunna bekämpa sexualbrott mot barn samt behovet av att upprätthålla en flexibel rättsutveckling och effektiv brottsbekämpning. Övervakning av elektronisk kommunikation är en riskfaktor varför intresseavvägningar som dessa är mycket viktiga i lagstiftningssammanhang, särskilt med hänsyn till den fortsatta teknikutvecklingen.

Käll- och litteraturförteckning

Offentligt tryck

Propositioner

Prop. 1988/89:124	Om vissa tvångsmedelsfrågor.
Prop. 1994/95:2	Ökat skydd för barn – Ytterligare åtgärder mot sexuella övergrepp, mm.
Prop. 1997/98:43	Tryckfrihetsförordningens och yttrandefrihetsgrundlagens tillämpningsområden – barnpornografifrågan mm.
Prop. 1999/00:61	Internationell rättslig hjälp i brottmål.
Prop. 2002/03:74	Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering.
Prop. 2002/03:110	Lag om elektronisk kommunikation, mm.
Prop. 2004/05:45	En ny sexualbrottslagstiftning.
Prop. 2005/06:173	Översyn av personuppgiftslagen.
Prop. 2006/07:133	Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, mm.
Prop. 2008/09:149	Vuxnas kontakter med barn i sexuella syften.
Prop. 2009/10:80	En reformerad grundlag.
Prop. 2010/11:46	Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG.
Prop. 2011/12:55	De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation.
Prop. 2013/14:237	Hemliga tvångsmedel mot allvarliga brott.
Prop. 2015/16:68	Förstärkt rättssäkerhet och effektivitet i förundersökningsförfarandet.
Prop. 2017/18:177	En ny sexualbrottslagstiftning byggd på frivillighet.
Prop. 2018/19:86	Datalagring vid brottsbekämpning – anpassningar till EU-rätten.
Prop. 2019/20:64	Hemlig dataavläsning.

Betänkanden

Ds 2005:6	Brott och brottsutredning i IT-miljö.
Ds 2007:13	Vuxnas kontakter med barn i sexuella syften.
SOU 1984:54	Tvångsmedel – Anonymitet – Integritet

SOU 1995:47	Tvångsmedel enligt 27 och 28 kap. RB samt polislagen.
SOU 2000:50	Från tombola till Internet översyn av lotterilagstiftningen.
SOU 2005:38	Tillgång till elektronisk kommunikation i brottsutredningar mm.
SOU 2007:22 del I	Skyddet för den personliga integriteten – kartläggning och analys.
SOU 2007:76	Lagring av trafikuppgifter för brottsbekämpning.
SOU 2009:1	En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen.
SOU 2010:71	Sexualbrottslagstiftningen – utvärdering och reformförslag.
SOU 2013:39	Europarådets konvention om IT-relaterad brottslighet.
SOU 2016:60	Ett starkare skydd för den sexuella integriteten.
SOU 2017:75	Datalagring – brottsbekämpning och integritet.
SOU 2017:89	Hemlig dataavläsnings – ett viktigt verktyg i kampen mot allvarlig brottslighet.
SOU 2017:100	Beslag och husrannsakan – ett regelverk för dagens behov.

Internationella överenskommelser

SÖ 2005:42	Konvention, upprättad av rådet på grundval av artikel 34 i fördraget om Europeiska unionen, om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater. Bryssel den 29 maj 2000.

Litteratur

Abrahamsson, Olle, ”Integritetsskydd med eller utan förnuft”, SvJT 2009 s. 421-434. [Cit. Abrahamsson].

Bring, Thomas, Diesen, Christian & Andersson, Simon, *Förundersökning*, 5 uppl., Norstedts juridik, Stockholm, 2019. [Cit. Bring m.fl.].

Davidson, Julia & Gottschalk, Peter (red.), *Internet child abuse: current research and policy*, Routledge, Abingdon, 2011. [Cit. Davidson & Gottschalk].

Diesen, Christian & Diesen, Eva F, *Övergrepp mot kvinnor och barn – den rättsliga hanteringen*, 2 uppl., Nordstedts juridik, Visby, 2013. [Cit. Diesen & Diesen].

Ekelöf, Per Olof, Edelstam, Henrik & Heuman, Lars, *Rättegång H. 4*, 7 omarb. och rev. uppl., Nordstedts juridik, Stockholm, 2009. [Cit. Ekelöf, 2009].

Ekelöf, Per Olof, m.fl., *Rättegång H. 3*, 8 uppl., Nordstedts juridik, Stockholm, 2018. [Cit. Ekelöf, 2018].

Ekfeldt, Jonas, *Om informationstekniskt bevis*, Juridiska institutionen, Stockholms universitet, Diss. Stockholms universitet, Stockholm, 2016. [Cit. Ekfeldt].

Felaktigt dömda – rapport från JK:s rättssäkerhetsprojekt, Elanders Gotab, Stockholm, 2006. [Cit. Felaktigt dömda, rapport].

Flyghed, Janne (red.), *Brottsbekämpning – mellan effektivitet och integritet. Kriminologiska perspektiv på polismetoder och personlig integritet.*, Studentlitteratur, Lund, 2000. [Cit. Flyghed, 2000].

Flyghed, Janne, ”Kriminalitetskontroll – baserad på tro eller vetande?”, *SvJT*, 2007, s. 59-68. [Cit. Flyghed, 2007].

Frändberg, Åke, ”Om rättssäkerhet”, *JT*, nr. 2 2000/01 s. 269-280. [Cit. Frändberg].

Hettne, Jörgen & Otken Eriksson, Ida (red.), *EU-rättslig metod: teori och genomslag i svensk rättstillämpning*, 2 omarb. uppl., Nordstedts juridik, Stockholm, 2011. [Cit. Hettne & Otken].

Jareborg, Nils, *Straffrättsideologiska fragment*, Iustus, Uppsala, 1992. [Cit. Jareborg, 1992].

Jareborg, Nils, ”Rättsdogmatik som vetenskap”, *SvJT*, 2004, s. 1-10. [Cit. Jareborg, 2004].

Kleineman, Jan, ”Rättsdogmatisk metod” i *Juridisk metodlära*, Nääv, Maria & Zamboni, Mauro (red.), 2 uppl., Studentlitteratur, Lund, 2018. [Cit. Kleineman].

Kronqvist, Stefan, *Brott och digitala bevis: en handledning*, 3 uppl., Norstedts Juridik, Stockholm, 2013. [Cit. Kronqvist].

Kävrestad, Joakim, *Fundamentals of Digital Forensics Theory, Methods, and Real-Life Applications*, Springer International Publishing, Cham, 2018. [Cit. Kävrestad].

Lindberg, Gunnel, ”Straffprocessuella tvångsmedel – några utvecklingslinjer”, *SvJT*, 2007, s. 50-58. [Cit. Lindberg, 2007].

Lindberg, Gunnel, *Straffprocessuella tvångsmedel: när och hur får de användas?*, 4 uppl., Karnov Group, Stockholm, 2018. [Cit. Lindberg, 2018].

Madeleine Leijonhufvud, *Svensk sexualbrottslag. En framåtsyftande tillbakablick.*, Nordstedts Juridik, Stockholm, 2015. [Cit. Leijonhufvud].

Naarttijärvi, Markus, *För din och andras säkerhet: konstitutionella proportionalitetskrav och Säkerhetspolisens preventiva tvångsmedel*, Iustus, Diss. Umeå: Umeå universitet, Uppsala, 2013. [Cit. Naarttijärvi].

Peczenik, Aleksander, *Vad är rätt?: om demokrati, rättssäkerhet, etik och juridisk argumentation*, 1 uppl., Fritze, Stockholm, 1995. [Cit. Peczenik].

Qvarnström Hilding, Agnetha, ”Rättssäkerhet och integritet – hur ser det ut i Sverige? Tankar ur ett åklagarperspektiv”, *SvJT*, 2007, s. 136-140. [Cit. Qvarnström].

Ramberg, Anne ”Tvångsmedel, rättssäkerhet och integritet – går det att förena?”, *SvJT*, 2007, s. 154-170. [Cit. Ramberg].

Reichel, Jane, ”EU-rättslig metod” i *Juridisk metodlära*, Nääv, Maria & Zamboni, Mauro (red.), 2 uppl., Studentlitteratur, Lund, 2018. [Cit. Reichel].

Sandgren, Claes, ”Är rättsdogmatiken dogmatisk”, *Tfr*, Vol. 118, 2005, nr. 4-5, s. 648-656. [Cit. Sandgren, 2005].

Sandgren, Claes, ”Rättsanalytisk metod. En väg framåt?” i Karnell, Gunnar (red.), *Liber amicorum Jan Rosén*, eddy.se [distributör], Visby, 2016. [Cit. Sandgren, 2016].

Sandgren, Claes, *Rättsvetenskap för uppsatsförfattare: ämne, material, metod och argumentation*, 4 uppl., Norstedts Juridik, Stockholm, 2018. [Cit. Sandgren, 2018].

Sutorius, Helena, *Bevisprövning vid sexualbrott*, 2 omarb. och uppd. uppl., Norstedts juridik, Stockholm, 2014. [Cit. Sutorius].

Svedin, Carl Göran & Banck, Lena, *Sexuella övergrepp mot flickor och pojkar*, Studentlitteratur, Lund, 2002. [Cit. Svedin & Banck].

Strömholm, Stig, ”Integritetsskyddet – Ett försök till internationell lägesbestämning”, *SvJT*, 1971, s. 695-736. [Cit. Strömholm].

Ulväng, Magnus, ”Brottsbekämpning, rättssäkerhet och integritet – vad är det som hänt och vad skall vi göra?”, *SvJT*, 2007 s. 1-16. [Cit. Ulväng].

Rapporter och myndighetspublikationer

Brå, *IT-relaterad brottslighet*, rapport 2000:2, Stockholm, 2000. <https://bit.ly/2QTnHdR> Hämtad 2019-11-12.
[Cit. Brå, 2000]

Brå, *Skolundersökningen om brott 2017 – Om utsatthet och delaktighet i brott*, rapport 2018:15, Stockholm, 2018. <https://bit.ly/2QumdYC> Hämtad 2019-10-22. [Cit. Brå, 2017].

Friends nätrapport, 2017. <https://bit.ly/37CXqXU> Hämtad 2019-10-22. [Cit. Friends nätrapport].

PTS, ”Vilka tjänster och nät omfattas av LEK? En vägledning”, PTS-ER-2009:12 <https://bit.ly/2usR3bx> Hämtad 2019-11-22. [Cit. PTS].

Shannon, David, *Vuxnas sexuella kontakter med barn via Internet: omfattning, karaktär, åtgärder*, Brå, Stockholm, 2007. <https://bit.ly/36yhOcy> Hämtad 2019-10-15. [Cit. Shannon].

SIS Teknisk rapport, *Terminologi för informationssäkerhet*, 2015:50, <https://bit.ly/2FyvTLs> Hämtad 2019-11-10.
[Cit. SIS, 2015].

Statens medieråd, *Ungar & medier 2019*, Stockholm. <https://bit.ly/36gqtQl> Hämtad 2019-10-22. [Cit. Ungar & Medier, 2019].

Åklagarmyndigheten, *Beslag: en handbok*, Utvecklingscentrum, Malmö, 2015, <https://bit.ly/2QUGndj> Hämtad 2019-10-29. [Cit. Beslagshandboken].

Åklagarmyndigheten, *Sexualbrott på internet mot unga brottsoffer*, RättsPM 2016:4, Utvecklingscentrum, Göteborg, 2016, <https://bit.ly/2rLUdGm> Hämtad 2019-12-30. [Cit. RättsPM, 2016].

Internationella dokument

Council of Europe, Chart of signatures and ratifications of Treaty 185. <https://bit.ly/2QWCUuz> Hämtad 2019-12-08. [Cit. Chart of signatories and ratifications of Treaty 185].

FN:s kommitté för barnets rättigheter, ”Barnets rätt till frihet från alla former av våld”, allmän kommentar nr. 13, 18 april 2011, CRC/C/GC/13. [Cit. FN, allmän kommentar].

Tidningsartiklar

Jerrstedt Fagerlund, Karin, ”Polisens uppskattning: 20 000 tips om barnpornografibrott i år”, *SvT, 22* juli 2019. <https://bit.ly/2s5SFHn> Hämtad 2019-12-03. [Cit. Jerrstedt].

Sadikovic, Adrian, ”Facebook hjälper svensk polis”, *Sveriges radio,* 26 december 2018. <https://t.sr.se/302nqJH> Hämtad 2019-11-25. [Cit. Sadikovic].

Elektroniska källor

Brå, statistik ”Våldtäkt och sexualbrott”, senast uppdaterad 2019-09-09. <https://bit.ly/35BfgJA> Hämtad 2019-09-27. [Cit. Brå, statistik].

Europol, Internet Organised Crime Threat Assessment (rapport), 2019, <https://bit.ly/37LgOSB> Hämtad 2019-12-13. [Cit. Europol, IOCTA].

Facebook, Användarvillkor, senast ändrad 2019-07-31 <https://bit.ly/2ZYW0Vc> Hämtad 2019-11-25. [Cit. Facebook, Användarvillkor].

Interpol, *Cybercrime*, 2019. <https://bit.ly/35Fby1H> Hämtad 2019-11-12. [Cit. Interpol, Cybercrime].

Kik, ”Information for Law Enforcement” <https://bit.ly/2s5vTzf> Hämtad 2019-11-26. [Cit. Kik, Law Enforcement Information.]

Nationalencyklopedin, skärmdump. <https://bit.ly/2N71esS> Hämtad 2019-09-27.

Snap Inc. Law Enforcement Guide, *Snapchat*, senast uppdaterad 2018-09-21, <https://bit.ly/37LaJWo> Hämtad 2019-11-25. [Cit. Snapchat, Law Enforcement Guide].

WhatsApp, ”Information for Law Enforcement Authorities” <https://bit.ly/2QYc6Kv> Hämtad 2019-11-26. [Cit. WhatApp, Law Enforcement Information.]

Övriga källor

P3 dokumentär, Nätpedofilen i Husby, 10 november 2019 <https://t.sr.se/2T4fjek> Hämtad 2019-11-19. [Cit. P3, 2019].

Telefonintervju, Lena Larsson, gruppchef för IT-relaterade sexualbrott mot barn på Nationellt IT-brottscentrum SC3 på Nationella Operativa Avdelningen, 29 november 2019. [Cit. Larsson, telefonintervju].

Mejlkonversation, Lena Larsson, gruppchef för IT-relaterade sexualbrott mot barn på Nationellt IT-brottscentrum SC3 på Nationella Operativa Avdelningen, 19 december 2019. [Cit. Larsson, e-post].

Rättsfallsförteckning

Tingsrätter
Solna tingsrätts dom den 4 juni 2015 i mål nr. B 8098-13.
Stockholms tingsrätt dom den 4 juli 2019 i mål nr. B 11206-18.

Hovrätter
Hovrätten för Västra Sverige dom den 23 mars 2015 i mål nr. B 4763-14.
Svea hovrätts dom den 1 mars 2016 i mål nr. B 5801-15.
Hovrätten för Västra Sverige dom den 8 juni 2017 i mål nr. B 1293-17.
RH 2018:6.

Högsta domstolen
NJA 1993 s. 616.
NJA 2015 s. 501.
NJA 2018 s. 1103.

EU-domstolen
C-293/12 och C-594/12, Digital Rights Ireland m.fl., ECLI:EU:C:2014:238.
[Cit. Digital Rights]

C-203/15 och C-698/15 Tele2 Sverige och Watson m.fl., CLI:EU:C:2016:970.
[Cit. Tele2 Sverige]

Europadomstolen
K.U. mot Finland, nr 2872/02, dom den 2 december 2008.
[Cit. K.U. mot Finland].