INSTITUTIONEN FÖR TILLÄMPAD IT

HEMLIG DATAAVLÄSNING

Möjligheter och begränsningar för Polismyndigheten

Sofia Adolfsson

André Dahlgren

Martin Hedström

Kandidatuppsats:	15 hp
Ämne:	Informatik
År:	2020
Rapport nr:	2020:091

Sammanfattning

Statlig hacking ökar över världen och i Sverige infördes 1 april 2020 *"Lagen om Hemlig dataavläsning"*. Lagen har givit brottsförebyggande myndigheter såsom Polismyndigheten tillgång till att använda verktyg för att avläsa data innan den krypteras genom att i hemlighet installera mjuk- eller hårdvara i till exempel en dator, mobiltelefon eller surfplatta. Hemlig dataavläsning kan appliceras när straffvärdet överstiger fängelse i två år och först när andra hemliga tvångsmedel visats verkningslösa. Syftet med studien är att undersöka vilka möjligheter och begränsningar som uppkommer vid användning av hemlig dataavläsning inom polismyndigheten. Då lagen inte hunnit tillämpas i någon större utsträckning när studien görs så har undersökningens fokus legat på att undersöka de möjligheter och begränsningar som IT-forensiker, med sin erfarenhet, tror kan uppkomma vid användning av hemlig dataavläsning. Den teori som har använts är teknologiska affordanser som har för avsikt att beskriva interaktionen mellan aktör och objekt i sin omgivning. I studien har teknologiska affordanser använts i en organisatorisk kontext, med flera aktörer involverade. Studien riktar sig mot artefakten hemlig dataavläsning, vars användning inte hunnit dokumenteras och som dessutom är belagd med sekretess. Av den anledningen har teorins specifika inriktning modifierats för att anta ett mer övergripande och kartläggande perspektiv. För att undersöka frågeställningen har en explorativ ansats med kvalitativt perspektiv använts. Insamlandet av data har skett via semi-strukturerade intervjuer, dokumentanalys och en podcast. Analysen av den data som samlats in resulterade i tre teman som är relaterade till möjligheter och utmaningar. De två första handlar om hur brist på kompetens och resurser begränsar användningen av hemlig dataavläsning medan kringgående av kryptering är den stora möjliggörande effekten.

Nyckelord

Tekniska Affordanser, Hemlig Dataavläsning, Statlig Hacking, IT-kompetens, Kryptering, Övervakning, Hemliga Tvångsmedel

Secret Data Reading

Opportunities and restrictions for the Police Authority

Abstract

Government hacking is increasing across the world and in Sweden, on April 1, 2020, the "*Act on Secret Data Interception"* was introduced. The law has given law enforcement agencies such as the Police Authority access to use tools to read data before it is encrypted by secretly installing software or hardware in, for example, a computer, mobile phone or tablet. Secret data reading can be applied when the sentence exceeds prison for two years and only when other secret coercive measures have been shown to be ineffective. The purpose of the study is to investigate the possibilities and limitations that arise when using secret data reading within the police department. Since the law has not been applied to any great extent at the time of the study, the focus of the investigation has been on examining the possibilities and limitations that IT-forensics, with their experience, believe can arise from the use of Secret data reading. The theory that has been used is technological affordances that intend to describe the interaction between an actor and an object in their environment. In the study, technological affordances were used in an organizational context, with several actors involved. The study focuses on the artifact Secret data reading, the use of which has not been documented and which is additionally laid with confidentiality. For this reason, the specific orientation of the theory has been modified to adopt a more comprehensive and mapping perspective. An explorative approach with a qualitative perspective has been used to investigate the issue. The data collection was conducted through semi-structured interviews, document analysis and a podcast. The analysis of the data collected resulted in three themes related to opportunities and challenges. The first two are about how a lack of skills and resources limits the use of secret data reading while bypassing encryption is the major enabling effect.

Keywords

Technological Affordances, Secret Data Interception, Government Hacking, IT-competence, Encryption, Surveillance, Secret Coercive Measures

Förord

Vi vill rikta ett stort tack till alla informanter som tog sig tid och bidrog med värdefull kunskap. Ett extra tack vill vi ge till Birgitta Dellenhed på Polismyndigheten som på ett mycket hjälpsamt sätt förmedlade viktiga kontakter. Vi vill också visa vår tacksamhet till familj och vänner som bidragit med råd och stöd under studiens gång.

Innehållsförteckning

Begreppsförklaring

Anti-forensik — *"Anti-forensik kan beskrivas som de metoder och tekniker vilket används för att försvåra eller förhindra analysen för en IT-forensiker. Andra anti-forensiska metoder mot IT-forensik kan vara kryptering av filer, partitioner eller av en hårddisk."* (Tagesson 2019)

Brute force — "[…] *används när alla andra metoder för att knäcka lösenord misslyckas. Det är en omfattande form av attack och är mycket tidskrävande att knäcka krypterade lösenord. Vid en brute force-attack testar ett program automatiskt kombinationer av stora mängder siffror, ord och bokstäver för att hitta lösenordet."* (IT-säkerhet 2020)

IT-forensik — "[…] *kriminalteknisk undersökning av brottsspår i IT-system. Även: undersökning av it-relaterad brottslighet. Ordet används ibland också i bredare betydelse om brotts-förebyggande åtgärder i it-system. Det används också om undersökningar av orsakerna till allmänna fel i systemet. De som är specialister på it-forensik kallas för it-forensiker."* (IDG u.å.)

Keylogger (Tangentloggare) — "[…] *program eller apparat som (oftast i smyg) registrerar alla knapptryckningar på en dator. Tangentloggare används för att samla in lösenord och användaruppgifter, eller för att kartlägga vilka webbsidor användaren besöker. Det kan vara ett rent datorprogram som rapporterar via internet eller via det lokala nätverket. Det kan också vara en liten dosa som kopplas in på tangentbordets sladd och som smälter in i röran på skrivbordet."* (IDG u.å.)

Kryptering — "[…] *omvandling av ett meddelande från klartext till en form som är obegriplig för obehöriga. Meddelandet omvandlas till kryptotext. Kryptotexten kan sedan skickas till mottagaren som dekrypterar den. Eftersom datorprogram för kryptering behandlar information i digital form, alltså som siffror, kan allt som kan sparas i digital form krypteras, även sådant som musik och bilder."* (IDG u.å.)

Patch	*"En patch är en korrigering eller mindre uppdatering av en programvara. Den byter ut en del av koden*." (IT- säkerhet 2020)
Skadlig programvara	*"*[…] *samlingsbegrepp för oönskade datorprogram eller delar av datorprogram som har utvecklats i syfte att störa IT-systemet, för att samla in information i smyg, eller utnyttjas för ändamål som inte gagnar användaren, såsom utskick av skräppost, intrång på andra datorer eller Denial of Service-attacker. Sabotageprogram installeras på en dator eller ett datornätverk utan administratörens samtycke, eller med ett samtycke som inte innefattar alla aspekter av programvaran."* (Wikipedia 2019)
Trojan	"[…] *program för sabotage, stöld eller dataintrång som smusslas in i en dator, och som sedan lagras och exekveras där, omärkligt för datorns användare."* (IDG u.å.)
Tvångsmedel	"*Tvångsmedel är åtgärder som används i brottsutredande syfte eller för att man ska kunna genomföra en rättegång vid misstanke om brott. De innehåller någon form av tvång mot antingen person eller att man tar egendom i beslag, t.ex. i bevissyfte. Gripande, anhållande och häktning är exempel på tvångsmedel, liksom husrannsakan, kroppsvisitation och beslag. Även hemlig teleavlyssning och liknande räknas som tvångsmedel."* (Åklagarmyndigheten u.å.)
Zero-day	*"*[…] *en sårbarhet för datorprogramvara som är okänd för eller oadresserad av de som borde vara intresserade av att mildra sårbarheten (inklusive leverantören av målprogramvaran). Till dess att sårbarheten åtgärdats kan hackare utnyttja den för att påverka datorprogram, data, ytterligare datorer eller ett nätverk."* (Wikipedia 2020)

1 Inledning

Statlig övervakning har ökat kraftigt, speciellt sedan attacken mot World Trade Center i New York 11 september 2001. Runt om i världen ökade stater omfattningen på den övervakning som sker inrikes (Haikola & Jonsson 2007).

Sen slutet av 1800-talet har vi kunnat kommunicera med fast telefoni och sedan 1938 har det i Sverige funnits lagstöd för hemlig teleavlyssning (Svensk Juristtidning 1992). Genom att överföra gamla lagar till att också verka på internet, har övervakning nått en annan dimension och möjlighet (Haikola & Jonsson 2007). Var gränsen går för vilken övervakning som är okej eller inte ur ett integritetsperspektiv förflyttas ständigt. I Sverige utökades omfattningen av statlig övervakning motiverat av växande hot från organiserad brottslighet, internationell terrorism och hänsynslös brottslighet (Haikola & Jonsson 2007). Ett annat argument som finns för att utvidga gränserna kring övervakning är den snabba tekniska utvecklingen, vilket innebär att staten behöver hänga med både tekniskt och lagmässigt för att möjliggöra en fortsatt övervakning (Haikola & Jonsson 2007).

När mobila kommunikationsenheter med tiden blev vanligare och de lagstöd som fanns för hemlig teleavlyssning inte längre räckte till, blev det svårare för rättsväsendet att utföra laglig avlyssning. Många länder ansåg då att de behövde se över sina lagar (Li, Huang, Lai, Lee & Wu 2018). I Sverige införde man då i rättegångsbalken "*Hemlig avlyssning av elektronisk kommunikation"* som i stora drag innebär att rättsväsendet i hemlighet får avlyssna eller genom tekniska hjälpmedel inhämta meddelanden som skickas till eller från ett telefonnummer eller annan adress. Avlyssningen får endast ske när en person är misstänkt och där straffvärdet är fängelse i två år eller mer (SFS 1942:740, 27 kap. 18 §). I samma kapitel i rättegångsbalken införde man också "*Hemlig övervakning av elektronisk kommunikation"* som i stället för direkt avlyssning innebär att rättsväsendet får möjlighet att i hemlighet inhämta metadata om meddelanden som har skickats eller som skickas till ett telefonnummer eller annan adress. Till exempel vilka enheter som befunnits sig inom ett visst område eller se var en viss enhet befunnit sig eller befinners sig (SFS 1942:740, 27 kap. 19 §). Utvecklingen går fort och även om lagen om hemlig teleavlyssning ändrades och anpassades till lagen om hemlig avlyssning av elektronisk kommunikation, så anser svenska staten att det inte är tillräckligt (Lagrådsremiss Hemlig dataavläsning 2019).

Med smartphones, internet och krypterade nätverk är möjligheterna till diskret kommunikation mycket goda vilket gör att glappet mellan den moderna kommunikationen och laglig avlyssning blir större och möjligheterna för att få fram användbar bevisning vid brott minskar (Li et al., 2018).

1.1 Bakgrund

I det moderna samhället använder många individer teknik som fångar upp daglig aktivitet såsom platser och rörelse (Li et al. 2018). För att upprätthålla en regelrätt balans mellan integritet och nationell säkerhet diskuteras det i vilken utsträckning statlig hacking ska tillåtas. Många organisationer motsätter sig laglig hackning som är godkänd av stater och dess rättsväsenden på grund av den grundläggande rätten till integritet. De oroas även över att hackingteknikerna skulle vara en fara för internetsäkerheten medan stater anser att de känner sig tvungna att använda statlig hacking för att skydda sina länder och invånare (Li et al. 2018).

I de övriga nordiska länderna har det sedan ett par år tillbaka lagstiftas om statlig hacking. I Sverige gjordes en utredning 2017 inför att eventuellt lagstifta om införandet av liknande lag (Delbetänkande av Utredningen om hemlig dataavläsning SOU 2017:89). Utredningen anser att det framförallt är den kraftigt ökade användningen av krypterade appar och enheter som är anledningen till att man bör införa en lag om hemlig dataavläsning. Mer än 90 procent av den internettrafik som avlyssnas vid tiden för utredningen är krypterad (SOU 2017:89).

2019 presenterade regeringen *"34-punktsprogrammet"* med förslag på åtgärder mot gängkriminaliteten med syfte att bekämpa grovt våld och nyrekrytering av unga personer till gäng och olika brottsliga nätverk. Den första punkten i programmet var att genomföra det förslag som lagts fram om hemlig dataavläsning (Regeringen 2019). Lagen trädde i kraft 1 april 2020 och innebär att Polismyndigheten samt andra myndigheter som Säkerhetspolisen, Tullverket och Ekobrottsmyndigheten i hemlighet får installera mjuk- eller hårdvara i till exempel en mobiltelefon, dator eller surfplatta och sedan läsa av datan. För att läsa av den data som genereras vid kommunikation kan till exempel en trojan installeras. Det kan också innebära att myndigheten skaffar sig tillgång till ett konto i sociala medier eller aktiverar kameran eller mikrofonen i en enhet och på så sätt hämtar in rörliga bilder och tal (Justitiedepartement, Faktablad 2019; SFS 2020:89). Lagen kommer att vara tillämpningsbar när straffvärdet är fängelse i mer än två år och lagen är tidsbegränsad till fem år då den ska utvärderas. Hemlig dataavläsning ska användas först när andra hemliga tvångsmedel visat sig verkningslösa (Justitiedepartement, Faktablad 2019).

1.2 Problemområde

Eftersom lagen är ny och de faktiska effekterna av dess införande inte går att utläsa än finns det inga studier på vilka möjligheter och begränsningar som uppkommer vid hemlig dataavläsning. Det är också relativt okänt vilka tekniker och tillvägagångssätt som kommer att användas vid applicering av tvångsmedlet. Därför finns det en kunskapslucka och ett behov av att studera den teknik och de tillvägagångssätt som kommer att användas, samt att titta på de antaganden som erfarna tjänstemän inom Polismyndigheten har om det nya hemliga tvångsmedlet. Brottsförebyggande Rådet (2016) menar att det är oklart utifrån tidigare rapporter på området om polisens kapacitet gällande brott med IT-inslag nyttjar de resurser som i nuläget redan finns och om ett nytt tvångsmedel möjliggörs eller begränsas av redan existerande faktorer. Det finns även en förlegad syn på IT inom polisen där det ses som en stödjande verksamhet och inte en möjliggörare. Samhället har gått vidare till att vara

ett informationssamhälle och det ställer nya krav på polisiära metoder (Brottsförebyggande Rådet, 2016).

1.3 Syfte och frågeställning

Syftet med studien är att undersöka vilka möjligheter och begränsningar som IT-forensiker anställda inom Polismyndigheten förväntar sig kommer att påverka användningen av tvångsmedlet hemlig dataavläsning. Då lagen som reglerar användning av tvångsmedlet inte hunnit tillämpas i någon större utsträckning när studien genomförs så kommer undersökningen inte att behandla de faktiska möjligheter eller begränsningar som IT-forensiker upplever, utan istället de möjligheter och begränsningar som de *förväntar sig* kan uppkomma, utifrån den erfarenhet de har som tjänstemän.

Med tanke på studiens omfång och problemområde förväntas inte ett generaliserbart resultat uppnås. Istället ämnar studien att ge en djupare förståelse för det behandlade fenomenet samt att skapa en språngbräda för ytterligare forskning och kunskapsinhämtning.

Studiens övergripande frågeställning:
Vilka möjligheter och begränsningar ger det nya tvångsmedlet hemlig dataavläsning för polisen vid utredning av brott?

Ovanstående fråga delas upp i två mer konkreta frågeställningar enligt nedan:
Vad möjliggörs vid användning av tvångsmedlet hemlig dataavläsning?

Vilka begränsande faktorer påverkar användningen av tvångsmedlet hemlig dataavläsning?

1.4 Avgränsningar

Planen inför studien var att intervjua personer som kommer att arbeta operativt med det hemliga tvångsmedlet. Hemlig dataavläsning kommer att användas av Polismyndigheten genom utredningsenheten vid Nationella Operativa Avdelningen (NOA), sektionen för särskilda insatser (Cordner 2020). Försök gjordes för att få kontakt med informanter att intervjua som arbetar på NOA men de gav ett avböjande svar via Polismyndighetens kommunikationsavdelning med hänvisning till att de inte kommenterar förmåga och användning av hemlig dataavläsning.

Även en del delvis oavsiktlig avgränsning har skett, då det initialt under studiens gång fanns förhoppningar om att få mer konkret information om den teknik som används vid hemlig dataavläsning och därigenom en mer tekniskt inriktad studie. På grund av sekretess har informanter varit tvungna att avböja frågor bland annat rörande organisatorisk struktur, teknik kring hemliga tvångsmedel samt handläggning av hemliga tvångsmedel. Därför har studien istället behandlat tvångsmedlet ur ett explorativt och organisatoriskt perspektiv i ett försök att fånga upp de kringliggande faktorer som påverkar användningen av tvångsmedlet.

Till sist har studien endast helt översiktligt berört integritetsfrågan. I sammanhanget statlig hacking är det en viktig fråga att behandla men då studien gjorts ur ett organisatoriskt perspektiv har det inte funnits utrymme till den inom föreliggande studies tidsram. Studiens författare uppmanar dock framtida forskare att undersöka tvångsmedlet mer utförligt ur ett integritetsperspektiv.

1.5 Disposition

Relaterad forskning och teoretiskt ramverk presenteras i avsnitt två. I avsnitt tre redovisas motivering till vald metod samt en presentation av använt material. Avsnitt fyra presenterar det insamlade resultatet och följs av avsnitt fem som redovisar en analys av resultatet samt en diskussion. I avsnitt fem presenteras också studiens praktiska och teoretiska implikationer samt reflektion kring studiens genomförande och resultat. Som avslutning beskrivs i avsnitt sex studiens sammanfattande slutsats.

2 Relaterad forskning och teoretiskt ramverk

I följande avsnitt presenteras först den relaterade forskning som har anknytning till problemområdet och sedan det teoretiska ramverk som används för att analysera studiens resultat.

2.1 Relaterad forskning

Nedan presenteras relaterad forskning med relevans för studien. Brottsförebyggande rådets rapport om IT-relaterad brottslighet som också använts i dokumentanalysen behandlas kort. Sedan etableras forskning om integritet, hacking och till sist om gapet mellan teknik och lagstiftning.

2.1.1 IT-inslag i brottsligheten och rättsväsendets förmåga att hantera dem

Brottsförebyggande rådet (Brå) är en myndighet som arbetar för att tryggheten i samhället ska öka och brottsligheten minska. I publikationen, *IT-inslag i brottsligheten och rättsväsendets förmåga att hantera dem, 2016:17 (2016)*, har syftet varit att genomföra en studie på uppdrag av regeringen. Med bakgrund av att det saknas sammanställd information om hur utvecklingen har sett ut och vilken kompetens och kapacitet som finns för att hantera brott med IT-inslag, så belyser rapporten de brister som finns vid hantering av brott med IT-inslag hos brottsförebyggande myndigheter. Studien använder svar från intervjuer och enkäter som skickats till IT-undersökare, åklagare och förundersökningsledare inom polismyndigheten. Publikationen har vetenskapligt granskats av professor emeritus Sven-Åke Lindgren, Göteborgs universitet.

Rapporten beskriver att den snabba tekniska utvecklingen och det ökande internetanvändandet haft stor inverkan på de brottsförebyggande myndigheternas arbete. Brott med IT-inslag ökar kraftigt och så även IT-beslag. I alla typer av brottslighet finns nu IT som en del av brottsverksamheten. Effekten av det är att behovet av IT-forensiskt stöd i utredningar bara kommer att öka. Att den tekniska utvecklingen och dess påverkan på brottsutredningar inte har prioriterats mer har det länge funnits frustration kring. En av anledningarna kan vara att många beslusfattare har kvar en förlegad syn på IT-brott och ser dem som enbart brott med IT som mål, rena IT-brott (Brå 2016). I rapporten kan man se att det är brist på vidareutbildning inom IT och att kunskapen om hur man säkrar IT-bevisning är låg. IT-relaterade delar av brottsutredningar sker helt utan struktur och de som är ansvariga är utelämnade åt eget nätverk och kompetens. Dessutom saknas det tillräckligt med kunskap kring det stöd som finns hos expertfunktioner. I rapporten kan man också läsa om en hög arbetsbelastning hos IT-undersökare, att det blir som en flaskhals i den IT-forensiska processen där utredningar läggs på hög. Det behövs också satsning

på system och teknisk utrustning där det när rapporten skrivs finns en brist och ett problem som utgör ett hinder för IT-undersökare, förundersökningsledare och åklagare. Slutsatsen som dras är att de satsningar som gjorts på IT-området inte är tillräckliga och att åtgärder för att höja kompetens och kapacitet är brådskande för att kunna säkra rättssäkerhet och effektivitet. De poängterar också i rapporten att det är viktigt att det inte blir en engångsåtgärd utan ett kontinuerligt arbete, så att satsningarna på IT-området hänger med i samma takt som utvecklingen (Brå 2016).

2.1.2 Att omdefiniera integritet

Medborgarnas integritet är en central fråga vid all statlig övervakning. Daniel Solove försöker i sin artikel *A taxonomy of privacy* (2006) omklassificera begreppet integritet och hur det, trots all diskussion kring begreppet, inte verkar finnas en klar bild av vad integritet faktiskt innebär. Solove (2006) vill därför med sin artikel omklassificera integritet och skapa ett ramverk för det rättsliga systemet för att bättre förstå integritet. Vid Soloves (2006) skrivande av artikeln är inte rättssystemet uppdaterat till informationssamhällets tidsålder. Vilket enligt Solove (2006) har lett till att många domstolar och beslutsfattare inte ens uppfattar att det finns ett integritetsproblem. Klassificeringen är således ett försök att hjälpa rättssystemet att närma sig, förstå och balansera åtgärder i informationssamhällets allt större problemområde rörande just integritetsfrågor.

För att göra detta utgår klassificeringen ifrån de aktiviteter som inkräktar på integriteten. Artikeln försöker sätta fokus på dessa potentiellt problematiska integritetskränkande aktiviteter och inte på integritet i sig. Genom att fokusera på de problematiska aktiviteterna kan klassificeringen enligt Solove (2006) ge lagstiftare en klarare bild av hur lagar kan skapas balanserade mellan behovet av integritet och behovet av nödvändiga åtgärder som kränker integriteten. Artikeln identifierar fyra områden som involverar potentiellt problematiska integritetskränkande aktiviteter: informationssamlande, informationsbearbetning, informationsspridning och intrång (Solove 2006). Studiens empiri utgår ifrån tidigare forskning och lagtext. Studien menar att amerikansk grundlag och praxis halkat efter informationsamhällets tidsålder och behöver granskas efter vad kritiska röster säger gällande integritet.

Slutsatsen blir att lagstiftare måste anpassa sig till den allt modernare världens större informations- och teknikmöjligheter. De bör dock inte enligt Solove (2006) behandla integritet för försiktigt utan förhålla sig till att det bör beaktas men att ibland krävs intrång från statens sida. Det är en balansgång, som visserligen är svår att applicera med avseende på hur amerikanska lagar ser ut, men som bör beaktas även här i EU och Sverige vid införandet av nya hemliga tvångsmedel.

2.1.3 Hacking - en organisatorisk resurs

Hacking innebär bland annat otillåten modifiering av programvara. Allt eftersom IT-sektorn vuxit har mängden hackare ökat. Flowers (2008) menar att det beror på en samtidig ökning av högkompetenta IT-arbetare. Dessa arbetare har förmåga och erfarenhet som lämpar sig väl för hacking. Hackare och de som använder deras modifierade eller skapade programvara på ett sätt som medvetet bryter mot lagar, regler eller andra organisationers skapade begränsningar benämns av Flowers (2008) som *Outlaw Users*. Innovationsprocessen att modifiera och skapa den här typen av utomlaglig programvara klassas som *Outlaw Innovation*. Flowers (2008) anser att

den företeelsen, precis som användare och externa innovationsprodukter, kan vara en resurs för organisationer på flera olika sätt och ställer upp fem kategorier som definierar hur organisationer kan tillgängliggöra sig detta.

Monitor eller observera innebär att att följa utomlagliga användares aktiviteter noga för att reagera mot eller ta över resultatet.

Adapt eller anpassa beskriver hur organisationer anpassar sig efter eller kopierar teknologier, metoder eller andra innovationer som utvecklats av utomlaglia användare.

Influence eller påverka innebär att organisationen försöker styra på vilket sätt utomlagliga användare utför aktiviteter relaterade till organisationens produkter. Detta kan ske genom incitament, dialog eller öppen källkod.

Absorb eller absorbera innebär att om de förmågor och kunskaper som hackare besitter är ovanliga eller kompletterande kan organisationen försöka rekrytera eller på andra sätt se till att kompetensen används enligt organisationens mål och regler.

Till sist anges kategorin *Attack* vilket innebär att organisationen med någon form av aggression, oftast juridisk, försöker att stänga ner de utomlagliga användarnas aktiviteter.

Organisationer kan använda sig av dess former av bemötande för sig själva eller i kombinationer beroende på vad som passar bäst för just deras situation eller produkt (Flowers, 2008).

2.1.4 Gapet mellan teknisk utveckling och reglering

Ny teknik ställer nya krav på samhället. Bör man hämma innovation för att försöka minska de negativa effekter som kan springa ur det som kallas disruptiv innovation? Den frågan ställer Fenwick, Kaal och Vermeulen i artikeln *Regulation tomorrow: What happens when technology is faster than the law?* (2017). De menar i artikeln att beslutsfattare står inför svåra val när teknologins utveckling går snabbare än rättsväsendets maskinerier för att skapa balanserade regleringar för dess användning. Artikeln tar upp hur den digitala utvecklingen i en exponentiell takt ställer nya krav på lagstiftare. Något som enligt Fenwick, Kaal och Vermeulen (2017), gör att lagstiftare ofta finner sig i en situation där förordningarna blir antingen strikta utan att baseras tillräckliga fakta eller en brist på åtgärder i brist på tillräckliga fakta. Hur och var bör samhället dra gränser för innovation? Är de lagar och förordningar samt de mekanismer som stiftar dem föråldrade? Enligt Fenwick, Kaal och Vermeulen (2017) behöver de lagstiftande mekanismerna bli mer proaktiva, dynamiska och framförallt lyhörda för att kunna hänga med i utvecklingen.

"*In an age of constant, complex and distruptive technology innovation knowing, what, when and how to structure regulatory interventions has become much more difficult*" (Fenwick, Kaal & Vermeulen 2017, s. 581-582).

De har exempel via statistiska underlag som visar bland annat på kraften hos datadrivna operationer och hur de stora mängder data som samlas in via exempelvis företaget *Pitchbook* kan användas för att se vilka typer av teknologi det görs

investeringar i, vilket i sin tur pekar på områden som kommer att utvecklas snabbt. Detta för att snabbare kunna omfokusera förordnings- och lagarbete till att agera mer dynamiskt och sätta sig in i det specifika området (Fenwick, Kaal & Vermeulen 2017). Artikeln har ett fokus på innovation och förordningar ur ett kommersiellt perspektiv. Däremot är debatten kring hur förordningar och lagar stiftas idag i förhållande till hur snabbt de kanske behöver kunna omformuleras för att tillmötesgå nya krav ställda av nya utmaningar viktig. Staten och Polismyndigheten hamnar idag i en reaktiv position mot ny teknik och de nya utmaningar det innebär, men bör inte för den sakens skull gå för proaktivt framåt heller. En riskerar utan adekvat underlag att hamna i en av de två fallgroparna Fenwick, Kaal och Vermeulen (2017) identifierar: överreaktion eller passivitet.

2.2 Teknologiska affordanser

Begreppet teknologiska affordanser är ämnat att beskriva interaktionen mellan en aktör och ett objekt i sin omgivning och kan beskrivas som potential till ett beteende hos en måldriven aktör. Hädanefter används för läsbarhetens skull helt enkelt *affordanser*. Teorin är ursprungligen menad att undersöka enskilda objekt hanterade av en enskild aktör men har genom applicering mot mer komplexa informationsteknologiska artefakter utvecklats och kompletterats för att undersöka användning av artefakter som informationssystem i en organisatorisk kontext, med flera aktörer involverade. Föreliggande studies problemområde riktar sig mot en artefakt, hemlig dataavläsning, vars användning inte finns dokumenterad och dessutom är sekretessbelagd, varför teorins specifika inriktning har modifierats för att appliceras mer övergripande och kartläggande. Mer konkret om teorins applicering i studien presenteras först i avsnittet Metod och senare under Diskussion, där appliceringen faktiskt sker.

Nedan redogörs för affordansteorins grunder, utveckling och rekommenderad användning enligt Volkoff och Strong (2018). Till sist görs en kritisk bedömning av teorin generellt samt mer specifikt i förhållande till föreliggande forskningsfråga.

2.2.1 Affordans-teorins grunder

Teorin definierades i sitt ursprung av Gibson (1977, 1979 se Volkoff & Strong 2018) för att beskriva tanken att en målorienterad aktör uppfattar ett föremål efter hur det kan användas snarare än som en uppsättning egenskaper som hör till det enskilda föremålet oberoende av aktören. De sätt på vilka föremålet kan användas, dess affordanser, uppfattas direkt, utan en analys av föremålets egenskaper. Dessutom existerar dessa affordanser oberoende av om aktören uppfattar dem eller inte. En stol, till exempel, ger enligt Volkoff och Strong (2018) en vuxen människa affordansen att sitta och detta är inte beroende av om personen medvetet analyserar stolens höjd, stabilitet eller styrka.

Debatter uppstod kring detta begrepp och vad affordanser egentligen är. Vissa menade att de är en egenskap hos omgivningen medan andra tyckte att de är relationella och uppstår i samspelet mellan varelse och miljö. En tredje syn menade att affordanser är just dessa relationer mellan miljö och varelse snarare än att de springer ur relationerna. Till slut gick två ledande forskare ihop och presenterade en kombination av sina tidigare ståndpunkter enligt följande:

"...affordanser är framträngande relationella egenskaper hos djur-omgivningssystem [samspelet mellan ett djur och dess omgivning, reds anmärkning]" (Chemero & Turvey 2007 se Volkoff & Strong 2018, s. 233)

Affordansbegreppet användes under den här tiden, och så även i nutid, på flera olika, och ofta motsägande, sätt. Vad gäller teknologirelaterade fält är dock det centrala användningssättet för begreppet nära det som Chemero och Turvey presenterat, att affordanser uppstår ur relationen mellan användare och teknologi (Volkoff & Strong 2018).

Gibsons affordansteori applicerad inom informatiken ger ett perspektiv som möjliggör en analys av specifik teknik i förhållande till social och kontextuell påverkan (Volkoff & Strong 2018). I samband med teorins användning inom informatik har det dykt upp nya behov i förhållande till hur affordanser uppstår vid användning av artefakter i organisationer och i grupp. Nya konstruktioner, som delade och kollektiva affordanser (Leonardi 2013 se Volkoff & Strong 2018) etableras för att försöka mätta detta behov. Affordans-perspektivet har använts för att studera organisatoriska förändringar och rutiner på flertalet olika sätt. Perspektivet har till exempel applicerats på studier om hur användning av social media inom organisationer påverkar socialisering, kunskapsdelning och maktutövning. Affordanser har också använts för att undersöka mjukvaruutveckling. Denna spridda användning har i mångt varit inkonsekvent och ibland motsägande. Ett av skälen till detta är att användningen inom informatik har tagit Gibsons teori, som var riktad mot en enda aktör, och placerat den i ett kollektivt eller organisatoriskt sammanhang. Artefakterna som undersökts har ändrat natur från enskilda objekt till komplexa och svårförstådda sådana. Denna förändring har lett till en utökning av teorin. Strong et al. (2014 se Volkoff & Strong 2018) har identifierat tre huvudsakliga problemområden gällande denna nya användning av affordansteorin:

För det första behövs en åtskiljning mellan affordansen (möjlighet till måldriven handling), aktualiseringen (den handling som faktiskt utförs) och resultatet av handlingen.

För det andra hör aktörer till grupper, organisationer och olika konstellationer, alla (inklusive aktören själv) med olika mål. Strong et al. (2014 se Volkoff & Strong, 2018) avgränsar målet till det direkta och konkreta resultatet av en uppgift som utförs under affordansens aktualisering.

För det tredje och sista är det inte bara flera aktörer som använder komplexa objekt, det uppstår dessutom flera affordanser och grupper, eller kluster, av affordanser under interaktionen mellan en aktör och en artefakt. Aktualiseringen av affordanser sker inte i ett vakuum varför samspelet mellan dessa affordanskluster samt affordanserna i dem bör beaktas och begrundas.

Utifrån dessa tre problemområden föreslår Strong et al. (2014 se Volkoff & Strong 2018, s. 235) en definition som tar hänsyn till begreppet affordanser i organisationer:

"*An affordance is the potential for behaviours associated with achieving an immediate concrete outcome and arising from the relation between an artifact and a goal-oriented actor or actors.*"

Översatt till svenska kan definitionen skrivas ut som följer:

En affordans är beteendet associerat med att uppnå ett direkt och konkret resultat och uppstår ur relationen mellan en artefakt och en eller flera målorienterade aktörer.

Med definitionen och dess bakgrund etablerade presenteras i följande avsnitt de rekommendationer som Volkoff och Strong (2018) ger kring hur affordansteorin bör appliceras i informationsteknisk forskning.

2.2.2 Affordanser som applicerat teoretiskt ramverk

Volkoff och Strong (2018) föreslår sex principer för användning av affordansteorin i informatikforskning.

Princip 1: *Kom ihåg att en affordans uppstår ur relationen mellan användare och artefakt, inte från en fristående artefakt.*

Det är lätt att hamna i ett språkbruk och en argumentation som behandlar affordanser som att de är samma sak som teknologins eller artefaktens funktioner. En teknisk artefakt har inga affordanser förutom i relation till en måldriven aktör. Med det sagt kan aktören vara en tänkt symbolisk aktör med fördefinierade uppgifter relaterade till ett specifikt mål.

Princip 2: *Var noga med att särskilja affordansen från dess aktualisering.*

Distinktionen mellan affordansen och dess aktualisering är kritisk. Affordansen, som är potentialen för handling driven av en aktörs mål, syftar mot funktion. Vad affordansen är användbar till och syftet med handlingen. En affordans är med andra ord potentialen för att uppnå ett resultat. Definitionen blir därmed abstrakt och appliceras på flera olika potentiella aktörer med samma mål och motsvarande förmågor. Aktualiseringen, den faktiska handlingen, är specifik och relaterar till struktur snarare än funktion. Strukturen är här den faktiska uppsättning av beteenden som bildar handlingen (Burton-Jones & Gallivan 2007; Morgeson & Hofmann, 1999 se Volkoff & Strong 2018). Där affordanser representerar möjliga handlingar och det syfte de är menade att uppnå, är aktualiseringen specifika handlingar som kommer att, eller har, genomförts av en specifik individuell aktör.

Princip 3: *Fokusera på handlingen, inte det stadie eller tillstånd som nås när den utförts.*

Affordanser handlar om potentiell handling, inte om det som uppnås när handlingen utförts. Det direkt konkreta resultatet är det tillstånd som uppnås när affordansen aktualiserats. Volkoff och Strong (2018) menar att om fokus läggs på resultatet skiljer sig forskningen inte nämnvärt från forskning kring påverkan, och viktigast, så förloras det som affordansteorin främst bidrar med, förståelsen för rollerna hos teknologi och användarens handlingar. För att hitta rätt föreslår de att affordanser benämns som verb i particip, exempelvis sittande eller kommunicerande.

Princip 4: *Välj en rimlig nivå av finkornighet.*

Den tidigare nämnda definitionen av affordanser säger inget om vilken finkornighet som är lämplig. Affordanser är grupperade och underordnade varandra på olika sätt. Ett exempel som ges av Gibson via Volkoff Strong (2018) är ett äpples affordanser. På en nivå ger äpplet en människa affordansen ätande, som i sin tur, på en lägre nivå, ger affordanserna bitande, tuggande och sväljande. På samma sätt ger ett mailsystem en individ den generella affordansen kommunicerande men också de underliggande möjligheterna att först skriva och sen skicka ett meddelande. Den lämpliga analysnivån avgörs beroende på vad som undersöks.

På samma sätt som affordanser kan vara underliggande kan de också aggregeras ihop till en högre, mer abstrakt nivå. Volkoff och Strong (2018) menar att det är på den här mer abstrakta nivån som det blir svårt att skilja mellan potential för handling och det tillstånd som handlingen resulterar i. De ger exemplet "visibility" eller "synlighet" som ofta benämns som en affordans. Istället vill de definiera "synlighet" som ett tillstånd som uppnås genom andra affordansers aktualisering. När "synlighet" används som en affordans maskeras både associerade handlingar och aktörer. De inblandade aktörerna är av två typer, dels den som tillgängliggör information dels den som tar emot den. Den förra kan, genom att "mata in data" under genomförandet av "tillgängliggörande av information" utföra olika typer av aktiviteter: "avslöjande av information" (ibland oavsiktligt), "berättande" (avsiktligt) eller "marknadsförande/propagerande" (aktivt). På samma sätt kan mottagaren när denne "får åtkomst till information" göra det genom "observerande", "övervakande" eller "undersökande". Volkoff och Strong (2018) poängterar att tillståndet "synlighet" kan vara ämne för många intressanta forskningsfrågor även utan att vara en affordans. De menar att detta är en av affordanslinsens fördelar, att den bidrar till att peka ut de aktörer som är inblandade och variationen i de potentiella handlingar de kan tänkas utföra när de använder en teknologi eller artefakt.

Princip 5: *Identifiera framträdande affordanser samt hur de interagerar.*

Utöver de aggregat av affordanser som nämns ovan har affordanser, och grupperingar/aggregat av affordanser interaktioner och relationer sinsemellan utan att de hör till samma aggregat eller gruppering. Vid forskning kring system och andra komplicerade artefakter är det enligt Volkoff och Strong (2018) av stort intresse att undersöka dessa interaktioner mellan olika affordansgrupperingar.

Princip 6: *Identifiera sociala krafter som påverkar aktualiseringen av affordanser.*

Affordanser aktualiseras i en social kontext. Därmed följer enligt Volkoff och Strong (2018) att sociala krafter sprungna ur grupper som aktörer tillhör eller agerar inom påverkar hur, hur bra och om affordanser alls aktualiseras. Utöver analys av traditionella sociala mekanismer som grupp- och kulturnormer (Bloomfield, Latham & Vurdubakis, 2010 se Volkoff & Strong 2018) bör det också undersökas hur närvaron av andra aktörer som använder samma artefakt med liknande syfte påverkar en aktörs beteende. Leonardi (2013 se Volkoff & Strong, 2018) gör skillnad på individuella, delade och kollektiva affordanser, vilket bidrar till ökad klarhet kring interaktionen mellan affordanserna och aktörerna. Individuella affordanser aktualiseras av en aktör som agerar oberoende av andra. Delade affordanser är samma affordans aktualiserad av flera aktörer på liknande sätt. Kollektiva affordanser aktualiseras av flera aktörer som utför olika handlingar för att uppnå ett

gemensamt mål. För IT-artefakter i en organisatorisk kontext är delade och kollektiva affordanser viktiga. Oavsett om det som studeras är individuella, delade eller kollektiva affordanser bör samlingar av affordanser och hur de interagerar undersökas.

Utöver dessa sex principer tar Volkoff och Strong (2018) också upp tre problematiker som inte har klara riktlinjer men som bör begrundas noga.

Problem 1: *Måste affordanser vara uppfattade för att aktualiseras?*

Vid teorins tidiga användning låg fokus på att förstå hur aktörer uppfattar artefakter i sin omgivning. Det är en teori om och en definition av hur uppfattning fungerar. Behållningen från den tidiga appliceringen var att aktörer i allmänhet uppfattar sin omgivning intuitivt, genom affordanser, potential till handling, snarare än genom kognitiv analys. Trots fokus på uppfattning menades det att affordanser inte måste vara uppfattade för att aktualiseras. Volkoff och Strong (2018) menar att detta leder till två betänkanden. Det första är att uppfattning eller uppfattningsförmåga måste definieras noggrant. Det engelska ordet som används, *perception* kan betyda allt från medveten kognitiv uppfattning till undermedveten intuitiv sådan. Särskiljningen är viktig eftersom teorins tidiga användning pekade på att vi generellt uppfattar saker mer intuitivt. Det andra betänkandet är att en aktör kan aktualisera en affordans utan att vara medveten om dess existens, ens på en intuitiv nivå. Till exempel kan en person som använder Facebook och medvetet aktualiserar en kommunicerande affordans genom att lägga upp något riktat till sina vänner utan att justera sekretessinställningar, samtidigt aktualisera en publicerande affordans eftersom vänners vänner och vänners vänners vänner kan se inlägget om det interageras med.

Trots att, som synes ovan, en aktör inte måste uppfatta en affordans för att aktualisera den, kan det ändå mycket väl vara så att medveten aktualisering gör aktören mer effektiv i sitt användande av en artefakt. Detta kan leda till en rad intressanta forskningsfrågor kring avgörande nivåer av medvetande för effektiv användning, eller typer av affordanser där omedveten användning troligen kan förekomma. Den typen av analyser kan medverka till att förklara eller förändra oväntade skeenden vid användning av artefakter. Med tanke på ovanstående menar Volkoff och Strong (2018) att termen "uppfattade affordanser" bör undvikas. Dels på grund av att teorin i grunden handlar om uppfattning, dels på grund av att uppfattning, eller den engelska termen *perceived* betyder många olika saker. Istället föreslår de termen medvetandenivå som en mer precis definition.

Problem 2: *Är affordanser möjliggörande och begränsande eller enbart möjliggörande?*

Det finns exempel som stödjer båda perspektiven. Till stöd för "bara möjliggörande"-perspektivet är att själva ordet *affordance* är positivt laddat och dessutom verkar det inte helt troligt att en aktör medvetet skulle aktualisera en affordans som begränsar dennes handlingar. Zammuto et al. (2007, s752 se Volkoff & Strong, 2018) stödjer dock "möjliggörande och begränsande" och uttrycker det såhär:

"Ett affordansperspektiv erkänner hur materialiteten hos ett objekt främjar, formar, eller bjuder in, och på samma gång begränsar en uppsättning specifika användningssätt".

Volkoff och Strong (2018) håller med och menar att affordanser förkroppsligar både möjliggörande och begränsande. När något möjliggörs blir något annat samtidigt begränsat helt enkelt eftersom de två är inkompatibla och eftersom de båda aspekterna inte går att separera. Ett lås på en dörr ger till exempel en aktör en barrikaderingsaffordans vilket är möjliggörande om aktörens syfte är att stänga ute andra och att få vara ifred. Å andra sidan kan affordansen ses som begränsande eftersom låset gör det svårare att fly om aktören känner sig hotad i sitt eget hem. På samma sätt kan användningen av ett enterprise resource planning system för att aktualisera en datainmatnings-affordans möjliggöra för aktören att dokumentera dagens aktivitet men samtidigt begränsa samma användare från att dölja sin långa lunchrast.

Problem 3: *Hur kapabel måste en aktör vara för att en affordans ska vara applicerbar?*

Affordansteorin inbegriper att den involverade är "kapabel" att aktualisera affordansen. Volkoff och Strong (2018) ställer frågan om det betyder fysiskt kapabel eller om det också kräver kunskap om hur handlingen ska utföras? I den tidiga användningen av teorin var artefakterna som undersöktes enkla fysiska objekt så fysisk förmåga spelade större roll än färdighet och kunskap. Volkoff och Strong (2018) argumenterar att om en användare placeras framför ett okänt nytt system finns affordanser trots att användaren saknar kunskap. Kunskap menar de, är inte en binär företeelse utan något som är i ständig förändring och utvecklas med tiden. Aktörens aktualisering av affordanserna kan ske mindre effektivt till en början men över tid och med träning och utbildning ökar dennes färdighet och därmed också hur effektivt affordansen aktualiseras. På samma sätt som affordanser existerar oavsett om aktören är medveten om dem eller inte, så existerar de också oavsett om aktören har vetskap om hur de aktualiseras eller inte, så länge den fysiska förmågan är tillräcklig. Detta gör det bland annat enklare att ställa frågor relaterade till kompetensutveckling och dess resultat.

2.2.3 Kritik mot affordans-teorin

Utöver de problem som Volkoff och Strong diskuterat, och som presenterats ovan har studiens författare identifierat följande problem med affordansteorin: den är akademiskt och abstrakt i sin natur till en så hög grad att den blir svårtillgänglig för dem som inte är akademiskt verksamma eller har satt sig in i teorin. Detsamma kan gälla flera teorier men studiens författare anser det iögonfallande att en teori med målet att förklara interaktionen mellan en användare och ett objekt, något som för de allra flesta ter sig relativt enkelt att förstå, gör det på ett sätt som med tiden har blivit så pass abstraherat att det är svårt att förklara teorin annat än i dess egna termer. När teorin ska appliceras på en verklig företeelse för den med sig stora fördelar genom att den stödjer kategorisering och hjälper till att relatera olika aspekter med varandra. Problemet är att alla de strikt definierade abstrakta termer som används för att beskriva verkligheten tillsammans bildar en sådan massa av betydelse att utrymmet för konkreta tillgängliga begrepp blir väldigt litet.

3 Metod och material

I följande avsnitt kommer studiens valda forskningsmetodik, urval, datainsamlingsmetod, genomförande samt dataanalys att redogöras och argumenteras för. Med avseende på problemområdets relativt outforskade natur samt att hemlig dataavläsning nyligen lagstadgades har studien en explorativ ansats med kvalitativt perspektiv. Insamlandet av data har skett via semi-strukturerade intervjuer av fyra informanter med IT-forensisk bakgrund som primärkälla och via dokumentanalys av artiklar och rapporter samt en podcast som sekundärkällor. Avsnittet avslutas med en kritisk reflektion över studiens tillförlitlighet.

3.1 Explorativ undersökning

Eftersom studien ämnar undersöka förhållande kring användandet av en teknik som lagstadgades först under studiens gång, samt att insyn i Polismyndighetens användning av tenkiken är hårt sekretessbelagd är möjligheten att utvinna kvantitativa data begränsad. Valet av metod föll då på en explorativ ansats med kvalitativt perspektiv för att undersöka frågeställningen. Denna metod menar Patel och Davidsson (2011) är fördelaktig när det finns kunskapsluckor och liten till ingen kunskap om området man ämnar studera innan undersökningen startar. Det kvalitativa perspektivet möjliggör analys av data via informationssamlande från semi-strukturerade intervjuer hos ett relativt lågt antal respondenter, i detta fall fyra, vilket lämpar sig väl med avseende på den begränsade tidshorisonten för studien. Semi-strukturerade intervjuer baserade på kvalitativ ansats möjliggjorde en rikare analys av informanternas förväntningar, farhågor och andra tankar som författarna från sin explorativa utgångspunkt annars inte skulle ha kunskapen att fråga om (Bell 2016; Patel & Davidsson 2011). Informanterna valdes utifrån deras kompetens inom det relevanta området, för att ge insikt i studiens relativt opaka område.

3.2 Empiriskt urval

Studiens empiri har hämtats dels från dokumentanalys, dels från semi-strukturerade intervjuer. För insamling av data har semi-strukturerade intervjuer genomförts utefter en intervjuguide. Fyra informanter intervjuades och spelades in. Informanterna valdes utifrån deras bakgrund och anställning som IT-forensiker. En IT-forensiker är enligt IDG:s (2020) ordlista en kriminaltekniker med inriktning på IT. Det är IT-forensikerna som hanterar användningen av de hemliga tvångsmedlen vilket gör dem till den grupp som studien bör använda som informanter för att få ett relevant studieresultat. Informanternas kunskap inom sitt yrke samt erfarenhet av tidigare implementationer av nya tvångsmedel ger vital information för studien. I Tabell 1 presenteras bakgrund och roller hos de informanter som deltagit i studien.

	Bakgrund	Roll	Erfarenhet som IT-forensiker
Informant 1	Polis	IT-forensiker	Nyligen tillsatt
Informant 2	Datavetenskap	IT-forensiker	13 år
Informant 3	Polis och intern vidareutbildning	IT-forensiker	20 år
Informant 4	Datavetenskap	IT-forensiker	ca 6 år

Tabell 1: Informanternas bakgrund och roller.

Förutom intervjuer har litteratur och podcasts relevanta för ämnesområdet analyserats för att i konjunktion med insikter från intervjuerna tas upp i resultaten. Podcasten har transkriberats och kodats på samma sätt som intervjuerna. Källorna har hittats med hjälp av handledare och sökningar. Sökningar har skett via Göteborgs Universitetsbibliotek samt Google Scholar. Exempel på sökord: Statlig hacking, it relaterade brott, hemlig dataavläsning.

Dokumenten samt den podcast som analyserats:

- Brottsförebyggande rådet (2016), *IT-inslag i brottsligheten och rättsväsendets förmåga att hantera dem*, 2016:17
- Forskningsdokument från Europaparlamentet (2017), *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*
- Granskningsrapport från Riksrevisionen (2015), *IT-relaterad brottslighet - polis och åklagare kan bli effektivare, RIR 2015:21*
- Lagrådsremiss från regeringen till Lagrådet (2019), *Hemlig dataavläsning*
- Patrick Cordner, chef Nationellt IT-brottscentrum, under en intervju i podcast *Allt du behöver veta om ny teknik* (2020). Ny Teknik
- Statens Offentliga Utredningar, Delbetänkande av Utredningen om hemlig dataavläsning, *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet, SOU 2017:89* (2017)

3.3 Datainsamling

Studiens primära datainsamling skedde via semi-strukturerade intervjuer vilket lämpar sig väl då studien håller ett kvalitativt perspektiv där en studerar hur individer upplever sin verklighet (Bell 2016; Patel & Davidsson 2011). Syftet var att fånga upp information via dessa intervjuer som en utomstående har svårt att komma åt, detta då problemområdet och Polismyndigheten överlag har stora krav på sekretess. Patel och Davidsson (2011) menar att syftet med en kvalitativ intervju är att upptäcka och identifiera egenskaper och beskaffenheten hos något i den intervjuades värld.

Med detta i åtanke tillsammans med författarnas låga grad av insyn i problemområdet sedan innan föll valet på semi-strukturerade intervjuer med en låg grad av struktur (Bell 2016; Bryman 2018). Detta möjliggör för att via öppna frågor och en relativt låg profil hos den som utför intervjuerna istället låta informanterna prata så fritt som möjligt. Intervjun bör dock skötas medelst en intervjuguide som skapas innan för att hålla en översikt på vad som är besvarat eller inte inom de områden man försöker belysa (Bell 2016).

Mycket tid lades på att utforma intervjuguiden. Tre teman identifierades där det under varje tema finns ett flertal frågor utformade för att vara öppna frågor som kan tas vidare för att ytterligare fånga upp informantens egna tolkningar och upplevelser (Patel & Davidsson 2011). Detta underlättar även för analys av data (Bell 2016). Formuleringen av frågorna utgick ifrån ett förarbete där författarna studerade tillgängligt material kring hemliga tvångsmedel, sammanslaget med de områden som var svåra att få insyn i.

Intervjuerna inleddes med frågor om informantens utbildning och bakgrund för att sedan gå över i något av de tre olika teman och en avslutning. Fokus lades inte på i vilken ordning de olika teman togs upp. Informanten fick istället prata så fritt som möjligt och följdfrågor ställdes med fokus på flexibilitet hos den som intervjuade för att snappa upp matnyttig data (Bryman 2018). Huvudfrågorna i intervjuguiden skickades ut i förväg till informanterna så de kunde förbereda sig inför intervjuerna samt information om att de skulle få vara anonyma. Utöver anonymitet utlovades att inspelningar och transkriberingar raderas efter studiens slutförande, allt för att tillåta informanterna att tala så fritt som möjligt (Bell 2016). Intervjuguiden finns bifogad till rapporten som *Bilaga 1 - Intervjuguide till IT-forensiker*.

Totalt utfördes fyra intervjuer som alla varade mellan 35–105 minuter. Informanterna medgav till att intervjuerna fick spelas in. Tre av intervjuerna utfördes på informanternas arbetsplatser och en intervju utfördes via länk. Dessa transkriberades sedan manuellt och gav upphov till 60 sidor transkriberat material.

3.4 Dataanalys

En viktig distinktion att göra är att författarna kodat materialet i två steg. I det första steget har teorin lämnats därhän för att i möjligaste mån hålla ett öppet sinne för resultaten utan att via det teoretiska ramverket påverka funna affordanser i ett för tidigt skede. Istället har affordansteorin applicerats på de utmaningar och teman som funnits vid den öppna kodningen och utvecklats vidare därifrån i en andra teoridriven kodning.

Bell (2016) menar att det är ordens betydelse och inte orden i sig som är viktiga. Med 60 sidor transkriberat material användes både öppen och teoridriven kodning som metod för att sortera informationen. Öppen kodning, som Saldaña (2013) kallar initial kodning och är det som forskaren får som första intryck vid läsandet av material, användes utan teori som lins för att inte färga resultatet och kunna utläsa fler utmaningar och teman. Vid den teoridrivna kodningen som Bryman (2018) benämner tematisk kodning identifieras meningar och ord som sammanfaller i mening utefter teman och utmaningar som identifieras. Efter det applicerades det

teoretiska ramverk studien lutar sig mot. De teman som identifierades hjälptes till viss del av de teman som konstruerats i intervjuguiden (Bell 2016). På så vis kunde stora delar av de många sidorna transkriberat material kondenseras till pregnanta citat med gemensamma nämnare (Bell 2016).

Kodningen skedde i flera steg. Det första steget innebar att författarna gick igenom texterna utan att samarbeta för att utan att påverka varandras åsikter kunna identifiera viktig information med öppen kodning. I nästa steg jämfördes vad författarna menade var viktig information från den öppna kodningen med varandra. En sållning genom diskussion och jämförelse reducerade informationen till mer hanterbara nivåer. Sedan utfördes ett andra steg med kodning där affordansteorin användes som lins. Dessa kärnfulla texter kunde sedan jämföras mot varandra i resultatet.

Specifikt hur appliceringen av affordansteorin gått till beskrivs närmare i samband med den faktiska appliceringen, under avsnittet Diskussion.

3.5 Studiens tillförlitlighet

Studien genomfördes med ett explorativt och kvalitativt perspektiv. Detta, som tidigare nämnts, på grund av den sekretessfyllda naturen av problemområdet hos polisens hemliga tvångsmedel. Datainsamlingsmetod bestod huvudsakligen av intervjuer. Bell (2016) menar att den stora utmaningen med att använda kvalitativa intervjuer är att inte låta resultatet bli påverkat av författarnas egna uppfattningar eller åsikter.

Under framställandet av intervjuguide, genomförande av intervjuer samt analys av material har författarna haft detta i åtanke och försökt hålla objektivitet främst. På grund av omständigheter utanför författarnas kontroll samt att tidsramen var snäv blev antalet informanter begränsat till enbart fyra. Något som kan påverka generaliserbarheten är dels det låga antalet informanter samt att alla informanterna kom från Polismyndigheten, region väst. Det går inte heller att undvika eventuell jävighet från informanterna som vid intervjuerna omedvetet kan ha påverkats av vetskapen att de spelas in (Bell 2016).

Patel och Davidsson (2011) menar att kvalitativa studier kännetecknas av en stor variation och det kan vara svårt att finna entydiga regler, procedurer eller kriterier för att garantera god kvalité. Författarna har försökt verka för bra kvalité genom att förhålla sig så objektivt som möjligt under datainsamling och analys för att sedan ställa informanternas svar mot dokumentation, relaterad forskning och därmed skapa teoretisk triangulering (Patel & Davidsson 2011).

4 Resultat

I analysen av det insamlade materialet identifierades tre teman som alla är relaterade till möjligheter och utmaningar: *Kompetens*, *Resurser* och *Kryptering*. De två första handlar om hur brist på kompetens och resurser begränsar användningen av hemlig dataavläsning medan kringgående av kryptering är den stora möjliggörande effekten. Dessa tre teman har sedan brutits ner i mer specifika områden som möjliggör eller begränsar inhämtad data från informanter, dokument och en podcast.

4.1 Resurser

En viktig faktor för myndighetens förmåga att använda tekniken bakom hemlig dataavläsning är de resurser som krävs för att kunna tillämpa den nya tekniken. Resurser i form av både högre kostnader och personalresurser pekades på av informanterna som något som kommer att påverka användningen av hemlig dataavläsning. I *Lagrådsremiss Hemlig dataavläsning (2019)* skriver de om resursåtgången i relation till effektivitet, vilket styrker informanternas uppfattning. Även Patrick Cordner pratar i podcasten, *Allt du velat veta om ny teknik (2020)* om resurser och om hur resurssatt Polismyndigheten redan är.

“skulle folk få veta och se allt de hemska vi ser så är jag övertygad om att vi skulle få ny lagstiftning och mer resurser ganska snabbt” (Cordner, 2020)

4.1.1 Högre kostnader

Att tekniken är kostsam och kräver resurser i form av ekonomiska medel var alla informanter överens om. Det får stöd i statens offentliga utredningar från justitiedepartementet, *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet, SOU 2017:89* (2017). Där har man beräknat de ökade kostnaderna för att verkställa hemlig dataavläsning till 100 miljoner kronor per år. I de kostnaderna har man räknat utbildning, rekrytering, kompetensutveckling, drift och underhåll samt kostnader för anskaffning av teknisk utrustning som den största posten.

”Jag har ingen aning men jag kan föreställa mig att det är kostsamt. Då får man väl väga det mot vad man får ut av det. (Informant 2)

I utredningen nämner de också att en stor del av av den beräknade kostnaden kommer att behöva läggas på nyrekrytering av personal med specialkompetens. Kostnader som redovisats i dokumentet är beräknade på en uppskattning om att kunna ha ca 20–30 installationer igång samtidigt. Det förklaras med att det ibland kan vara nödvändigt med flera installationer samtidigt mot samma målperson, samt att det ibland bara behövs relativt kort förberedelse och relativt enkel installation.

4.1.2 Personalresurser

Informanterna pratade om att det är en lång process för de som arbetar med fall där hemlig dataavläsning kan tänkas användas. Det krävs ett gediget förarbete och tar lång tid att samla in den information de behöver för att kunna ansöka om tillstånd i domstol för att kunna använda hemlig dataavläsning. Två av informanterna upplevde att det finns ett begränsat antal personer som arbetar med tekniken bakom hemlig dataavläsning vilket medför att det inte kommer att bli applicerbart på många ärenden samtidigt.

”[…] så har vi ju begränsat med personal som jobbar med det och det blir ju nästa fråga då, hur många ärenden kan vi ha igång samtidigt då och den uppgiften kan jag ju däremot inte lämna ut för den är ju känslig” (Informant 2)

Det bekräftas av Patrick Cordner i podcasten *Allt du velat veta om ny teknik (2020).* Där pratar han om att det finns många fall med IT-relaterad brottslighet men inte tillräckligt med personal som kan hantera den bevisningen. Han pratar också om att det behövs mer personal.

“Är en flaskhals hos IT-forensikerna. Mycket utredningar stannar upp för att det finns material som väntas på att undersökas.” (Cordner, 2020)

“Fylla på regionerna med resurser och fler personer. Vi är bra men vi är för få som är bra.” (Cordner, 2020)

4.2 Kompetens

Ett av de hinder som informanterna tror kan påverka användningen av hemlig dataavläsning är IT-kompetensen inom polismyndigheten. Deras upplevelse av kompetensbrist är baserad på deras uppfattning som tjänstemän inom myndigheten. Uppfattning styrks i den rapport som gjordes av Brottsförebyggande rådet, *IT-inslag i brottsligheten och rättsväsendets förmåga att hantera dem, 2016:17* (2016) och i en Granskningsrapport från Riksrevisionen, *IT-relaterad brottslighet - polis och åklagare kan bli effektivare, RIR 2015:21* (2015). Informanterna var även överens om att IT-kompetensen hos kriminella har ökat vilket försvårar brottsutredningarna. Det kan man också läsa om i en av statens offentliga utredningar från justitiedepartementet, *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet, SOU 2017:89* (2017).

4.2.1 IT-kompetens inom polismyndigheten

Samtliga informanter pratade om en bristande IT-kompetens inom polismyndigheten. Detta framställdes av informanterna i varierande grad, några upplevdes mer försiktiga i sina svar medan andra var mer raka och tydliga. Den sammanfattande upplevelsen kan ändå tolkas som att kompetensen är ett hinder för att kunna använda hemlig dataavläsning på ett sätt som ger en maximal effekt vid bekämpandet av den grova organiserade brottsligheten.

“Det är väldigt skiftande kunskaper” (Informant 1)

"Kompetensen är ibland låg, skrämmande låg. Även om det finns duktiga poliser som jobbar inom IT." (Informant 4)

Informanterna pratade om att den allmänna IT-kompetensen är låg och att den bara blir sämre. Det kan påverka användandet av hemlig dataavläsning då kringliggande sektioner inte har den kunskap som behövs för att kunna göra korrekta beställningar av sektionen som ansvarar för hemlig dataavläsning.

"Den största anledningen till att digitala bevis går förlorade är för att poliser inte vet när de ska ringa till IT-forensikerna, eller de vet inte hur de ska hantera första triageläget när det kommer till digital bevisning." (Informant 4)

Även nyexaminerade poliser har generellt sett en låg IT-kompetens då det saknas utbildning i IT-relaterad brottslighet i grundutbildningen. Det finns att läsa om i Riksrevisionens granskning (2015). Där kan man även se att de vidareutbildningar som finns inom polismyndigheten inte är tillräckliga.

"[...] det är inte så många som håller på med datorer och då får man inte den djupa kunskapen på samma sätt. Man håller på med sin telefon, man vet egentligen inte hur det funkar, man klickar lite och så. Du vet inte tekniken bakom hur det fungerar. Så nej, de blir inte bättre, de blir snarare sämre." (Informant 2)

"Generellt är den oerhört dålig men jag tycker den har blivit sämre sen folk började få mobiltelefoner då har de ingen koll alls, förut hade de lite koll i alla fall." (Informant 3)

Det som informanterna uttrycker om kompetensen inom polismyndigheten hos kringliggande avdelningar får stöd av Brottsförebyggande rådets utredning (2016). I utredningen påvisar de att det finns en generell okunskap om IT och de expertfunktioner som finns inom Polismyndigheten, exempelvis Nationella Operativa Avdelningen, där sektionen som hanterar hemlig dataavläsning finns. Även den granskning som Riksrevisionen (2015) gjort påvisar samma sak. Där har man i granskningen redovisat att brist i kompetensen hos poliser gör att förmågan att utreda brott med IT-inslag på ett tillfredsställande sätt inte är tillräcklig.

"Spetskompetensen uppfattas vara mycket god hos IT-forensiker och en mindre grupp mer specialiserade medarbetare, men man framhåller att detta inte är tillräckligt." (Riksrevisionen RIR 2015:21, s. 50)

IT-kompetensen hos de som anställer är även den låg och även om man mer och mer försöker rekrytera personer med IT-utbildning så varierar kunskapen stort beroende på utbildning och lärosäte. Det kan vara svårt för rekryterande personer att avgöra kompetensnivå och var kompetensen är bäst applicerbar, när de som rekryterar inte själva besitter expertkunskap. I Riksrevisionens granskning (2015) trycker man på vikten av att ha en bra kompetensförsörjning och att det finns brister i kompetensförsörjningen som behöver förbättras för att kunna hantera brott med IT-inslag.

"[…] jämför du Sverige med vissa andra länder, kan till exempel både nämna Storbritannien och USA så är lönenivåerna för IT-forensiker en helt annan vilket gör att man kan behålla kompetens." (Informant 4)

4.2.2 IT-forensikers uppfattning om kriminellas IT-kompetens

Att IT-kompetensen ökat hos kriminella var alla informanter överens om. De pratade om det som ett hinder för brottsutredare och IT-forensiker då de kriminella ligger före, eftersom de kan använda teknik utan att behöva vänta på lagstöd. I den typen av brott, med det straffvärdet som behöver uppnås för att kunna applicera hemlig dataavläsning är generellt kompetensen och informationssäkerheten hög hos de kriminella.

"Det är inga korkade personer som vi är ute efter, det handlar inte om att få ut lite mobiltrafikdata ur en pundare som har köpt ett par kilo hasch utan det handlar om att slå mot toppen av näringskedjan, de som kan riktigt mycket. Så här stor organiserad brottslighet har garanterat sina egna IT-tekniker och personer som är specialiserade på IT." (Informant 4)

Precis som i övriga samhället ökar användningen av digitala metoder för att kommunicera och dela data bland kriminella. Anti-forensiska metoder används mer och mer av brottslingar för att gömma bevis. Det kan vara metoder som radering eller kryptering. Det är något som framkommer både i Statens offentliga utredning om hemlig dataavläsning (2017) och i Riksrevisionens granskningsrapport om IT-relaterad brottslighet (2015)

"[...] särskilt vid organiserad eller annan allvarlig brottslighet fanns ofta vissa deltagande personer som var utomordentligt skickliga i användningen av datorer och utnyttjade sina kunskaper fullt ut." (Statens offentliga utredningar, SOU 2017:89, s. 106)

4.3 Kryptering och tekniken bakom hemlig dataavläsning

Kryptering av data som skickas och lagras är en anti-forensisk metod som används av kriminella, vilket är ett hinder som försvårar för polisen vid spaning och förundersökningar. Att det är den primära och särdeles största orsaken till införandet av "*Lagen om Hemlig Dataavläsning"* och därigenom det hemliga tvångsmedlet är alla informanter tydligt överens om. Det kan man också läsa om i statens offentliga utredningar från justitiedepartementet, *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet, SOU 2017:89 (2017),* vilket styrker informanternas uppfattning. Tekniken bakom hemlig dataavläsning som blivit möjlig för polisen att använda som tvångsmedel vid införandet av "*Lagen om Hemlig Dataavläsning"* möjliggör för utredare och IT-forensiker att komma runt krypteringen och läsa information i klartext innan det krypteras eller när det har dekrypterats. Alla informanter pratar om att det är så tekniken övergripande kommer att användas och hänvisade ofta till hur den används i övriga europa. Samtidigt kan det tolkas som att några informanter är mer kritiska till vilken effekt den faktiska

tekniken kommer att ha, både på grund av kompetens hos kriminella och på grund av resurser och kompetens inom polismyndigheten.

4.3.1 Kryptering av data

Att det idag är enkelt att kryptera sin data försvårar det utredande arbetet och gör det enkelt för kriminella att hindra att data avläses. Informanterna pratade om det som ett problem när man inte kan lyssna på kommunikation i klartext.

"Om du möter en brottsling som är duktig och använder kryptering och är duktig på att dölja sina spår och allt det där så är det väldigt svårt att kunna undersöka deras dator på ett effektivt sätt. Om du liksom gör ett tillslag och datorn blir avstängd så är det oftast kört, och där har ju hemlig dataavläsning ett användningsområde." (Informant 4)

De pratade också om hur lätt det är att kryptera sin data idag med de inbyggda tekniker som finns i många av de vanligaste apparna. I lagrådsremissen som regeringen överlämnade till Lagrådet för granskning, *Lagrådsremiss Hemlig dataavläsning (2019)* skriver man om samma sak. Där nämner de chat-appar som Messenger och WhatsApp. En av informanterna nämnde även Signal och Snapchat som också är vanliga appar som används för att kommunicera. De inbyggda krypteringstjänsterna i apparna är användarvänliga och möjliggör för användare att kommunicera utan risk för att utomstående ska ta del av kommunikationen.

"[...] huvudsyftet är att man har ett problem med att kriminella, speciellt de här grövre kriminella som är slipade och vet vad de håller på med, pratar väldigt mycket på krypterade appar. Det här möjliggör ju att kunna avläsa även dessa appar, och det skulle kunna bli revolutionerande men vi vet ju inte ännu." (Informant 1)

Även i Statens offentliga utredningar från justitiedepartementet, *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet, SOU 2017:89* (2017) pratar de om krypteringen som ett problem i form av att det tar stora resurser och ställer högre krav vid spaning och tillslag för att försöka till exempel hinna fram till en dator innan den stängs av och blir krypterad. En av informanterna pratar om samma sak och berättar om ett fall där man haft tur att göra tillslaget precis när den misstänkte satt vid sin dator och just öppnat sitt krypteringsverktyg.

"[...] även om vi har lyssningar och sådant så hör vi inte vad de säger och då måste vi ha något annat och då tror jag att folk har mer förståelse för det nu." (Informant 2)

4.3.2 Tekniken bakom hemlig dataavläsning

Vidare diskuteras vilken information som behövs för att kunna använda tvångsmedlet effektivt. Exempelvis vilken enhet som är målet, vilket operativsystem som används, vilka appar som används och så vidare. Vilken den faktiska tekniken är som används har informanterna varit förtegna om. Svaren kan tolkas som antaganden, samtidigt som de ofta hänvisar de till den teknik som används i de länder i Europa där olika former av statlig hacking är lagstiftad.

"[...]utmaning att veta vilka telefoner de har då för att på något sätt komma åt dem eller på något sätt få in något i dem." (Informant 2)

De antaganden som gjordes av informanterna kring tekniken var att man behöver, efter att ha identifierat vilken enhet och mjukvara den kriminella använder, ha kunskap om en sårbarhet i den mjukvara man vill utnyttja. Antingen genom kända sårbarheter där användaren inte har uppdaterat sin mjukvara och sårbarheterna inte har patchats, eller genom en zero-day-sårbarhet. Vidare spekulerades kring hur myndigheten skulle få tag i sådana sårbarheter. Antingen köpa sårbarheten från externa aktörer som företaget Zerodium, som köper och säljer bland annat zero-days, eller hitta egna sårbarheter. Man spekulerade också kring om det skulle vara möjligt med ett samarbete med andra länder men konstaterade snabbt att det inte är troligt när det handlar om just zero-day sårbarheter. Då man vill hålla dessa för sig själv och inte riskera att de läcker ut och blir patchade.

"[...] hittar man en sårbarhet även om underrättelsetjänsten gör det, för olika försvarsmakter och sådant där så vill man ju inte, man vill ju inte bränna dem utan man vill ju ha det öppet så länge som möjligt." (Informant 2)

"[...] man måste ju ha någon som sitter och funderar på vad det är för plattform som personen som misstänks för brottet har och om man har någonting som man kan använda på den plattformen då och det får inte läcka vilken sårbarhet, man vill ju inte att de ska plugga igen den liksom." (Informant 2)

I nästa steg behöver Polismyndigheten få in till exempel en trojan eller en keylogger i mjukvaran. Har de då inte vetskap om någon sårbarhet så hade informanterna två olika alternativ på hur det skulle kunna gå till. Antingen på något sätt beslagta enheten och installera programvaran eller att man skulle kunna få användaren att klicka på en länk, exempelvis en uppdatering med en trojan inbäddad.

"*om man då ska ha den nya tekniken där man får ha någon form utav trojan eller någonting eftersom trafiken är krypterad, då måste du få in den innan krypteringen eller efter om man säger det så"* (Informant 2)

Den programvara som används när man väl kommit in i plattformen tror informanterna kommer vara samma programvara som används i andra länder. Där är det inte lika sårbart om det skulle läcka ut vilken programvara som används tror informanterna. De nämner också att det inte finns så många olika sätt som det kan gå till på. Vilket får stöd av Patrick Cordner under en intervju i podcast *Allt du behöver veta om ny teknik* (2020), där säger han att han inte kan gå in på detaljer kring tekniken men att vem som helst som är lite teknikkunnig kan googla och dra egna slutsatser om hur det kommer att gå till. I podcast avsnittet säger han också att *"vi använder den teknik som finns ihop med den lagstiftning som finns" (2020).*

"Vi uppfinner ju säkert inget nytt utan vi använder säkert den teknik som man använder i ett annat land." (Informant 3)

Informanterna pratar också om en del svårigheter kring tekniken. Så som att kriminella byter mobiler, vilket då medför att den mjukvara man stoppat in i mobilen blir verkningslös och man behöver få in mjukvara i den nya mobilen för att kunna fortsätta bedriva avläsning. Då behöver man på nytt identifiera vilken enhet och

vilken mjukvara den kriminella använder, samt att hitta en väg in i den nya enheten, vilket kan kräva omfattande arbete.

"Eller att man byter telefoner ofta då, det är också ett bekymmer, om man, du vet att en person byter telefoner regelbundet och man ska ha den här avlyssningen igång hela tiden de blir ju problematiskt." (Informant 2)

I *Lagrådsremiss Hemlig dataavläsning (2019)* beskrivs hur tvångsmedlet hemlig dataavläsning skulle kunna verkställas. Under planering och kartläggning beskriver de att syftet är att identifiera vilken typ av teknisk utrustning som målpersonen använder. Detta bekräftar informanternas teori om hur man behöver gå tillväga innan man kan få tillstånd från domstol och inleda det praktiska arbetet. De skriver att målet kan vara fysiskt, som en dator eller en mobil men det kan också vara en app eller ett program. Nästa steg är intrång och installation. Då behöver myndigheter identifiera sårbarheter. De skriver att det kan vara tekniska brister och mänskliga svagheter. De nämner inget om zero-day sårbarheter men de nämner attackmetoden *exploit* som är ett samlingsnamn som används för att beskriva själva attacken, metoden och den sårbarhet som använts (Lagrådsremiss Hemlig dataavläsning 2019). De skriver också att hemlig dataavläsning skulle kunna genomföras med installation av hårdvara på eller vid teknisk utrustning eller vid installation av mjukvara i en enhet. Mjukvaran kommer att behöva anpassas till olika förutsättningar. Det är något som informanterna pratar om som ett hinder bland annat om den kriminella ofta byter enhet.

4.3.3 Teknikanvändning vid hemlig dataavläsning i Europa

Flera informanter hänvisade till den användning av teknik som andra stater i Europa använder för att avläsa sina egna medborgares data vid misstanke om brott. För att bekräfta detta har informanternas svar relaterats mot ett forskningsdokument från Europaparlamentet, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices (2017).* Inte heller där går de in på djupet i teknikanvändningen men vi kan ändå göra en övergripande analys av de vanligaste tekniker som används och då dra slutsaten att Polismyndigheten i Sverige kommer att använda sig av samma teknik anpassat till den svenska lagstiftningen kring hemlig dataavläsning.

I Italien anser experter att man använder skadlig programvara i form av trojaner som till exempel skulle kunna avlyssna kommunikation, ta kontroll över enhetens kamera och mikrofon och ge åtkomst till lagrad data (Europaparlamaentet, 2017). I Nederländerna är det mer specificerat vad de får göra och därigenom får vi mer kunskap om den teknik de faktiskt använder. De får använda en sårbarhet i mjukvaran, göra intrång med en falsk identitet eller med brute force eller använda en trojan för att infektera enheten med skadlig programvara. I andra länder som till exempel Storbritannien är de likt Sverige mer förtegna om vilka tekniker de använder och har en bredare mer övergripande lagstiftning. Anledningen som Storbritannien framhåller är lik de antagen som gjorts av informanterna. De vill inte avslöja detaljer för att kunna bevara effektiviteten mot den grova organiserade brottsligheten (Europaparlamentet 2017).

"Vi menar att vi ska använda det här mot IT-kunniga skurkar och de kommer ha antivirusprogram, de kommer ha säkerhetsåtgärder, de kommer ha kryptering, har de inte det då behöver vi inte den här lagen. Och har de det då behöver vi sitta på, polisen sitta på extremt starka verktyg för att det ska bli rimligt" (Informant 4)

Vidare i forskningsdokumentet från Europaparlamentet (2017) beskriver de att resultaten pekar åt ett tydligt håll. De menar att utvecklingen går mot att att man använder intern expertis och ibland till och med egenutvecklade hackerverktyg. I exempelvis Frankrike så används främst keyloggers för att samla in uppgifter. Dessutom har myndigheter i Frankrike utvecklat egna verktyg för att få fjärråtkomst över enheter. I Tyskland har man tagit ett beslut om att man har för avsikt att utveckla egna verktyg. Italien arbetar åt samma håll som Tyskland och utvecklar sin förmåga för att utveckla interna verktyg.

Informanterna resonerade kring zero-day sårbarheter och Sveriges användning av sådana sårbarheter. Bara ett land, vilket det är nämns inte, hänvisar till utnyttjandet av sårbarheter för att få tillgång till en enhet, vilket gör det svårt att tolka hur vanligt förekommande det är för att kunna dra några slutsatser om hur man kommer att arbeta i Sverige. Man uttrycker ändå att det inte går att utesluta möjligheten att även andra länder utnyttjar kända eller okända sårbarheter men att den teknik och de metoder de använder är hemligstämplad information.

5 Diskussion

I nedanstående avsnitt relateras först teorin till det insamlade resultatet. Affordansteorins definitioner och termer placeras in i resultatets sammanhang och en diskussion förs kring hur olika företeelser kan tolkas ur teorins lins. I slutet av den diskussionen besvaras studiens frågeställningar konkret. Efter det diskuteras studiens möjliga implikationer på relaterad forskning och praktisk verklighet. Till sist görs en reflektion kring studiens resultat och genomförande ur ett kritiskt perspektiv.

5.1 Hemlig dataavläsning ur ett affordansperspektiv

På grund av den sekretess som råder kring den konkreta appliceringen av hemlig dataavläsning har resultatet som samlats in fått en relativt hypotetisk karaktär. Informanterna var uttryckligen förbjudna att i detalj diskutera konkreta metoder och tekniker kring realiseringen av tvångsmedlet. En direkt följd av att det studerade tvångsmedlet införts under studiens gång, och alltså är en ny företeelse, är att det inte heller finns någon dokumenterad användning. Enligt informanterna pågår det förundersökningar där tvångsmedlet används men det finns ännu inte några fällande domar, och därmed inte heller någon information att tillgå kring resultat eller genomförande av användning. För att ändå kunna hålla en relevant diskussion har studiens fokus därför lagts på de faktorer som potentiellt skulle kunna påverka tvångsmedlets användning. Här ingår de aktörer som använder eller påverkar användning av tvångsmedlet, det direkta resultat som en aktualisering av hemlig dataavläsning är tänkt att ge och de övergripande mål och syften som driver aktörerna som är inblandade. Diskussionen förs med målet att utforska och kartlägga de förutsättningar som kan blottläggas genom att undersöka ovan nämnda faktorer utifrån affordansperspektivets lins. Volkoff och Strong (2018) menar att teorin med fördel kan användas på detta mer utforskande sätt, och inte enbart för att identifiera och kategorisera affordanserna själva. Eftersom studiens material har den karaktär som nämns ovan anser författarna att den här typen av applicering av teorin som ett perspektiv är det mest givande för studien.

I underliggande avsnitt konkretiseras först dessa faktorer efter studiens insamlade resultat och allmänna affordanser identifieras. Efter detta förs tematiserade diskussioner med utgångspunkt i relevanta principer och problematiker som Volkoff och Strong (2018) ger för en lyckad applicering av affordansteorins perspektiv.

5.1.1 Kartläggning av problemområde

Den definition av vad en affordans är som ges av Strong et al. (2014 se Volkoff & Strong, 2018) har använts för att identifiera relevanta faktorer som står i relation till affordanser.

En affordans är beteendet associerat med att uppnå ett direkt och konkret resultat och uppstår ur relationen mellan en artefakt och en eller flera målorienterade aktörer.

Utifrån denna definition kan följande konkreta faktorer utläsas: Artefakt, Aktör eller aktörer, Resultat och Mål/Syfte. Nedan listas vad som representerar dessa faktorer i föreliggande studie.

- Artefakt: Tvångsmedlet hemlig dataavläsning

Den artefakt som avses undersökas är tvångsmedlet. Notera särskiljning från dels ”*Lagen om hemlig dataavläsning”* som reglerar hur tvångsmedlet får appliceras och dels från den teknik som används för att utföra tvångsmedlet

- Aktörer: IT-forensiker, operativa enheter, domstol som dömande och tillåtande element, åklagare som förundersökningsledare, resten av polismyndigheten (utredande, beställande med mera)

De aktörer som listas ovan är de som på ett eller annat sätt är inblandade i aktualiseringen av tvångsmedlet. Informanter och analyserade dokument visar tillsammans på att flera olika instanser berör hanteringen. IT-forensiker är de aktörer som är mest involverade. De hanterar den data som ges åtkomst till och de bidrar med kunskap om hur, var och på vilket sätt tvångsmedlet kan appliceras. Andra delar av Polismyndigheten står genom operativa insatser och utredningsarbete dels för det spaningsarbete som krävs för att insamla den kunskap som ligger till grund för beslut om och hur tvångsmedlet ska aktiveras, dels för den faktiska applicering av de tekniska lösningar som åstadkommer dataavläsning. Åklagare deltar dels som förundersökningsledare, en form av beställare av användningen, dels som nyttjare av resultatet, den bevisföring som blir aktuell vid en rättegång. Andra delar av rättsväsendet är involverade dels genom beslutande element, då användning av tvångsmedlet måste godkännas genom beslut i domstol, dels när den insamlade bevisningen används vid rättegång.

- Resultat: Åtkomst till enheter, data och bevisföring.

De konkreta resultat som förväntas vid tvångsmedlets användning är åtkomst till enheter som ska avläsas, åtkomst till data på dessa enheter och efter att denna data har sorterats och analyserats, bevisföring som går att använda i brottsmål.

- Mål/Syfte: Att kringgå kryptering. Fällande domar för brott med ett straffvärde på minst två års fängelse, minskad brottslighet, bekämpning av terrorism och organiserad brottslighet.

De mer övergripande målen med användning av tvångsmedlet, och det som styr de aktörer som använder det, är minskad brottslighet generellt, mer specifikt bekämpning av terrorism och organiserad brottslighet. Mer konkret är syftet fällande domar för brott med ett straffvärde som börjar med två års fängelse genom att kringgå kryptering.

Ovanstående element står via definitionen av affordanser, som redan presenterats, i relation till tre övergripande affordanser som presenteras efter detta stycke. Volkoff

och Strong (2018) poängterar att affordanser inte realiseras annat än när en måldriven aktör använder en artefakt. I det här fallet används artefakten av flera grupper av aktörer men det konkreta direkta resultatet som eftersöks är fortfarande detsamma. Likaså de övergripande mål som eftersträvas. Eftersom studiens artefakt, tvångsmedlet hemlig dataavläsning, som tidigare nämnts är nytt och metoderna för användning är lagda under sekretess har fokus lagts på att kartlägga förhållanden kring och mellan dessa affordanser snarare än affordanserna själva. Hade studiens material kunnat visa på exakt vilken teknik som används och hur hade mer konkreta affordanser kunnat utläsas och en mer teknisk studie gjorts. Med det material som finns att tillgå får perspektivet istället läggas på ett mer övergripande plan, varför diskussionen blir utforskande och kartläggande snarare än teknisk i sitt utförande. Detta följer vad Volkoff och Strong (2018) menar är en av affordansteorins fördelar, nämligen att genom dess lins identifiera aktörer, deras handlingar och andra faktorer som påverkar användningen av en artefakt. Av samma skäl har affordanserna som etablerats en övergripande karaktär. Volkoff och Strong (2018) anser att affordansers finkornighet bör bestämmas efter studiens karaktär och forskningsfråga. På grund av de skäl som angivits ovan angående studiens material sätts finkornigheten lågt och fokus läggs på förhållanden som påverkar affordanser och användning av artefakten. Affordanserna som identifierats är:

- Åtkomst till, och användning av, tekniken (zero-days, trojaner, keyloggers)

Kan tyckas självklart men eftersom särskiljningen gjorts mellan tvångsmedlet och tekniken är beteendet ovan något som möjliggörs av och genom aktualisering av tvångsmedlet. Utan en laglig bas, den juridiska konstruktion som tvångsmedlet hemlig dataavläsning är, kan inte rättsväsendet använda sig av eller införskaffa den teknik som används i aktualiseringsprocessen.

- Göra intrång

Användningen av hemlig dataavläsning möjliggör för aktörer att göra intrång på krypterade enheter genom användning av den teknik vars åtkomst möjliggörs genom ovanstående affordans.

- Åtkomst till data

Den tredje affordansen i ordningen, som också följer av de två ovanstående är åtkomst till data. Denna data kan senare bli bevismaterial men det mer övergripande beteendet som möjliggörs är åtkomst till data på de enheter som ovanstående affordans möjliggör intrång på.

De här tre affordanserna kan sägas vara beroende av varandra då den första leder till den andra som i sin tur leder till den tredje. Volkoff och Strong (2018) menar att affordanser kan vara aggregerade mot varandra och använder ett exempel om äpplen för att illustrera. Äpplet som artefakt ger en aktör en ätande affordans. Den kan aggregeras ner till bitande, tuggande och sväljande affordanser. Jämfört med exemplet skulle affordanserna *att göra intrång* och *åtkomst till data* kunna sägas vara aggregerade under affordansen *åtkomst till och användning av tekniken*. Tydligt är åtminstone att de är beroende i ett på varandra följande led.

Leonardi (2013, se Volkoff & Strong, 2018) delar upp affordanser i olika kategorier beroende på om flera aktörer aktualiserar dem och isåfall på vilket sätt. Vad gäller ovanstående affordanser kan alla tre betecknas som *kollektiva* eftersom alla tre kräver inblandning av flera aktörer med olika typer av arbetsuppgifter men med samma övergripande mål och resultat i sikte. Om dessa övergripande affordanser delas upp i underliggande, mer specifika sådana, kan de dessutom potentiellt vara *delade*. Då flera operatörer kan göra samma mer specifika arbetsuppgift med samma mål.

Utifrån listade element och affordanser söker studien i följande avsnitt ta reda på möjligheter och begränsningar i förhållande till vilka omständigheter som krävs vid användning av hemlig dataavläsning. Återkoppling till resultatet görs genom att de teman som där identifierats används för att gruppera möjligheter och begränsningar. Affordansteorin används här som lins och perspektiv snarare än specifikt ramverk.

5.1.2 Omständigheter kring hemlig dataavläsning

Appliceringen av hemlig dataavläsning är resurskrävande i både tid och pengar. Dels är de tekniska lösningar som potentiellt kan komma att användas dyra, dels är det förarbete som krävs för att veta hur, och ens om, tvångsmedlet kan användas både omfattande och tidskrävande. Hanteringen av resultatet av användningen, den data som tillgängliggörs, kräver i sin tur en ansenlig mängd tid och kompetens för att användbar bevisföring ska kunna tas fram. Dels på grund av att det ofta är stora datamängder som ska sorteras och kategoriseras, dels på grund av att även data i klartext kan kräva avkodning. Den kan vara utskriven i ett språk som inte rakt av förstås av personal inom polismyndigheten vilket kräver anlitande av tolk som blir en extra kostnad. Data kan också vara i form av kodord vilket kräver arbete för att tolkas och förstås. Här ses en koppling med hur Volkoff och Strong (2018) resonerar kring om affordanser kan vara både möjliggörande och begränsande. Trots att åtkomst till data möjliggörs begränsas aktualiseringen av de inneboende krav på resurser som medföljer. Här stärks tanken att affordanser är möjliggörande och begränsande i kombination.

Resultatet visar att det enskilt största syftet med införandet av hemlig dataavläsning är att kringgå kryptering. Enheter, applikationer och data krypteras idag i allt större utsträckning och presenteras som en del av användarfunktionalitet i applikationer som WhatsApp, Signal och Snapchat. Funktionaliteten är en fördel för den genomsnittlige användaren som vill skydda sin personliga integritet. Problem uppstår när brottsliga element använder krypteringen för att planera eller dölja brottslig aktivitet. Hemlig dataavläsning möjliggör användandet av teknik som kommer åt data genom att kringgå kryptering.

Som redan nämnts kräver användningen ett gediget förarbete. Ur ett affordansperspektiv blir en mer detaljerad kartläggning av vad det innebär ett fokus på strukturen, en del av det som definierar aktualisering av affordanser. I jämförelse betecknas själva affordansen av artefaktens funktion och syfte (Volkoff & Strong, 2018). Dessa listades ovan varför en mer strukturell och detaljerad beskrivning av faktorer som påverkar aktualisering bör komplettera och bidra till en rikare kartläggning. Information som påverkar aktualiseringen och därmed behöver inhämtas under förarbetet är bland annat typ av enhet, typ av operativsystem och

vilka applikationer som används. Vidare behövs kännedom om sårbarheter hos en eller flera av ovan nämnda punkter. Dessa sårbarheter införskaffas genom inköp, samarbete med andra myndigheter eller intern forskning. Nästa steg är att genom sårbarheten installera programvara som läser av och sänder data. Utan en sårbarhet måste installationen ske genom andra medel. Exempel som informanterna ger är fysisk åtkomst genom beslag av enhet eller genom att lura målet för avläsningen att trycka på en länk som installerar mjukvaran. Till exempel en operativsystemsuppdatering med en inbakad trojan. Den fysiska åtkomsten är svår att genomföra utan att bli avslöjad och andra sätt kräver sofistikerad maskering av uppsåt och relativt låg IT-kompetens hos målpersonen. En faktor som ytterligare ökar svårigheten med aktualisering är när brottslingar byter telefoner ofta. Detta kan göra att hela processen ovan blir verkningslös. Utöver nämnda faktorer krävs också beslut i domstol för att godkänna användningen av hemlig dataavläsning. Detta medför i sig en juridisk process och ytterligare förarbete för att följa de lagar och regler som styr användningen.

Som synes ovan är aktualiseringsprocessen lång och krävande vilket ytterligare stärker tanken om att affordanser kan vara inneboende begränsande i sitt möjliggörande. Särskiljningen mellan funktion och struktur var användbar för att göra kartläggningen tydligare. Likaså Volkoff och Strongs (2018) princip om fokus på handlingen snarare än resultat i förhållande till aktualisering. Det har lett till en tydlig skiljelinje mellan vad som görs och vad det leder till.

I resultatet var ett tydligt tema kompetens. Alla informanter beskrev en hög spetskompetens men en skiftande och generellt låg it-kompetens överlag i organisationen. De sekundära källorna stödjer den uppfattningen, framförallt Brottsförebyggande rådets rapport som detaljerat beskriver problematiken kring polisens IT-kompetens. Volkoff och Strong (2018) beskriver två problematiker med användning av affordansteorin som går att koppla till kompetens. Den första är problematiken kring om affordanser måste vara uppfattade för att kunna aktualisera. Kontentan av deras argumentation är att nej, de måste inte vara uppfattade men vilken medvetandenivå aktören har kring affordansen kan troligen påverka hur effektivt den aktualiseras. Den andra problematiken handlar om hur aktörers grad av förmåga att aktualisera affordanser påverkar hur applicerbara de är. Här menar Volkoff och Strong (2018) att affordanser är applicerbara oavsett förmåga (bortsett från den grundläggande fysiska sådana) och kunskap om aktualiseringen. Saknas kunskap och förmåga aktualiseras affordansen inte effektivt till en början men eftersom kunskap inte är binärt utan flytande och kan förändras över tid kan aktören bli mer kapabel i aktualiseringen av affordansen. Detta medför att förmåga och kunskap påverkar aktualisering av affordanser beroende på hur mycket av dessa aktörer besitter.

Resultatet visar att tankarna kring medvetandenivå kan stämma. Informant fyra säger uttryckligen att digital bevisning går förlorad på grund av att utredande poliser inte alltid vet när de ska kalla in IT-forensiker. Här kan en ökad medvetandenivå leda till att mer viktig digital bevisning tas om hand och utnyttjas. Andra informanter menar att det finns en flaskhals för utredningen av brott med IT-inslag på grund av att det är få som har tillräckligt med kompetens för att utföra det arbete som krävs. Här ses potentiellt en nivå av förmåga och medvetande som är för låg för att affordanserna

ska kunna aktualiseras av vissa aktörer. Det kan också bero på en medvetandenivå hos styrande element som är låg i förhållande till uppfattning för vilka som potentiellt skulle kunna aktualisera affordanserna, om än ineffektivt jämfört med de fullt kompetenta. En tredje potentiell förklaring skulle kunna vara att styrande element bedömt graden av förmåga korrekt och inga andra än IT-forensikerna har tillräckligt med förmåga och kunskap för att aktualiseringen ska bli så pass effektiv att den är applicerbar. Ingen av dessa tre möjliga hypoteser kan bekräftas av förestående studies resultat, men kan vara av intresse för framtida studier att undersöka.

Ytterligare ett antal faktorer som påverkar kompetens identifieras i resultatet. Rekryterares bristande IT-kompetens leder till låg effektivitet vid anställning och placering av personal. En ökning av rekryterarnas medvetandenivå kring behovet av IT-kompetens i organisationen skulle kunna påverka denna effektivitet på ett positivt sätt. Avsaknande av IT-element i polisens grundutbildning bidrar till en generellt låg förmåga och kunskap kring IT. Vidareutbildningar finns men upplevs av flera informanter som otillräckliga. De menar också att det som enligt studien betecknas som medvetandenivå är låg kring var spetskompetens finns och på vilka sätt den kan stötta övriga avdelningar. Till sist nämns det av flera informanter en resurskopplad faktor som påverkar polisens IT-kompetens. Lönesättningen inom polisen är påtagligt lägre än vad motsvarande kompetens kan ge på andra myndigheter och hos privata företag. Detta bidrar troligen till svårigheter att rekrytera kompetens samt att behålla kompetens inom organisationen.

5.1.3 Svar på studiens frågeställningar

Studiens övergripande frågeställning riktar fokus på användningen av hemlig dataavläsning enligt nedan.

Vilka möjligheter och begränsningar ger det nya tvångsmedlet hemlig dataavläsning för polisen vid utredning av brott?

För att konkretisera delas frågeställningen upp i två frågor riktade mot fördelar och nackdelar med tvångsmedlet:

Vad möjliggörs vid användning av tvångsmedlet hemlig dataavläsning?

Ur studiens resultat framkommer det ett tydligt syfte med tvångsmedlets införande, nämligen att kringgå kryptering av enheter, applikationer och data. Det här är också det som möjliggörs vid användningen av tvångsmedlet. För en konkretisering av vad det innebär kan de identifierade affordanserna med fördel användas. *Åtkomst till, och användning av, tekniken* som gör det möjligt att göra intrång, att faktiskt *göra intrång* samt *åtkomst till data* är alla saker som möjliggörs vid användning tvångsmedlet hemlig dataavläsning. Den data som tillgängliggörs blir förhoppningsvis till användbar bevisföring som kan användas för att uppnå det mer övergripande syftet med tvångsmedlet, fällande domar och minskad grövre brottslighet.

Vilka begränsande faktorer påverkar användningen av tvångsmedlet hemlig dataavläsning?

De begränsande faktorer som framkommit vid analys av resultaten är bristande kompetens kring IT och dess användande inom polismyndigheten, avsaknad av resurser samt en del tekniska komplikationer. Dessa begränsningar är både skilda från varandra men kan även korrelera där exempelvis uppfattningen av IT hos ansvariga påverkar tillgängliga resurser eller löneläget påverkar kompetensbehållning inom polisen.

Vad gäller kompetensen är framförallt den generellt låga nivån av förmåga och medvetande kring IT utmärkande. Detta leder till att den spetskompetens som finns inte utnyttjas effektivt samt till att potentiell digital bevisföring går förlorad. Resursmässigt finns en generell begränsning dels i form av låga tillförda resurser och dels i höga kostnader för tekniska verktyg. Låg lönesättning ses av flera informanter som en stor orsak till svårigheter både för att rekrytera och för att behålla kompetens. Tekniska aspekter som sticker ut är informationskrav för effektiv användning, svårigheter kring att faktiskt applicera programvaran samt att den resulterande datamängd som inhämtas är så stor att ett omfattande hanteringsarbete krävs innan den relevanta bevisföringen kan sorteras fram. Informationskraven innefattar bland annat typ av enhet som ska angripas, typ av operationssystem och vilka applikationer som används. Detta leder till att ett omfattande förarbete med spaning och research krävs. Även när den informationen är inhämtad kvarstår problematiken kring hur programvaran ska appliceras med svårigheter kring fysisk åtkomst eller fjärråtkomst. Hanteringsarbete krävs för att identifiera relevant data bland mängder av icke relevant data även när allt kan avläsas i klartext.

5.2 Studiens praktiska och teoretiska implikationer

I nedanstående avsnitt presenteras hur studien relaterar dels till problemområdets praktiska verklighet dels till relaterad forskning. Slutligen ges förslag på vidare forskning.

5.2.1 Praktiska implikationer för användning av hemlig dataavläsning

Utifrån svar på frågeställningar och den diskussion som förts kring resultatet ställs ett antal förslag upp för hur Polismyndigheten skulle kunna minska eller lätta en del av de identifierade begränsningarna. En nyckelposition verkar vara rekryterare och rekrytering till organisationen. Förutom den självklara men också av resursskäl svåra lösningen, att öka lönesättningen, bör rekryterares medvetandenivå kring kompetensbehov och IT generellt höjas. Det kan åstadkommas antingen genom utbildningar och ökad insyn i IT-forensikers arbete eller genom att IT-forensiker får större eller helt överta inflytandet över rekrytering till sina avdelningar. Det bör leda till rätt kompetens på rätt plats och därmed leda till att minska de flaskhalsar i utredningsarbete av brott med IT-inslag som upplevs idag. Utöver detta är den grundläggande IT-kompetensen ett fortsatt problem. Åtgärder behöver tas för att minska den begränsningen. Tillsammans med allmänna insatser, som att införa IT-element i grundutbildningen, föreslår studiens författare riktade insatser mot exempelvis en person i varje arbetsgrupp. Dessa insatser kan vara utökad fortbildning men helst också en tillfällig förflyttning till de instanser där IT-arbetet

pågår. Detta bör leda till bättre förståelse för hur spetskompetensen ska utnyttjas på bästa sätt.

5.2.2 Implikationer för forskningsfält och vidare forskning

En fråga att beakta vid införandet av en såpass potentiellt integritetskränkande teknik är integritetsaspekten och om tekniken kan användas utanför dess tänkta område. Kritiker till tvångsmedlet bör i dagsläget kunna anse oansvarigt användande som en omöjlighet. De begränsningar studien har identifierat, specifikt resurser, gör en oansvarig användning av tvångsmedlet till en praktisk omöjlighet. Detta gäller i ännu högre grad eventuell massövervakning. Detta helt utan att ta förordningar skapade av lagen i åtanke då det är resurskrävande på en nivå som gör användande utanför det tänkta området omöjligt i dagsläget. Dock bör vidare forskning på området ta i beaktning de möjligheter som kommer med den snabba tekniska utveckling och exempelvis de databearbetningsverktyg som kan komma att trivialisera delar av teknikens användning som i dagsläget begränsar den. Att då vara redo för nya förordningar och kunna göra dessa på ett måttfullt och effektivt vis påverkar framtida möjligheter och begränsningar (Fenwick, Kaal & Vermeulen 2017). Integritetsfrågan måste alltid beaktas men det är tydligt att i kapprustningen mellan polisens tvångsmedel och informationssamhällets teknikanvändning, måste även polisens möjligheter utökas (Solove 2006). Det är en balansgång mellan ansvar och rättigheter.

Delar av resultatet behandlar brottslingars IT-kompetens. Det var svårtolkat utifrån affordansteorin då brottslingarna är en del av målet snarare än användare i föreliggande studie. Dock kan paralleller dras mot relaterad forskning kring hackare, deras kompetens och innovation samt hur organisationer kan utnyttja dem som en resurs. De brottslingar som benämns som mål för tvångsmedlet i studien kan inte klassas som hackare, men de har enligt både informanter och sekundärkällor i många fall hög IT-kompetens och nyttjar anti-forensiska metoder för att dölja och planera brottslig aktivitet, vilket skulle kunna sägas vara motsvarande. Flowers (2008) ställer upp en rad kategorier som behandlar organisationers bemötande av utomlagliga användares innovationer av IT-produkter. På grund av studiens sammanhang och problemområde, där organisationen i fråga är Polismyndigheten och innovationen som sker handlar om kryptering av data och försök att komma runt den krypteringen, faller en del kategorier bort per automatik. Den mest intressanta kategorin enligt studiens författare är den som handlar om *absorbering*. Eftersom det enligt resultatet verkar finnas punktvis väldigt hög IT-kompetens bland brottsliga element, som dessutom har insyn i metoder och rutiner, bör det vara av stort intresse att rikta rekrytering mot dessa individer. Givet organiserad brottslighet och terrororganisationers natur är det inte en enkel uppgift. Ur resultatet går det inte att dra slutsatser om sådana insatser redan görs men detta får förmodas. Kopplingen mellan Flowers (2008) *absorbering* och vad resultatet säger om kriminellas IT-kompetens ger en indikation på att den typen av bemötande kan ge god effekt om det lyckas.

För vidare forskning finns flera intressanta vägar att gå. Den kanske mest relevanta är en mer konkret teknisk studie med utgångspunkt i faktisk användning av tvångsmedlet hemlig dataavläsning. I nuläget är lagen som reglerar användningen tillfällig med en prövotid på fem år. I samband med att prövotiden närmar sig sitt

slut, och med protokoll från fällande domar som del av materialet, kan en klarare bild ges av hur användningen faktiskt kommer att gå till och slutsatser dras om hur effektiv denna användning är. Vidare är det också av intresse att undersöka tvångsmedlets användning i förhållande till personlig integritet. Begreppet ligger utanför föreliggande studies område men har berörts kort och det verkar som att integriteten inte hotas eftersom tvångsmedlets applicering är resurskrävande i en för hög grad. När tvångsmedlet har applicerats i större utsträckning, och denna applicering dokumenterats, finns det mer material och större möjlighet att undersöka frågan. Resursläget kan förändras antingen genom att mer resurser tillsätts eller genom nya tekniska möjligheter varför området bör bevakas framöver.

5.3 Reflektioner kring studiens genomförande och resultat

Studiens explorativa karaktär, och det faktum att användning av den undersökta artefakten inte hunnit dokumenteras, leder till en generellt låg nivå av generaliserbarhet. Det relativt låga antalet informanter ger samma effekt och likaså det faktum att de uttalar sig spekulativt med utgångspunkt som yrkeskunniga och är från samma geografiska region. Studiens tillförlitlighet bör dock under omständigheterna kunna betecknas som tillräcklig. Informanternas utsagor har så långt det gått kompletterats och kontrollerats genom sekundärkällor med hög legitimitet. Intervjuer, kodning, tematisering och analys har efter författarnas bästa förmåga genomförts enligt korrekta metoder. Intervjuguidens utformande stödjer studiens explorativa karaktär och frågornas allmänna natur gav ett rikt och utförligt material att analysera.

Det teoretiska ramverk som använts, teorin om tekniska affordanser, har varit till stor hjälp för att identifiera och kategorisera problemområdets olika beståndsdelar. Som nämnts tidigare är teorin egentligen tänkt att appliceras mot specifik teknik men kan också användas som en lins och ett perspektiv enligt det sätt som föreliggande studie begagnat sig av. Volkoff och Strongs (2018) principer och problematiker kring användningen gav många olika infallsvinklar och termer som var till stor användning för att tematisera och skapa förståelse kring resultatet. Med tanke på att stora delar av svaren från informanterna handlade om resurser och kompetens, områden som kan betecknas som organisatoriska i sin natur, skulle studien potentiellt kunnat genomföras med en organisatorisk teori som stöd. Eftersom fokus låg på användning av en artefakt, hemlig dataavläsning, togs ändå beslutet att hålla fast vid affordanser som centralt begrepp. Detta då teorins koncept kretsar kring just användning.

Målet för undersökningen är ett nyinfört verktyg med syftet att realisera teknik gjord för att ta sig runt kryptering. Detta för att samla data som ska bli bevisföring mot grov och organiserad brottslighet. På grund av detta fanns det redan från början en del farhågor kring hur mycket information som faktiskt skulle gå att utvinna ur informanterna. De var också förtegna kring specifika detaljer och metoder varför resultatet har den mer allmänna och organisatoriska natur det har. Studiens initiala syfte, att kartlägga olika typer av tekniska verktyg som blev applicerbara genom tvångsmedlet, fick även det justeras mot en mer allmän kartläggning. Tillräckligt

med svar av relevant natur gick ändå att få, tack vare informanternas förmåga att tala runt ämnet, för att göra en meningsfull analys.

6 Slutsats

Samhällets användning av teknik ökar och de kriminella blir mer avancerade inom teknologi. Anti-forensiska metoder är en utmaning för polisen som hamnar i en kapprustning mot de kriminella. Det mest använda av dessa anti-forensiska metoder är kryptering. Kryptering avser kryptering av enheter, applikationer och data. Att kringgå kryptering är det viktigaste som möjliggörs vid användning av hemlig dataavläsning. Då tvångsmedlet är det senaste i en rad av tidigare tvångsmedel inom området är det polisens senaste verktyg i den tidigare nämnda kapprustningen och är således den senaste upptrappningen av hemliga tvångsmedel i dagsläget. Det som möjliggjorts är måhända uppenbart men rigida lagar har stiftats runt användningen av detta tvångsmedel för att säkerställa rätt användning vid rätt instans mot rätt individ (*SFS 2020:62*).

Genom att identifiera utmaningar och begränsningar vid användning av hemliga tvångsmedel har studien fastställt att framför allt kompetens och resurser påverkar i vilken grad tekniken blir begränsad i sin användning. De påverkar var för sig men är även kopplade till varandra via rekrytering, kompetensbehållning och kapacitet. Vidare tyder informationen angående löneläge, rekrytering och kompetensbehållning i samklang med Brå (2016) på ett förlegat synsätt avseende IT inom Polismyndigheten. Att det ses som en stödjande funktion snarare än något som genomsyrar hela organisationen och samhället. Även tekniska aspekter begränsar användningen av hemlig dataavläsning. Informationskrav kring vilken typ av enhet som ska avlyssnas, applicering av programvaran och hantering av datamängder gör all användandet resurskrävande.

Referenser

Bell, J. & Waters, S. (2016). *Introduktion till forskningsmetodik.* 5 [uppdaterade] uppl., Lund: Studentlitteratur AB.

Brottsförebyggande rådet (2016). *It-inslag i brottsligheten och rättsväsendets förmåga att hantera dem, Rapport 2016:17.* Stockholm: Brottsförebyggande rådet https://www.bra.se/download/18.3c6dfe1e15691e1603ec36fc/1475217105668/2016_17_It-inslag_i_brottsligheten.pdf

Bryman, A. & Nilsson, B. (2018). *Samhällsvetenskapliga metoder.* 3. uppl., Stockholm: Liber

Flowers, S. (2008). *Harnessing the hackers: The emergence and exploitation of Outlaw Innovation*. Research Policy, 37(2), pp.177–193.

Haikola, S. & Jonsson, S. (2007). *State Surveillance on the Internet – The Swedish Debate and the Future Role of Libraries and LIS*. Libri, 57(4), pp.209–218.

IDG (u.å.). *IT-ord.*
https://it-ord.idg.se/ (hämtad 2020-05-21)

IT-säkerhet (2020). *Patch*
https://www.xn--itskerhet-x2a.com/patch/ (hämtad 2020-05-21)

IT-säkerhet (2020). *Vad är brute force?* https://www.xn--itskerhet-x2a.com/brute-force/ (2020-05-21)

Justitiedepartementet (2019). Faktablad, *Hemlig dataavläsning – ett viktigt verktyg för brottsbekämpningen.* Stockholm: Justitiedepartementet https://www.regeringen.se/4ad5b8/contentassets/ad64b831fcc44d00948e0b1d1862b2b6/hemlig-dataavlasning--ett-viktigt-verktyg-for-brottsbekampningen.pdf

Li, C-Y., Huang, C-C., Lai, F., Lee, S-L. & Wu, J. (2018). *A Comprehensive Overview of Government Hacking Worldwide*. IEEE Access, 6(99), pp.55053–55073.

Malmsten, K. (1992). *Hemlig teleavlyssning och hemlig teleövervakning.* Stockholm: Svensk juristtidning
https://svjt.se/svjt/1992/529 (hämtad 2020-03-16)

Ny Teknik (2020). *Allt du behöver veta om ny teknik #13 Patrick Cordner, Chef SC3 (Nationellt IT-Brottscentrum) Om Modernt Utredningsarbete.*
https://www.nyteknik.se/podcast/13-patrick-cordner-chef-sc3-om-modernt-utredningsarbete-6991279

Patel, R. & Davidson, B. (2011). *Forskningsmetodikens grunder: Att planera, genomföra och rapportera en undersökning*. 4. uppl., Lund: Studentlitteratur AB.

Regeringen (2019). *34-punktsprogrammet: Regeringens åtgärder mot gängkriminaliteten.* Stockholm: Justitiedepartementet https://www.regeringen.se/regeringens-politik/ett-tryggare-sverige/34-punktsprogrammet-regeringens-atgarder-mot-gangkriminaliteten/ (hämtad 2020-05-22)

Regeringen (2019). *Lagrådsremiss Hemlig dataavläsning.* Stockholm: Regeringen https://www.regeringen.se/4ad5b3/contentassets/c6bd2cff11164d62bfdbbe31caea1e05/hemlig-dataavlasning.pdf

Riksrevisionen (2015). *It-relaterad brottslighet – polis och åklagare kan bli effektivare, RIR 2015:21.* Stockholm: Riksrevisionen https://www.riksrevisionen.se/download/18.78ae827d1605526e94b2df0e/1518435506137/RiR_2015_21_IT-relaterade-brott_Anpassad.pdf

Saldaña, J. (2013). *The coding manual for qualitative researchers* 2. ed., London: Thousand Oaks, Calif.: SAGE, 1-32.

SFS 1942:740 *Rättegångsbalk.* Stockholm: Justitiedepartementet http://rkrattsbaser.gov.se/sfst?fritext=1942%3A740&upph=false&sort=desc

SFS 2020:62. *Lag om Hemlig dataavläsning.* Stockholm: Justitiedepartementet http://rkrattsbaser.gov.se/sfst?bet=2020:62

Solove, Daniel J. (2006). *A taxonomy of privacy*. University of Pennsylvania Law Review, 154(3), pp.477–564.

Statens Offentliga Utredningar (2017). *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet. SOU 2017:89.* Stockholm: Statens Offentliga utredningar. https://www.regeringen.se/4ac6ed/contentassets/03541a809a0c4c6183463d15f27fa998/hemlig-dataavlasning--ett-viktigt-verktyg-i-kampen-mot-allvarlig-brottslighet-sou-201789

Tagesson S. (2019). *Anti-Forensik mot minnesforensik.* Kandidatuppsats, institutionen för informationsteknologi. Skövde: Högskolan i Skövde

Vermeulen, E., Fenwick, M. & Kaal, W. (2017). *Regulation tomorrow: What happens when technology is faster than the law*. American University Business Law Review, 6(3), pp.561–594.

Volkoff, O. & Strong D. (2018). *Affordance theory and how to use it in IS research.* In The Routledge Companion to Management Information Systems. Routledge, pp. 232–245.

Wikipedia (2019). *Sabotageprogram* https://sv.wikipedia.org/wiki/Sabotageprogram (hämtad 2020-05-21)

Wikipedia (2020). *Zero-day*
https://en.wikipedia.org/wiki/Zero-day_(computing) (hämtad 2020-05-21)

Åklagarmyndigheten (u.å.). *Ordlista*
https://www.aklagare.se/ordlista/ (hämtad 2020-05-21)

Bilaga 1 - Intervjuguide till IT-forensiker

Inledning

- Kortfattat beskriva bakgrunden och syftet med vårt arbete.
- Förklara att hen kommer att vara anonym.
- Är det okej att ditt svar används i studien?
- Är det okej att vi spelar in intervjun?

Generellt

- Hur länge har du arbetat här?
- Vad har du för titel?
- Utbildning?
- Hur länge har du arbetat inom området?
- Vilka typer av ärenden arbetar ni med?
    - Vilka ärenden kommer att vara relaterade till tvångsmedlet?

Tvångsmedlet

- Hur ser du på det nya tvångsmedlet "hemlig dataavläsning"?
    - Möjligheter/fördelar?
    - Hinder/nackdelar?
    - Effekter?
    - Kompetens?
    - Vad möjliggörs, utöver kryptering t.ex., av tvångsmedlet? Följdfrågor, utforska!

- Hemlig avlyssning av elektronisk kommunikation & Hemlig övervakning av elektronisk kommunikation vs hemlig dataavläsning?
    - Vad är nytt/annorlunda?
    - Applicerbart på mer än organiserad brottslighet?

- Hur ser arbetsprocessen ut i den här typen av fall?
    - Översiktlig genomgång från början till slut?
    - Var i brottsutredningsprocessen tar ni vid?
    - Var i utredningsprocessen lämnar ni vidare?

- Är ni beroende av andra avdelningar i detta arbete och på vilket sätt samarbetar ni?
    - Forensiker
    - Utredare
    - Andra?

Tekniken

- Hur kommer tekniken fungera?
    - Vilka kommer att hantera den faktiska tekniken?
    - Vad kommer tekniken att möjliggöra som är i enlighet med lag/tvångsmedel?

    - Vad möjliggör tekniken som inte får göras?

- Vilka typer av tekniska lösningar kommer att användas för att realisera tvångsmedlet?
    - Zero-day?
    - Kända svagheter?
    - Trojaner?
    - Fysiskt intrång?

- Hur införskaffas de tekniska lösningar som ska realisera tvångsmedlen?
    - Zerodium?
    - Research?
    - Företagssamarbete?

- Risker kopplade med specifika tekniker?
    - Kortsiktiga (Felanvändning, annat)
    - Långsiktiga (Blue sea?)

- Hur ser resultatet av teknikanvändningen ut?
    - Datatyper
    - Mängder

- Vem tolkar resultatet?
    - Flera led?
    - Forensiker
    - Åklagare
    - Andra?

Kompetens

- Hur ser kompetensen ut relaterad till användning av tekniken?
    - Interna utbildningar? Vilka? Hur går man tillväga för att gå dem?
    - Nytt inför den här lagen/tvångsmedlen/tekniken?
    - Policyförändringar?
    - Fortbildning?

- Kringliggande avdelningars kompetens i förhållande till tvångsmedel/teknik
    - Beställare
    - Tolkare
    - Forensiker
    - Åklagare
    - Definition av vad just deras avdelning gör specifikt i förhållande till andra avdelningar. Mer om process och organisation! Följdfrågor, utforska!

- Får ni väldefinierade och konkreta beställningar/arbetsuppgifter?
    - Förstår de som ber er göra saker vad de ber er att göra?
    - Pratar ni samma språk?
    - Kan ni göra allt som de ber er att göra?
    - Kan ni göra mer?
    - Förstår de vad de kan göra med resultatet?

Avslutning

- Finns det någonting som du skulle vilja tillägga?
    - Det kan vara tankar/idéer/insikter som du tror skulle kunna vara relevanta.
- Har du några frågor till oss?
- Vill du att vi skickar det färdiga arbetet till dig?
- Är det okej att maila dig med eventuella kompletterande frågor