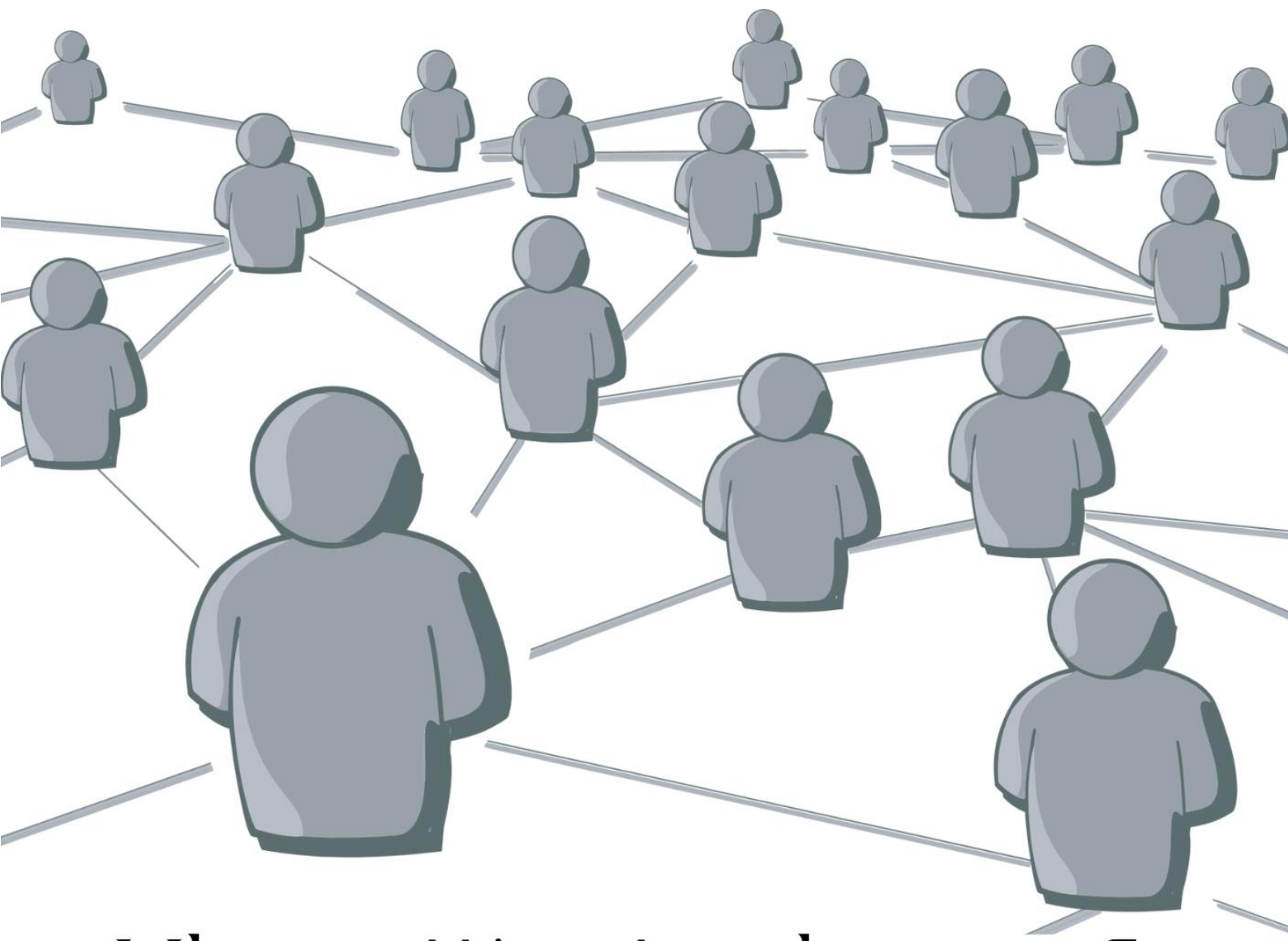


Uberettiget adgang & Ulovlig billeddeling

En kvalitativ Crime Script undersøgelse af, hvordan gerningspersoner opnår uberettiget adgang til intimt materiale samt videredeler dette ulovligt efterfølgende.
Udarbejdet på baggrund af et samarbejde med NC3.

Forfattere:
Katrine Abildgaard Jensen - 20166036
Sara Bunzel Schølarth - 20172967
Victoria Kathrine Kriegbaum Jørgensen - 20175208
Uddannelse & semester: 4. semester speciale på kandidatuddannelsen i Kriminologi, Aalborg Universitet
Gruppenummer: 8
Vejleder: Rasmus Munksgaard
Afleveringsdato: 7. juni 2022
Antal ord: 30.783

Tro- og loveerklæring

Det erklæres herved på tro og love, at jeg/vi egenhændigt og selvstændigt har udformet nærværende opgave. Alle citater i teksten er markeret som sådanne. Jeg/vi er bekendt med reglerne for eksamenssnyd, herunder også plagiering og har læst Aalborg Universitets regler på: https://www.aau.dk/uddannelser/studievejledning/regler/plagiat.

Jeg/vi er bekendt med, at overtrædelse af reglerne vil blive indberettet for rektoratet og i sidste ende kan ende med bortvisning.

Endelig står jeg/vi inde for, at oplysninger om antal ord stemmer overens med virkeligheden.

Abstract

Due to the rapid development of technology, Denmark has become more digitized. Most people have a smartphone and can therefore access the internet at any time. In the light of the digital evolution, cybercrime has thus emerged. This master's thesis is based on a qualitative study in collaboration with *NSK: National enhed for Særlig Kriminalitet, Nationalt Cyber Crime Center (NC3).* The study provides a Crime Script analysis on the steps involved in unauthorized access and illegal image sharing. Our main goal is to contribute to the knowledge of the execution of these criminal acts.

The theoretical framework consists of *Routine activity theory* by Lawrence Cohen and Marcus Felson and *Social learning theory* by Ronald Akers. These theories enable a comprehensive explanation of how crime can occur through environmental and social circumstances. The methodological framework is based on a qualitative approach and is inspired by *Triangulation*. We conducted five interviews with experts and used 30 academic documents as supporting literature in an analytical approach. The purpose of the combination of different empirical data is to get a wide set of explanations on how perpetrators prepare, execute and leave the criminal acts.

With the applied theories, existing research and our own analytic findings, we conducted four Crime Scripts. The main finding of the analysis is a substantial difference between spontaneous and planned unauthorized access and illegal image sharing. The perpetrator can use very simple tactics to get access to sexual material. This is often with reference to an intimate relationship, where casual consensual sharing of sexual content can lead to revenge porn. Additionally, psychological methods such as Social Engineering are more commonly used in the planned execution of unauthorized access. After manipulating and deceiving the victim, the perpetrator can anonymously share the collected material on the dark web through networks such as Tor and VPN. Because of the deep knowledge, as well as the thorough preparations, this group of criminals is thus seen as a complex form of the previous. By determining the steps involved in both spontaneous and planned unauthorized access and illegal image sharing, we can unveil ideas on how to optimize cybercrime prevention in the future.

Forord

Indeværende speciale er udarbejdet i perioden fra februar til juni 2022 og er et resultat af et samarbejde med NSK: National enhed for Særlig Kriminalitet, Nationalt Cyber Crime Center (NC3). I den forbindelse vil vi gerne sende en særlig tak til vores kontaktperson Michael Karpf, som til dagligt arbejder som forebyggelseskoordinator hos NC3. Tak for at introducere os for dette særligt spændende emne samt at hjælpe med etablering af kontakt til relevante fagpersoner.

Ydermere skal der lyde en tak til politikommissær hos NC3 Flemming Kjærside, specialanklager Morten Rasmussen, analytiker hos NC3 Christoffer Herlufsen, post doc forsker Sidsel Harder samt forsker i cybercrime Lene Wacher Lentz, for at have taget sig tid til at bidrage med spændende synspunkter og et indblik i deres arbejde med uberettiget adgang, ulovlig billeddeling samt IT-kriminalitet generelt. Denne viden har oprigtigt bidraget til at belyse indeværende speciales problemstilling.

Sidst men bestemt ikke mindst skal der lyde en stor tak til vores vejleder Rasmus Munksgaard for altid at stå til rådighed ift. støtte og brugbar samt konstruktiv vejledning gennem hele specialeskrivningsprocessen.

Dette speciale er udarbejdet af:
Katrine Abildgaard Jensen
Sara Bunzel Schølarth
Victoria Kathrine Kriegbaum Jørgensen

Indholdsfortegnelse

Kapitel 1
Litteratursøgningsproces

1. Litteratursøgningsproces

Det indledende arbejde i indeværende speciale bestod af en udførlig litteratursøgningsproces. På denne måde kunne vi tilegne os en bred forståelse af indeværende speciales omdrejningspunkt omhandlende uberettiget adgang samt ulovlig billeddeling. Selvom at søgningen i høj grad blev tilrettelagt på forhånd, var der stadig plads til overvejelser og refleksion omkring specifikke søgeord og valg af databaser undervejs i processen. De hyppigst anvendte informationskilder visualiseres i en tabel, som fremgår i Bilag 1. Heri indgår der databaser såsom Google, Google Scholar samt Primo. Selve ordsøgningen på disse databaser er delt ind i forskellige 'led'. Et udsnit af de ord der oftest blev søgt på illustreres i Bilag 2. Herunder fremgår der både danske og engelske termer. Det er således ikke alle søgninger og informationskilder som præsenteres i bilagene men derimod blot et udkast af særligt relevante begreber i henhold til granskning af viden på området. Følgende afsnit består af en kort beskrivelse af, hvordan litteratursøgningen har fundet sted.

Første led bestod af en overordnet søgning på IT-kriminalitet generelt, således at der blev skabt et overblik over, hvilket kriminologisk område vi i specialet bevæger os inden for. Eksempler på søgninger relateret hertil er: *Cybercrime, udviklingen af internetkriminalitet* og *computer network* (Bilag 2). Udover at søge i diverse databaser (Bilag 1), og efter bestemte nøgleord (Bilag 2), er der ligeledes blevet gjort brug af *Snowball-effekt* (Wohlin, 2014, s. 1). Med dette menes der, at én udgivelse ofte har givet anledning til, eksempelvis gennem den pågældende litteraturliste, at stifte bekendtskab med andre udgivelser, der kunne være relevante at inddrage i belysningen af specialets emne. Denne fremgangsmåde har således været med til at udbrede vores kendskab til allerede eksisterende litteratur og yderligere spore os ind på det specifikke afgrænsede felt for specialet.

Andet og *tredje led* indebar tilnærmelsesvis den samme proces. Andet led bestod af en søgning på de omstændigheder, der gør sig gældende hos uberettiget adgang og ulovlig billeddeling, heriblandt *digitale krænkelser, brugen af sociale medier* og *online efterforskning*. Dette muliggjorde, at der kunne dannes et overblik over, hvilke konsekvenser kriminalitetsformerne har haft, hvordan andre har undersøgt selvsamme emne, samt hvilket fokus der har været rettet imod fænomenerne i både dansk såvel som international kontekst. Omdrejningspunktet i tredje led var i højere grad rettet mod den konkrete problemstilling, dvs. udførelsen af de to kriminalitetsformer, samt de fænomener og omstændigheder, som typisk kobler sig hertil.

Social Engineering og *Image-based sexual abuse* er blot nogle af de specifikke fænomener, der blev søgt på i tredje led. En fordelagtig forskningskilde der blev anvendt for at brede søgningen yderligere ud, var *Connected papers* (Bilag 1). Dette er et visuelt værktøj, der finder relevant akademisk arbejde, der har ligheder til den litteratur, der søges på. Det gjorde litteratursøgningsprocessen lettere og muliggjorde samtidig, at vores faglige horisont blev udvidet yderligere.

Foruden ovenstående litteratursøgningsprocesser har vi også undersøgt, hvilke artikler i de danske medier, der gør sig gældende, når det omhandler specialets fokusområde. Vi er her stødt på artikler fra forskellige udgivere, hvori vi har opnået et større kendskab til, hvad der er sket i dansk kontekst de sidste par år. Dog er det vigtigt at understrege, at disse avisartikler mm. udelukkende er brugt som baggrundsviden og til at underbygge væsentlige pointer, da vi selvfølgelig er bekendt med eventuelle faldgruber ved at benytte mediedækning som kilde. Disse faldgruber dækker bl.a. over, at journalister uddannes til at formidle artikler på en bestemt måde, og der derfor kan foreligge en skjult agenda bag (Duedahl & Jacobsen, 2010, s. 32). Ikke desto mindre giver artiklerne et indblik i de problematikker, der eksisterer i det danske samfund i relation til specialets emne, hvilket synes relevant i forståelsen af opnåelsen af uberettiget adgang og ulovlig billeddeling.

Kapitel 2
Problemfelt

2. Problemfelt

I dette kapitel introduceres problemfeltet, som er udarbejdet med henblik på at danne et overblik over den relevante og eksisterende litteratur og forskning, der forefindes om uberettiget adgang samt ulovlig billeddeling. Sidst præsenteres problemformuleringen, som er en præcisering af det problem, der således undersøges.

2.1 IT-kriminalitet

Et stort udbud af digitale tjenester, som danske borgere og virksomheder har taget til sig, har medvirket til at FN i 2020 for anden gang i træk kårede Danmark som det land, der er længst fremme ift. offentlig digitalisering. IT spiller derfor en stor rolle i danskernes arbejds- og privatliv (Digitaliseringsstyrelsen, 2020; DKR, 2021, s. 7). Det er eksempelvis blevet en del af dagligdagsrutinerne at logge på netbank, at kommunikere med virksomheder via e-mail, at pleje sine relationer gennem online chats samt at bestille varer med et enkelt klik (Kruize, 2013, s. 14; DKR, 2021, s. 5). I 2020 var der hele 97 % af danske familier, som havde internetadgang i hjemmet, 96 % havde en mobiltelefon og 91 % havde en PC (Danmarks Statistik, 2020, s. 7). Disse høje procenter visualiserer og understreger altså, hvor stor en del digitale tjenester faktisk fylder i den danske befolknings hverdag. Dog har udviklingen ligeledes påvirket karakteren af kriminalitet og afvigelse, hvilket ydermere har affødt IT-kriminalitet (Holt & Bossler, 2016, s. 1; DKR, 2021, s. 5; Kruize, 2013, s. 15).

IT-kriminalitet har ikke en entydig definition, da betegnelsen dækker over flere forskellige kriminalitetsformer. I 1970'erne blev termen *Computer crime* anvendt til at beskrive misbruget af computere og data. Internettet blev stort set ikke anvendt af almene borgere på daværende tidspunkt, hvorfor det hovedsageligt var medarbejdere, der havde adgang hertil, og som dermed havde mulighed for at begå denne form for kriminalitet (Holt & Bossler, 2016, s. 6). I takt med den teknologiske udvikling ændrede terminologien sig. I slutningen af 1990'erne omtalte David Wall kriminalitet, der blev udført online som *Cybercrime*. Peter Grabosky anvendte derimod den første term computer crime til at referere til computermisbrug, hvor gerningspersonen anvender speciel viden omkring computerteknologi (Holt & Bossler, 2016, s. 6). Flere nutidige forskere har dog adopteret betegnelsen cybercrime til forklaring af forbrydelser, der sker i online miljøer (Holt & Bossler, 2016, s. 7).

Yderligere beskrev Europol IT-kriminalitet i 2021 som følgende:

> *"Criminals are digital natives. Virtually all criminal activities now feature some online component and many crimes have fully migrated online. Criminals exploit encrypted communications to network among each other, use social media and instant messaging services to reach a larger audience to advertise illegal goods, or spread disinformation"* (Europol, 2021).

Som citatet indikerer, kan IT-kriminalitet foregå på flere forskellige måder, dog med *online* som den væsentligste komponent. Det er derfor også forskelligt, hvor stor en mængde af teknologisk viden, typerne af IT-kriminalitet kræver. Eksempler på IT-kriminalitet der kræver en vis mængde af teknologisk viden for at kunne udføres er identitetstyveri, databedrageri, informationstyveri og traditionel hacking (Viano, 2017, s. 3). Ikke desto mindre spiller teknologi en væsentlig rolle i relation til IT-kriminalitet, enten med elektroniske enheder som et tilsigtet mål, eller som et værktøj der bruges til at begå de forbrydelser, der påvirker individer, organisationer eller statslige enheder (Viano, 2017, s. 4). Definitionen af IT-kriminalitet fremstår derfor mangefacetteret. I dansk litteratur anvendes der eksempelvis betegnelserne *IT-kriminalitet, Internetkriminalitet* og *Cyberkriminalitet* til at beskrive selvsamme fænomen (DKR, 2021, s. 5; Danmarks statistik, 2020, s. 39; Kruize, 2013, s. 15). For simplicitetens skyld vil *IT-kriminalitet* være den betegnelse, som indeværende speciale benytter i belysningen af kriminel aktivitet, der udføres online.

2.1.1 Kriminalitetsformer

Det er omdiskuteret blandt kriminologer, hvorvidt IT-kriminalitet består af særegne kriminalitetsformer, eller om betegnelsen kan forklares ud fra eksisterende teorier, der gør sig gældende i den *offline* verden (Kruize, 2013, s. 16; Kruize, 2018, s. 17). For at kortfatte IT-kriminalitet anvendes Walls typologi fra 2001, hvori der indgår eksempler på *Computer-assisterede aktiviteter*, som har ligheder til kriminelle handlinger i den fysiske verden, og *Computer-fokuseret aktiviteter* som er særskilt den virtuelle verden (Holt & Bossler, 2016, s. 15). Wall opdeler IT-kriminalitet i fire kategorier, som indkapsler online kriminel adfærd (Holt & Bossler, 2016, s. 11). Kategorierne, der præsenteres i følgende afsnit, anses som værende idealtyper, da de forskellige kriminalitetsformer sjældent kun falder inden for den enkelte kategori.

Forbrydelser relateret til *Cyber-trespass* har til hensigt at få adgang til computersystemer, e-mail-konti eller beskyttede netværk, som gerningspersonen ikke ejer. Der bliver således krydset usynlige, dog etablerede, grænser af ejerskab i disse online miljøer. Det er forbrydelser, der skader computeren i form af eksempelvis hacking og distribuering af malware, heriblandt virus, orme eller trojanske heste programmer, botnets mm. Hver metode har sine egne karaktertræk, men de kan alle anvendes til flere forskellige formål. Det kunne eksempelvis være at forringe netværksforbindelsen, få adgang til filer, slette materiale eller aktivere computeren, således at den kan blive fjernstyret af gerningspersonen (Holt & Bossler, 2016, s. 11). Disse former for forbrydelser, der er rettet imod selve computeren, kan anses som værende nye ift. de traditionelle offline kriminalitetstyper (Kruize, 2013, s. 16). Cyber-trespass kriminalitet defineres derfor af Wall som computer-fokuseret kriminalitet, da adgang til disse systemer opstod som følge af computerens opfindelse (Holt & Bossler, 2016, s. 15).

Den anden kategori i Walls typologi, *Cyber deception and theft*, omfatter brugen af internettet til at stjæle information eller ulovligt at tilegne sig værdigenstande fra enten individer eller virksomheder. Kategorien hænger derfor ofte sammen med cyber-trespass, eftersom hackere ofte forsøger at indfange følsomme oplysninger og data gennem ulovlig indtrængen (Viano, 2017, s. 5). Hackere retter sig typisk mod finansielle, medicinske og statslige institutioner for at stjæle store mængder data. Dette har medført en stigning i online markeder, hvor kriminelle kan sælge stjålne data til andre såsom kreditkortnumre (Holt & Bossler, 2016, s. 12). Derudover henviser Wall til romance scams, aktiemanipulation, e-mail scams og piratkopiering i relation til online tyveri (Holt & Bossler, 2016, s. 12-13).

Walls tredje kategori, *Cyber porn and obscenity*, repræsenterer seksuelt materiale online, heriblandt pornografi, sexturisme og pædofili. Internettets anonymitet muliggør, at individer kan deltage i online aktiviteter, som ikke accepteres i det større samfund. Nogle aktiviteter kan derfor være legale, heriblandt pornografi med aktører over 18 år, såfremt at det er i Danmark. Hvis det derimod indebærer personer under 18 år, er der tale om kriminelle aktiviteter ifølge straffelovens § 235 (Holt & Bossler, 2016, s. 13; Viano, 2017, s. 5), hvilket uddybes yderligere i afsnit 2.3.2 omkring relevante paragraffer. Ovenstående har nuvel eksisteret inden internettets fremtræden, hvilket betyder, at det er computer-assisteret kriminalitet. Dog har den online anonymitet og globale tilgængelighed skabt et miljø, der fremmer skabelsen og delingen af denne form for materiale (Holt & Bossler, 2016, s. 14-15).

Cyber violence, som er den fjerde kategori Wall præsenterer, indebærer de forskellige måder hvorpå individer gennem teknologi kan forårsage skade i virkelige eller virtuelle miljøer (Viano, 2017, s. 6; Holt & Bossler, 2016, s. 14). Typisk er det emotionel skade gennem skam eller stigma hos offeret. Dog kan fysisk skade ske, hvis individet internaliserer smerte på sig selv i form af eksempelvis alkoholmisbrug eller selvmord (Holt & Bossler, 2016, s. 14). Nogle typiske cyber-voldelige handlinger er stalking, chikane og mobning (Viano, 2017, s. 6; Holt & Bossler, 2016, s. 15). Teknologien giver adgang til materiale og information, som kan være skadeligt, såfremt de ender hos en motiveret gerningsperson, der har ønske om at anvende det mod et tilsigtet mål (Holt & Bossler, 2016, s. 15).

2.1.2 Mørketal

Der findes ikke et konkret tal på, hvor mange kriminelle aktiviteter der i så fald udspiller sig online. Gerningspersonen kan i langt højere grad være anonym samt anvende skiftende metoder for at opnå deres fremsatte mål. Ydermere kan der eksistere et mørketal i relation til IT-kriminalitet, dvs. kriminalitet der aldrig bliver anmeldt til politiet (Sørensen, 2013, s. 26). Dette kan variere i størrelse afhængig af, hvilken kategori kriminalitetstypen hører under. Nogle eksempler på hvorfor der eksisterer et mørketal blandt IT-kriminalitet kan bl.a. være, at offeret ikke har vurderet hændelsen som ulovlig eller særlig alvorlig, eller at offeret ikke tror, at politiet vil tage anmeldelsen alvorlig og dermed håndtere den (Justitsministeriets Forskningskontor, 2021, s. 121-123). Ydermere kan der argumenteres for, at det faktum at få stjålet eller delt eksempelvis intimt materiale af sig selv kan være yderst grænseoverskridende for offeret, hvilket kan afholde vedkommende i at gå videre med det til politiet (Bejder, Sørensen, Pihl, Spanier & Jørgensen, 2014, s. 22; Kruize, 2018, s. 13-14).

Der kan derfor argumenteres for, at mørketallet for IT-kriminalitet kun kan reduceres, hvis ofrene hyppigere rapporterer disse forbrydelser, således der faktisk registreres et mere realistisk antal på, hvor mange der bliver udsat for kriminalitet online. Dette vil ydermere også være nødvendigt for, at der hos politiet prioriteres flere ressourcer til området, hvilket unægteligt vil skabe bedre muligheder for at bekæmpe IT-kriminalitet (Waschke, 2017, s. 169-171). I forlængelse heraf argumenterer daværende politiinspektør hos NC3 Claus Birkelyng for, at selve det at anmelde en kriminel handling er blevet lettere, da politiet i april 2019 gjorde det muligt at anmelde digitalt på politiets hjemmeside, hvor anmelderen her bliver mødt af guides, som hjælper politiet med at få de rette informationer fra start af. Inden denne mulighed for

digital anmeldelse gjorde det sig gældende, at offeret enten skulle møde op fysisk på den lokale politistation eller ringe 114 (Ritzau, 2020a). Der er derfor sket en forbedring ift. ofres muligheder for at anmelde IT-kriminalitet. Alligevel anser vi stadig feltet som værende kompliceret, hvorfor dette kræver yderligere fokus.

2.1.3 Efterforskningsmuligheder

IT-kriminalitet anses som et stigende problem i takt med, at samfundet netop bliver mere digitaliseret. Dette har også betydning for politiets efterforskning, da den online verden anses som værende et mere aktuelt område end tidligere netop grundet den stigende digitalisering. Det problematiske herved er, at der stadig mangler bestemmelser, som er eksplicitte omkring, hvad politiet må og ikke må foretage sig på internettet. Retsplejeloven fastsætter de rammer, politiet skal indordne sig efter i den offline verden i forbindelse med efterforskning af diverse forbrydelser. Dette kan eksempelvis omhandle, hvordan en afhøring skal foregå, hvornår retten skal give lov til politiets indgreb over for en borger mm. Retsplejelovens regulering er fremsat således, at jo grovere en forbrydelse er, desto mere må politiet gøre i forbindelse med efterforskningen (Lentz, 2018, s. 137). Der foreligger altså klare retningslinjer omkring, hvad politiet er berettiget til at gøre i relation til efterforskning i den fysiske verden. Dette gælder dog ikke bestemmelser omhandlende internettet, da sådanne bestemmelser netop ikke findes eksplicit i lovteksten. Der er eksempelvis ikke klare regler om, hvordan politiet kan infiltrere og overvåge de sociale medier for bl.a. falske profiler (Lentz, 2018, s. 138). At bestemmelser omkring politiets efterforskning på internettet ikke fremgår i retsplejeloven gør, at det er op til domstolene at tage stilling ud fra den enkelte forbrydelse. Domstolene må således, fra sag til sag, sammenholde de nye efterforskningsmetoder med retsplejelovens bestemmelser om bl.a. ransagning og telefonaflytning. Her skal dommeren således gøre op med, hvorvidt der forefindes lovhjemmel til den nye efterforskningsmetode, hvad den nye metode minder mest om ift. det, der står i retsplejeloven, samt hvor intensivt den nye metode synes at være for den enkelte borger (Lentz, 2018, s. 138).

Fraværet af manglende klare lovregler omkring efterforskning på internettet, samt tilstrækkelig og udførlig retspraksis herfor, kan give flere udfordringer. Der er bl.a. risiko for at efterforskningen, på baggrund af de nye digitale kriminalitetsformer, går for langt og dermed risikerer at krænke borgeren. Omvendt er der også den risiko, at politiet af (over)forsigtighed

dropper en efterforskning, selvom at den både er legitim og nødvendig for at opklare den pågældende forbrydelse (Lentz, 2018, s. 139).

Ved IT-kriminalitet er der mindre risiko for, at eksempelvis hackere kan blive opdaget, da de som bekendt i højere grad kan fremstå anonyme og derfor langt nemmere kan skjule sine spor. Derudover vil det fra politiets side være vanskeligt at opklare og retsforfølge gerningspersonerne, da det ofte kræver involvering fra andre lande (Demant, Jørgensen & Harder, 2018, s. 47; Center for cybersikkerhed, 2021, s. 4-5; DKR, 2016, s. 10). Den foreliggende forskningslitteratur indikerer altså et bredt felt inden for IT-kriminalitet, som har udviklet sig gennem flere årtier i takt med den fremskredne teknologi. Der skal ydermere tages højde for andre faktorer, når kriminaliteten foregår online i stedet for offline. Det at skaffe sig uberettiget adgang til en anden persons platforme er blot en af de kriminalitetsformer, der har mangeartede facetter, og som har vundet indpas i den generelle forståelse af IT-kriminalitet. Dette vil følgende afsnit således belyse.

2.2 Uberettiget adgang til intimt materiale

Politiet definerer uberettiget adgang som følgende:

> *"Uberettiget adgang er, når nogen skaffer sig adgang til din computer, dine programmer, din e-mail eller sociale profil uden din tilladelse. Det kan fx indebære, at der er nogen, der sletter, ændrer eller kopierer dine oplysninger"* (Politi, s.d.-a).

Ud fra den danske straffelov er det ulovligt, når en person uberettiget skaffer sig adgang til et datasystem (Digitalt ansvar, s.d.). Når individet opnår adgang til dette på illegal vis, kan der således straffes efter Straffelovens § 263 stk. 1:

> *"Med bøde eller fængsel indtil 1 år og 6 måneder straffes den, der uberettiget skaffer sig adgang til en andens datasystem eller data, som er bestemt til at bruges i et datasystem"*

Der eksisterer dog flere forskellige måder at opnå denne uberettigede adgang på. Følgende afsnit indebærer en beskrivelse af Social Engineering; en hyppigt anvendt metode inden for uberettiget adgang til andres platforme.

2.2.1 Social Engineering

I takt med den øgede digitalisering er det i højere grad blevet en nødvendighed med datasikkerhed. Der anvendes varierende typer af teknologi for at forhindre, at andre får uberettiget adgang til ens sensitive oplysninger. Uanset hvor opdateret ens software er, og hvilke antivirusprogrammer der er installeret, vil der dog samtidig altid være en grad af sårbarhed - nemlig *mennesker* (Lohani, 2019, s. 385). Fænomenet Social Engineering kan defineres og forstås på flere forskellige måder. I indeværende speciale vil begrebet defineres som en psykologisk manipulation af en bestemt adfærd, eksempelvis i form af bedrag. Ofre for denne metode er ofte intetanende omkring, at gerningspersonen forsøger at narre vedkommende til at udlevere private oplysninger såsom et kodeord. Denne manipulation omfavner bl.a. venskab eller romantik, netop med det for øje at opbygge et tillidsforhold til det pågældende offer, for derefter at udnytte dette forhold til at få adgang til de pågældende oplysninger (Chantler & Broadhurst, 2008, s. 1). Social Engineering er således en hyppig anvendt metode blandt kriminelle, da den typisk anses som mindre krævende end traditionel hacking. Dette skyldes, at det ofte er nemmere at udnytte folks tillid, end det er at opdage forskellige måder, hvorpå offerets software kan hackes. Et eksempel hertil er, at det vurderes relativt let at narre et kodeord fra et offer, sammenlignet med det at forsøge at gætte og hacke sig frem til selvsamme adgangskode (Webroot, s.d.).

Eksisterende litteratur påviser, at der dog kan opstilles et generelt mønster i angrebet, hvori der indgår fire faser: 1. Indsamling af oplysninger om målet, 2. Udvikling af et forhold til målet, 3. Udnytte den tilgængelige information og herefter udføre selve angrebet, og 4. Forlade uden nogle spor (Salahdine & Kaabouch, 2019, s. 2; Chantler & Broadhurst, 2008, s. 4-5). Konkret gør det sig gældende, at gerningspersonen udvælger sit offer på baggrund af specifikke krav. Herefter vil gerningspersonen således forsøge at skabe et tillidsbånd til offeret enten gennem en mere direkte kontakt eller via e-mail kommunikation. Dette tillidsbånd kan således fordre, at offeret udleverer personlige oplysninger til gerningspersonen og dermed falder i gerningspersonens fælde. Det tilegnede materiale kan eksempelvis anvendes til personlige formål eller som en salgsvare på det sorte marked eller mørkenet (Salahdine & Kaabouch, 2019, s. 2). Slutteligt er det gerningspersonens job at forlade situationen uden nogle former for spor, så vedkommende ikke bliver opdaget (Salahdine & Kaabouch, 2019, s. 2). Dog er det væsentligt at have for øje, at hvert Social Engineering-angreb er unikt, hvorfor der højst sandsynligt kan forefindes flere faser (Chantler & Broadhurst, 2008, s. 5).

Et eksempel på en særdeles aktuel sag fra Danmark omhandlende Social Engineering, er den mediedækkede hackersag fra Herning, som i skrivende stund verserer for Herning Byret. Her udnyttede gerningspersonen således ofrene ved at udgive sig for at være deres veninde, eller hjælpe dem med at fjerne virus fra deres computer for på den måde at lokke adgangskoder ud af dem (Midt- og Vestjyllands politi, 2021; Ritzau, 2022a).

Social Engineering skal således anskues som én måde at opnå uberettiget adgang til ofrenes intime materiale. Denne metode er dog særdeles avanceret at forebygge. Den anses nemlig for at udfordre teknologiens sikkerhed, forstået på den måde, at ældre og velkendte teknologiske sikkerhedsprogrammer såsom firewalls, systemer til registrering af uberettiget adgang samt anti-virusprogrammer ikke beskytter mod denne type angreb (Salahdine & Kaabouch, 2019, s. 1). Yderligere kan der argumenteres for, at denne form for angreb ikke umiddelbart kan stoppes, men blot opdages og forsøges forebygges (Salahdine & Kaabouch, 2019, s. 2).

Det vurderes, at Social Engineering bedst kan indfanges af Walls kategori Cyber deception and theft. For at kunne opnå adgang til eksempelvis intimt materiale, kræver det indhentning af specifikke oplysninger fra det pågældende offer. I henhold til Social Engineering kan dette gøres gennem netop bedrag eller et tillidsbrud (Chavez & Bichler, 2019, s. 102; Chantler & Broadhurst, 2008, s. 1). Disse oplysninger kan således anvendes til vidt forskellige formål, heriblandt online deling eller salg af de tilegnede private billeder (Holt & Bossler, 2016, s. 12).

2.3 Ulovlig billeddeling af intimt materiale

Ulovlig billeddeling er en kriminalitetsform, der medfører digitale krænkelser hos ofrene. Rigspolitiet definerer en digital krænkelse som følgende:

> ” *[…] En handling, hvor nøgenbilleder eller video/billeder af seksuel karakter bliver delt eller offentliggjort uden tilladelse fra den afbildede person. Digitale sexkrænkelser foregår typisk via sociale medier, online fora, private mobilbeskeder samt applikationer til smartphones. Gerningsstedet vil ofte omfatte internetplatforme såsom hjemmesider, sociale medier og fildelingstjenester, der typisk er placeret på servere, der kan være placeret i udlandet”* (Rigspolitiet, 2018).

Sager herved handler oftest om, at gerningspersonen tilegner sig privat materiale samt information, som kan bruges til at skade et enkelt individ eller gruppe. Materialet kan derfor

bl.a. benyttes til at nedgøre, udstille, afpresse eller true offeret. I indeværende speciale beskrives ulovlig billeddeling som en handling, hvor der opnås adgang til andre personers intime billeder og/eller videoer i form af online videredeling uden ophavsmandens samtykke. Et eksempel på en aktuel sag i dansk kontekst er sagen fra Hillerød, som der netop er faldet dom i. Her medgiver gerningspersonen at have delt en mappe med over 800 unge forurettede i (Ritzau, 2022b; Ritzau Krimi, 2022). I sager som disse opstår der derfor uberettiget adgang på ny, hver gang et nyt individ får fat i det intime materiale.

Som tidligere argumenteret for i afsnit 2.1, omhandlende IT-kriminalitet, sker der en stadig stigning i anmeldelser om IT-kriminalitet generelt, hvilket også gør sig gældende for ulovlig billeddeling. Statistik fra politiet viser, at der i 2017 var 324 anmeldelser omhandlende ulovlig billeddeling, hvor tallet i 2018 var 428. I begyndelsen af december 2019 var tallet dog steget til 688 anmeldelser. Det er dog svært at konkludere, hvorvidt der reelt er sket en stigning i ulovlig billeddeling, eller den stigende anmeldelsesprocent i stedet skyldes større opmærksomhed på denne kriminalitetsform, og der dermed er sket en form for aftabuisering (Ritzau, 2020a). Opmærksomheden omkring ulovlig billeddeling er ikke desto mindre skærpet de seneste par år. Stifter af foreningen Digitalt Ansvar Miriam Michaelsen mener, at dette kan skyldes, at den generelle holdning til området er ændret, således at skylden ikke længere foreligger hos offeret. Hun argumenterer yderligere for, at vi ikke skal lang tid tilbage, før at selv politiet gjorde brug af såkaldt *victim-blaiming* i sager omhandlende digitale krænkelser. Forhåbningen hos hende er, at der, efter Umbrellasagen i 2015[1], eksisterer en generel forståelse for, at ulovlig billeddeling har samme alvorlige konsekvenser som krænkelser i den offline verden (Mølgaard, 2019, s. 197-199). Lina Sjögren, som er leder og psykolog ved Red Barnet, argumenterer for, at der dog stadig foreligger en forskel i konsekvenser af online- og offline kriminalitet. Hun pointerer, at overgreb i den fysiske verden har et start- og sluttidspunkt, hvilket krænkelser på nettet ikke nødvendigvis har, da det ikke kan udelukkes, at materialet bliver opbevaret andetsteds. At skaffe uberettiget adgang til personers private filer, herunder intime billeder og videoer, må derfor have betydelige følgevirkninger for offeret, heriblandt angst, social isolation, depression, søvnbesvær, skyld og skam (Mølgaard, 2019, s. 131-134; Call, 2021, s. 32).

[1] En sag hvor over 1000 unge blev sigtet for børneporno ved at have delt et videoklip af to 15-årige. Sagen har herefter medført et aldeles stort fokus på digitale krænkelser (Ritzau, 2020b).

Der hersker altså ingen tvivl om, at digitale krænkelser, herunder på baggrund af ulovlig billeddeling, de sidste par år har vakt stor interesse i både medierne, hos politiet samt politikerne. Bl.a. skrev Berlingske i 2020 artiklen "*Anmeldelser af billeddelinger er fordoblet på få år"* (Ritzau, 2020a), og Jyllands-Posten i 2021 artiklen "*Kære regering: Digitale krænkelser blandt unge kræver større indsats"* (Christensen, 2021). Derudover beskriver Jakob Demant, hvordan der i dagens Danmark hersker en myte omkring, at langt de fleste unge, som modtager nøgenbilleder, sender disse videre. Demant argumenterer yderligere for, at det bl.a. er medierne, der er med til at skabe dette syn på ungdommen, men at befolkningen aldrig bliver gjort bekendt med dem, der tager den rigtige beslutning og netop ikke videresender dette intime materiale. Denne forståelse er ud fra data, som stammer fra Ungeprofilundersøgelsen 2017, hvor flere end 60.000 unge deltog. Tallene heri viser, at fire ud af fem unge altså ikke vil videresende intime billeder eller videoer. At diskursen i medierne påpeger det modsatte, kan således være med til at skabe den såkaldte *Flamingoeffekt*, hvor de unge tror, at normen er at videresende disse materialer uden samtykke, hvorfor dette netop vil få flere til at agere herefter (Mølgaard, 2019, s. 125-127).

2.3.1 Forebyggende indsatser og rådgivning

I takt med at fokusset på ulovlig billeddeling er blevet større, er der ligeledes et bredere fokus på forebyggelsen heraf. Fyns Politi, samt politikredsens kommuner, har udarbejdet en samarbejdsplan for 2022, hvori der forekommer ekstra fokus på samarbejdet omkring kriminalitetsforebyggelse på flere områder, herunder forebyggende indsatser mod børn og unges digitale risikoadfærd. I denne samarbejdsplan argumenteres der ligeledes for, at i takt med interessen for digitale medier stiger, stiger IT-kriminaliteten ligeså. Eksplicit viser Fyns politis analyse, at det særligt er ulovlig billeddeling, hvor de unge kommer i problemer (Politi, 2022, s. 8). Derudover var vinderen af *Den kriminalpræventive Pris* i 2017 undervisningsmaterialet *Dit Liv På Nettet*, hvilket er udviklet af Skoleforvaltningen i Aalborg Kommune i samarbejde med Center for Digital Pædagogik. Materialet omfavner ideen om tidlig information omkring digital adfærd som helhed, hvor hensigten er at øge elevers trivsel samt dannelse gennem bl.a. viden, refleksion og dialog omkring digital adfærd og liv (DKR, 2017). Ydermere gik Regeringen ind i kampen om at skærpe indsatsen mod digitale krænkelser med rapporten *Skærpet indsats mod digitale sexkrænkelser* fra 2017. I rapporten indgår bl.a. initiativer omkring højere straf, bevissikring, hjælp til ofrene samt etablering af hotline om krænkende adfærd i ungdomsuddannelserne (Regeringen, 2017).

Indeværende afsnit tydeliggør således aktuelle eksempler på relevante forebyggelsestiltag samt forslag hertil. Disse forskellige indsatser tyder ligeledes på, at der i højere grad end før er brug for fokus på oplysning og generelle initiativer for at imødekomme IT-kriminalitet såsom ulovlig billeddeling. For at kunne danne sig et bedre overblik omkring netop ulovlig billeddeling i juridisk forstand, vil vi derfor i følgende afsnit præsentere væsentlige paragraffer, som knytter sig hertil.

2.3.2 Hvad siger loven?

Når man i et juridisk perspektiv beskæftiger sig med ulovlig billeddeling, er særligt tre paragraffer relevante. Nedenstående repræsenterer således de tre mest anvendte, når det omhandler digitale krænkelser:

Straffelovens § 232: Omhandler blufærdighedskrænkelse. At krænke andres blufærdighed kan gøres på flere forskellige måder: At dele uden samtykke, krænkende kommentarer samt uopfordrede billeder af eksempelvis kønsdele.

Straffelovens § 235: Børnepornobestemmelsen. Omhandler udbredelse og besiddelse af pornografiske billeder eller videoer af personer under 18 år. Det er vigtigt at have in mente, at selvom den seksuelle lavalder i Danmark er 15 år, må billeder og videoer af seksuel karakter af børn og unge under 18 år aldrig deles videre. Dette gælder også på trods af at vedkommende har givet samtykke. Derudover må billeder og videoer af seksuel karakter af børn og unge under 15 år aldrig gemmes. Dette gælder også, selvom vedkommende selv har sendt det og har givet samtykke. Det skyldes, at børn og unge under 15 år ikke anses som værende i stand til at kunne give samtykke til dette (Enevoldsen, s.d.).

Straffelovens § 264 d: Omhandler videregivelse af private billeder vedrørende et andet individs private forhold eller billeder af den pågældende under omstændigheder, der åbenbart kan forlanges unddraget offentligheden.

I 2017 fremsatte Folketinget et forslag omkring udarbejdelse af en ny paragraf i Straffeloven i henhold til digitale krænkelser. I dette forslag argumenteres der bl.a. for, hvordan eksempelvis deling og efterspørgsel af krænkende materiale befinder sig i en såkaldt gråzone ift. lovgivningen. Digitale krænkelser har ikke sin egen bestemmelse i Straffeloven, men hører derimod under andre bestemmelser, jf. de tre ovenstående. I forlængelse heraf argumenteres

der yderligere for, at denne gråzone kan skabe forvirring og uklarhed omkring retstilstanden, hvilket både gør sig gældende for gerningspersoner og ofre. Folketingets mål er således, at digitale krænkelser fremadrettet skal kategoriseres som seksualforbrydelser med en ny selvstændig bestemmelse, så det sikrer tydeliggørelse af, at deling af intime billeder uden samtykke anses som værende en grov krænkelse af seksuel karakter på samme stadie som andre seksualforbrydelser (Folketinget, 2017, s. 2).

Ulovlig billeddeling kan indebære vidt forskellige motiver og måder at videredele intimt materiale på. Det er derfor muligt, at kriminalitetsformen kan placeres under flere af Walls kategorier som er uddybet i afsnit 2.1.1 omhandlende kriminalitetsformer. I indeværende speciale vurderes kategorierne Cyber-trespass og Cyber porn and obscenity dog som værende de mest relevante i henhold til besiddelse og deling af intimt materiale. Ud fra disse to forståelser har gerningspersonen opnået uberettiget adgang til det seksuelle materiale og efterfølgende spredt det online (Holt & Bossler, 2016, s. 11, 13). Det er dog ligeledes muligt, at gerningspersonen ikke selv har tilegnet sig materialet, f.eks. hvis vedkommende har fået det tilsendt uopfordret af en anden person. I dette tilfælde er der ikke nødvendigvis tale om Cyber-trespass, men derimod blot Cyber porn and obscenity, i så fald vedkommende vælger at beholde materialet og yderligere videredele det.

2.4 Problemformulering

Vi ønsker i indeværende speciale at belyse og kortlægge ovenstående kriminalitetsformer, uberettiget adgang og ulovlig billeddeling, ud fra en *Crime Script* forståelse. Denne tankegang bygger på ideen om, at kriminelle handlinger skal forstås som en flertrins dynamisk proces, der involverer en sammenhængende kæde af forskellige trin. Disse beslutninger baseres på en løbende evaluering af vedkommendes tilgængelige muligheder i den givne situation, hvilket gør, at handlingen kan gå flere veje. Dette betegnes også som *manuskripter*, som er forbundet med personlige og situationelle synsvinkler (Haelterman, 2016b, s. 7-10). Kriminalitet anskues derfor i indeværende speciale som en proces, der indebærer flere sekvenser i udførelsen heraf. Crime Script er således et gennemgående element i specialet, som danner grundlag for både problemformuleringen, forskningsdesignet i afsnit 4.1, analysestrategien i afsnit 4.11 samt analysen i afsnit 5.

På baggrund af Crime Script som forskningsdesign er fokusset i indeværende speciale således ikke på, *hvorfor* gerningspersoner vælger at opnå uberettiget adgang til andre personers elektroniske enheder og videredele dette materiale, og ej heller hvilke konsekvenser dette kan have for offeret. Interessen i indeværende speciale er derimod at belyse, *hvordan* disse kriminelle handlinger helt konkret udføres ud fra specifikke skridt og manuskripter.

Med afsæt i ovenstående problemfelt er følgende problemformulering blevet udarbejdet til at belyse specialets problemstilling:

Hvilke skridt indgår i anskaffelsen af uberettiget adgang til intimt materiale samt den ulovlige videredeling heraf?

Kapitel 3
Teori

3. Teori

I belysningen af hvordan der anskaffes uberettiget adgang til intimt materiale og ulovlig billeddeling heraf, inddrages to teorier i forklaringen af dette. Indledningsvist præsenteres Routine Activity Theory[2] af Cohen og Felson, der tydeliggør, hvilke elementer der skal være til stede for, at en kriminel handling kan fuldføres. Dernæst redegøres der for Social Learning Theory[3] af Akers, hvis fokus er på tillæring af kriminalitet.

3.1 Rutineaktivitetsteori

I 1970'erne påpegede Cohen og Felson et spændende paradoks: Selvom der i en lang årrække havde været en stabil velstandsstigning, faldt kriminaliteten ikke. Denne opdagelse udfordrede de dengang mest anerkendte sociologiske teorier omhandlende kriminalitet. Disse påpegede nemlig, at årsagerne til kriminalitet bundede i de statusfrustrationer, som ansås som en følgevirkning af, at specifikke borgere i et samfund havde dårlige muligheder for at være en del af den legitime samfundsøkonomi (Møller, 2013, s. 199). Cohen og Felson vendte dog dette perspektiv på hovedet: Frem for at tage udgangspunkt i den enkelte lovovertræders motivation til at begå kriminalitet, fokuserede de i stedet på de muligheder for at begå kriminalitet, som samfundets nye rutiner medførte (Møller, 2013, s. 199).

Cohen og Felson påpeger, at de strukturelle forandringer i samfundet er med til at fremme kriminalitet. Det kunne eksempelvis være den øgede digitalisering, som tidligere er omtalt i afsnit 2.1 omhandlende IT-kriminalitet. De nye strukturer medfører således også en række ændrede rutiner, som dermed yderligere skaber nye mønstre for adfærd (Cohen & Felson, 2013, s. 469-470). Denne rutineændring fordrer ligeledes, at kriminaliteten efterhånden stiger, da der enten opstår flere egnede mål, eller at der i større grad forekommer et fravær af kapable vogtere (Felson & Clarke, 1998, s. 4-5). Tre elementer skal ifølge Cohen og Felson konvergere i tid og rum for at en lovovertrædelse kan finde sted; en *motiveret gerningsperson,* et *egnet mål* og *fravær af kapable vogtere* (Felson & Clarke, 1998, s. 4). Fraværet af bare ét af disse elementer anses for at være tilstrækkelig til at forhindre kriminalitet (Cohen & Felson, 2013, s. 469-470; Felson & Clarke, 1998, s. 4) En vellykket og gennemført overtrædelse kræver således som minimum én motiveret gerningsperson med både kriminelle tilbøjeligheder samt evnen til at

[2] På dansk: Rutineaktivitetsteori
[3] På dansk: Social læringsteori

udføre disse, en person eller genstand som udgør et passende mål for gerningspersonen og fraværet af kapable vogtere, som er i stand til at forhindre den kriminelle handling (Cohen & Felson, 2013, s. 471). Kapable vogtere refererer derfor til tilstedeværelsen af ethvert individ eller objekt, som har kapaciteten til at afbryde den kriminelle aktivitet enten direkte eller indirekte (Felson & Clarke, 1998, s. 4).

Med udgangspunkt i den motiverede gerningsperson bygger Rutineaktivitetsteorien ligeledes på synet omkring, at gerningspersonen er et overvejende rationelt tænkende individ. Dette syn drager paralleller til *Rational choice*-tankegangen. Denne beror på, at individet er motiveret for at begå kriminalitet som udgangspunkt, men at individet gennem rationalitet vil opveje fordele samt ulemper ved at begå den pågældende kriminelle handling (Cornish & Clarke, 2013, s. 437; Felson & Clarke, 1998, s. 7). I modsætning til mange andre kriminologiske teorier er omdrejningspunktet i Rutineaktivitetsteorien således ikke at undersøge, *hvorfor* individer eller grupper er kriminelt tilbøjelige, men derimod at motiverede gerningspersoner er overvejende rationelle, hvorfor alle anses som værende motiverede for at begå kriminalitet (Cohen & Felson, 2013, s. 470). Den motiverede gerningsperson er derfor ifølge teorien en selvfølge. Fokusset i teorien er dermed i højere grad rettet imod de to andre elementer, egnede mål og kapable vogtere, som ofte er skiftende alt efter den pågældende situation (Felson & Clarke, 1998, s. 4).

Tidligere var TV'et et klassisk eksempel på et egnet mål. Dette skyldes store sociale ændringer, hvor bl.a. kvinderne deltog i aktiviteter væk fra hjemmet, heriblandt uddannelse og arbejde. Dette betød, at hjemmene var uden opsyn pga. manglende kapable vogtere (Cohen & Felson, 2013, s. 472, 475-476). Denne tidsperiode affødte bl.a. en revolution af små elektroniske apparater, som gjorde det lettere for motiverede gerningspersoner at stjæle disse (Cohen & Felson, 2013, s. 476; Felson & Clarke, 1998, s. 5). Den føromtalte teknologiske udvikling resulterede ydermere i, at motiverede gerningspersoner, egnede mål og kapable vogtere flyttede terræn, hvorfor de nu også udspiller sig online i form af IT-kriminalitet. Der eksisterer her et utal af motiverede gerningspersoner, som ønsker at få fat i eksempelvis personlige oplysninger- og materiale (Leukfeldt & Yar, 2016, s. 265). De som kan forhindre kriminalitet online, er eksempelvis vogtere i form af netværksadministratorer, forum moderatorer eller andre brugere, men det kan ligeså vel være mere automatiserede kapable vogtere såsom firewalls, ID-godkendelse samt adgangsstyringssystemer (Leukfeldt & Yar, 2016, s. 265).

3.2 Social læringsteori

Social læringsteori har eksisteret i mere end fire årtier og beskrives overordnet som en teori, der omhandler kriminalitet og afvigende adfærd (Akers & Jennings, 2019, s. 113). Akers' originale tekst om social læring blev i 1966 udgivet af ham selv og Robert Burgess, som en udvikling af Edwin H. Sutherlands' *Differential association theory.* Akers og Burgess har derfor videreudviklet Sutherlands' teori ud fra et psykologisk perspektiv og har således kaldt den nye teoretiske version for Social læringsteori (Akers & Jennings, 2019, s. 114). Akers forsøger med sin teori at forklare, hvordan kriminelle handlinger tillæres, hvorimod Sutherlands' teori udelukkende redegør for, hvorvidt disse handlinger er tillært eller ej (Akers, 2011[1994], s. 130; Akers & Jennings, 2019, s. 114). Sutherlands' teori postulerer således, at kriminel adfærd er lært i samspil med andre, men den anskueliggør dog ikke de mekanismer, hvormed sådan en adfærd er tillært. Sutherland har eksempelvis blot fokus på: *"A person becomes delinquent because of an excess of definitions favorable to violation of law over definitions unfavorable to violation of the law"* (Akers & Jennings, 2019, s. 114). Dog er grundtanken i både Akers' og Sutherlands' læringsteorier, at individer netop tillærer kriminel adfærd fra deres nære relationer, eksempelvis venner og familie (Akers, 2011[1994], s. 130). Sutherland og Akers mener derfor begge: "*That we learn to engage in crime through exposure to and the adoption of definitions favorable to crime"* (Akers, 2011[1994], s. 130).
Akers' sociale læringsteori er således ikke en erstatning af Sutherlands' teori. Den skal i stedet anses som en mere præcis udgave, der netop giver mulighed for at besvare de processer, der ikke er beskrevet i Sutherlands' teori (Akers, 2011[1994], s. 130; Akers & Jennings, 2019, s. 114-115).

I Akers Social læringsteori findes der fire centrale grundbegreber om, hvordan det enkelte individ netop tillærer kriminelle handlinger. Begrebet *Differential Association* beskriver, hvor det enkelte individ henter inspiration fra, eksempelvis familiemedlemmer, naboer, venner samt virtuelle fællesskaber. Det er derfor en proces, hvor det pågældende individ bliver udsat for definitioner, hvor netop afvigende adfærd kan betragtes som enten værende af positiv eller negativ karakter. Processen indebærer henholdsvis *adfærdsinteraktionelle-* samt *normative dimensioner*. Hvor de adfærdsinteraktionelle dimensioner består af den direkte interaktion med andre individer, som er involveret i en given adfærd, består de normative dimensioner i stedet af forskellige normer og værdier, som det pågældende individ eksponeres for gennem interaktionen. Akers argumenterer i forlængelse heraf for, at det er i de grupper, et individ

associciserer sig mest med, at individet tilegner sig normative definitioner, værdier samt favorable og ikke-favorable holdninger til en given adfærd. Det vil altså sige, at hvis vedkommende associerer sig mere med individer, som er involveret i en given kriminel og/eller afvigende adfærd, opstår der en større risiko for, at vedkommende indoptager denne adfærd (Akers, 2011[1994], s. 132; Akers & Jennings, 2019, s. 115).

Begrebet *Definitions* beskriver individets egen holdning til og forståelse af en adfærd. Det kunne eksempelvis være, hvorvidt vedkommende anser en bestemt handling som favorabel eller ej (Akers, 2011[1994], s. 132). I forlængelse heraf skelnes der mellem *generelle definitioner* og *specifikke definitioner*. De generelle definitioner dækker over individets traditionelle værdier og normer, der afspejles i en bred vifte af adfærd og situationer, hvor de specifikke definitioner i stedet er individets egne definitioner på handlinger. Akers argumenterer for, at der således kan skabes en kløft herimellem, hvis eksempelvis individet respekterer en gældende lov, men alligevel ikke overholder denne (Akers, 2011[1994], s. 132-133). Herunder præsenterer Akers og Jennings *positive definitions*, der evaluerer en given adfærd som værende positiv og som en legitim handling. *neutralizing definitions* beskriver derimod handlinger, der ikke anses af vedkommende selv som legale men i stedet acceptable eller berettiget i den givne situation. Akers hævder heraf, at når vedkommende opfatter afvigende adfærd som værende acceptabel, er det i højere grad neutraliserende definitioner, der er på spil, og ikke de positive definitioner (Akers & Jennings, 2019, s. 116). For at imødekomme denne kløft, kan individet gøre brug af *neutraliseringsteknikker*, som Gresham Sykes og David Matza redegør for i deres teoretiske perspektiv (Akers & Jennings, 2019, s. 116; Akers, 2011[1994], s. 132-133). Begrebet forklarer forskellige teknikker, som kriminelle gør brug af til at legitimere deres afvigende adfærd i en given situation (Sykes & Matza, 2013, s. 221).

Begrebet *Differential reinforcement* beskriver menneskets forventning om enten belønning eller straf til en specifik adfærd. Der kan således både forekomme *positive reinforcement*, et ønsket udbytte af den pågældende adfærd, samt *negative reinforcement*, en uønsket konsekvens eller straf som udbytte til den pågældende adfærd. Den konsekvens som handlingen har, påvirker således individets reaktion. Såfremt individet modtager belønning, vil dette styrke den pågældende adfærd, hvorimod straf vil have den modsatte effekt. Belønning og straf behøver dog ikke at indebære et socialt element. Det kan ligeledes være i form af en direkte fysisk effekt, eksempelvis i forbindelse med alkohol eller narkotika (Akers, 2011[1994], s. 133-134;

Akers & Jennings, 2019, s. 117). Derudover er det den adfærd, der anses for at have en forstærkende effekt, som individet vælger at deltage i, uanset om der er mulighed for en alternativ adfærd eller ej (Akers & Jennings, 2019, s. 117).

Det fjerde og sidste grundbegreb som Akers har opstillet, er begrebet *Imitation*, hvilket beskriver, når mennesket kopierer andres adfærd. Det enkelte individ kan således imitere adfærd, hvis det fremstår som værende favorabelt. Imitation er dog ikke udelukkende ud fra den specifikke handlings teknik og motiv men ligeledes erfaringen, der observeres, eksempelvis om den pågældende handling lykkes, og om det vurderes at have været det værd eller ej (Akers, 2011[1994], s. 134; Akers & Jennings, 2019, s. 118). Helt konkret forekommer imitation, når et individ indgår i en bestemt adfærd, som vedkommende enten direkte eller indirekte tidligere har observeret. Dog vil sandsynligheden for, at vedkommende efterligner den givne adfærd være betinget af andre faktorer, såsom den observeredes egenskaber, den faktiske adfærd samt de observerede konsekvenser af den pågældende adfærd. Tidligere har Akers dog postuleret, at selvom Imitation spiller en rolle i både fortsættelse og ophør af en given adfærd, er det mere sandsynligt, at imitationen vil have en effekt på ny adfærd. Hvis ikke individet har udført handlingen før, vil vedkommende således i højere grad imitere den fordelagtige adfærd (Akers & Jennings, 2019, s. 118).

Disse fire sociale læringsmekanismer argumenterer Akers for er en del af menneskets fundamentale læringshistorie (Akers, 2011[1994], s. 134). Læring anses som værende en kompleks proces, som kontinuerligt påvirkes af henholdsvis observation samt læring. På baggrund heraf opnår individet respons, hvilket Akers omtaler som *feedback momenter,* hvilket enten vil forstærke eller forskyde individets adfærd. Af denne årsag kan den givne adfærd løbende ændres alt afhængig af hvilken respons, der kommer heraf (Akers, 2011[1994], s. 134-135).

Akers har senere udvidet sin sociale læringsteori til at kunne anvendes på makroniveau. Denne teori betegnes *Social structure and social learning* (SSSL) og indebærer, udover læringskomponentet, et socio-komponent. Udvidelsen af læringsteorien er udviklet til på bedre vis at kunne begrunde gruppeforskelle, herunder forskelle mellem sociodemografiske grupper såsom klasse og køn, da det enkelte individ påvirkes gennem indflydelse af større sociale miljøer (Akers, 2011[1994], s. 135-136; Akers & Jennings, 2019, s. 118-119). Akers illustrerer i udvidelsesteorien fire dimensioner, *Differential Social Organization, Differential Location in*

the Social Structure, Theoretically Defined Structural Variables samt Differential Social Location, der anses som medvirkende til de generelle læringssammenhænge for det enkelte individ (Akers, 2011[1994], s. 135-136; Akers & Jennings, 2019, s. 119). Der er dog taget et valg i udarbejdelsen af indeværende speciale omkring, at SSSL ikke vil redegøres eller argumenteres yderligere for, da dette ikke synes relevant for indeværende speciale qua valget af forskningsdesign jf. afsnit 4.1.

3.3 Sammenkobling af teori

Afslutningsvist vurderes det, at de to præsenterede teorier, Rutineaktivitetsteori og Social læringsteori, kan komplimentere hinanden i indeværende speciale. En sammenfatning af de to teorier kan således indebære, at Akers teoretiske forståelse er med til at forklare, hvordan at motiverede gerningspersoner har lært, hvilke mål der er egnede, og hvordan de kapable vogtere bedst imødegås gennem eksempelvis bekendte eller online fællesskaber. Denne læring imødekommer således den motiverede gerningspersons ønske om bedst muligt at fuldføre en given kriminel handling. Dette er formentlig sket på baggrund af Feedback momenter eller Imitation, hvor der tidligere er observeret og efterlignet favorabel adfærd i udførelsen af enten uberettiget adgang eller ulovlig billeddeling. Disse observationer kan eksempelvis forekomme, når andre motiverede gerningspersoner forklarer om deres specifikke fremgangsmåde til at opnå uberettiget adgang til andres platforme.

Ligeledes muliggør inddragelsen af begge teorier en større forståelse af de mulige udfald ved at begå kriminalitet. Som tidligere argumenteret for indeholder Rutineaktivitetsteorien elementer fra Rational-choice tankegangen, hvorfor individet opvejer fordele og ulemper ved hver handling, vedkommende foretager sig. Denne tankegang kan drage paralleller til Akers begreb omhandlende Differential reinforcement. Dette argumenterer vi for, da den pågældende person kan observere andre kriminelles resultater. Såfremt individet ser, at udfaldet ved adfærden giver belønning, vil vedkommende selv i højere grad benytte sig ad samme adfærd. Dette argumenterer vi for, da den pågældende person kan observere andre kriminelles resultater. Såfremt der forekommer belønning, har vedkommende opvejet belønningen højere end konsekvenserne herved.

Dog vælger vi alligevel at argumentere for, at der forefindes en væsentlig nuanceforskel i de to teorier, der er værd at have for øje. Akers teori omhandlende social læring skal i højere grad anskues som værende intuitivt behavioristisk indlært, hvorfor indlæringen forekommer passiv. Passiviteten forekommer, da individet i samspil med andre indirekte påvirkes af deres handlinger. I rutineaktivitetsteorien beskrives individers handlinger i højere grad som værende aktive, da de netop kalkulerer mellem fordele og ulemper ved en given handling.

Rutineaktivitetsteorien har derfor hovedsageligt fokus på de miljømæssige muligheder for at en motiveret gerningsperson kan komme i kontakt med et egnet mål i manglen på kapable vogtere. Der er således ikke særlig meget fokus på det individuelle perspektiv. Det styrker derfor teorien, at der kobles læringsteori på, da denne kan forklare, hvordan den enkelte motiverede gerningsperson lærer kriminalitet. Social læringsteori kan ej heller stå alene, da vi således vil miste en forståelse af, hvilke omkringliggende omstændigheder der gør sig gældende i udførelsen af kriminalitetsformerne. Inddragelsen af begge teorier muliggør derfor en udførlig beskrivelse af, hvordan uberettiget adgang og ulovlig billeddeling udspiller sig.

Kapitel 4
Metode

4. Metode

I det følgende kapitel gennemgår vi specialets metode. Indledningsvist præsenteres specialets forskningsdesign- og tilgang. Herefter redegøres der for indsamlingen af empiri, herunder triangulering som inspirationskilde og individuelle ekspertinterviews, samt hvordan dette er udført. Slutteligt inddrages kvalitetskriterier og etiske overvejelser og følgelig en strategi for den senere analyse.

4.1 Crime Script som forskningsdesign

I en empirisk undersøgelse er det nødvendigt at udarbejde en strategi for, hvordan ens problemstilling bedst kan belyses og besvares. Dette betegnes som specialets forskningsdesign. Et forskningsdesign omhandler sammenhængen og logikken mellem specialets problemformulering samt måden hvorpå, denne kan besvares. Dette betyder også, at designet er afgørende for, hvilke konkrete metoder der skal anvendes (Andersen, Binderkrantz & Hansen, 2020, s. 69). For bedst at kunne besvare specialets problemformulering, er *Crime Script* valgt som forskningsdesign. På denne måde er det muligt at undersøge hele kriminalitetsprocessen, herunder de handlinger samt overvejelser der bliver foretaget før, under og efter, at forbrydelserne begås. Crime Script vurderes som et nyttigt værktøj til at undersøge kriminalitet, eftersom der inddrages forskellige elementer, der skal til for at fuldføre en given kriminel handling. Følgende afsnit består derfor af en redegørelse af Crime Script-tilgangen, samt hvordan denne anvendes i indeværende specialet.

Crime Script er oprindeligt adopteret fra den kognitive videnskab, men blev en del af kriminologien for to årtier siden med hjælp fra Derek Cornish (Haelterman, 2016a, s. vii). Ideen bag Crime Script-begrebet inden for kognitiv videnskab samt kunstig intelligens er, at handlinger lagres i menneskets hukommelse, hvorfor episoderne huskes som en standardiseret og generaliseret episode. Dette gør, at vedkommende næste gang undgår at bruge for meget tid og kræfter på at fortolke selvsamme situation, og hvordan denne situation skal gribes an igen (Haelterman, 2016b, s. 8). Disse manuskripter, som individet agerer efter, indlæres gennem social læring i form af modellering og forstærkning på baggrund af andre, der har lignende manuskripter (Haelterman, 2016b, s. 9). Individet indsamler og lagrer derfor kontinuerligt viden for at kunne udføre de handlinger, der kan opfylde det ønskede mål. Netop denne viden hjælper og vejleder vedkommende i fremtidige situationer.

Standardscript defineres som:

> *"Sequences of events that have occurred or that have been witnessed frequently and in a specific order are being captured in our memory as a standard script that can easily be recognized and recovered based on just some events that form part of its causal chain"* (Haelterman, 2016b, s. 9).

Disse Standardscripts er således både lette at genkende og gendanne. Når den givne adfærd, der er forbundet med et bestemt manuskript, er blevet brugt gentagne gange og har vist sig at være succesfuld, vil manuskriptet lettere blive aktiveret fremadrettet (Haelterman, 2016b, s. 9).

Med udgangspunkt i ovenstående forståelse, at enhver handling består af lagrede scripts, bliver Crime Script-tilgangen defineret i indeværende speciale som en systematisk måde, hvorpå der generes, identificeres og organiseres viden om den specifikke kriminalitetsform ud fra en trin-for-trin tilgang. Fokusset i specialet er således på rækkefølgen af de beslutninger, som gerningspersonen tager, og de ressourcer det kræves for at begå lovovertrædelsen (van der Bruggen & Blokland, 2021, s. 953). Crime Script anvendes derfor som en detaljeret analyse af, hvordan kriminalitetsformerne, i dette tilfælde uberettiget adgang og ulovlig billeddeling, udføres. Dette betyder også, at der ikke blot findes ét enkelt script i henhold til at begå en kriminel handling, men derimod en variation af scripts, alt afhængig af gerningsperson, mål og kriminalitetstype (Keatley, 2018, s. 128). Scripts består derfor også af organiseret viden omkring andre lignende situationer, hvorfor de nemt kan overlappe hinanden. Dette er med til at reducere unødvendig kompleksitet og giver individet mulighed for lettere at udføre de nødvendige rutiner for at opnå det opsatte mål. Derudover kan scripts være relativt specifikke men kan derimod også afdække mere abstrakte omstændigheder (Keatley, 2018, s. 128).

Igennem tiden er Crime Script blevet anvendt som enten et metodisk- eller et analytisk værktøj (van der Bruggen & Blokland, 2021, s. 953; Hutchings & Holt, 2015, s. 598; Lavorgna, 2014, s. 2). At der ikke er en klar afgrænsning af anvendelsen af Crime Script, anser vi som en fordel. Det giver os nemlig muligheden for at opnå en bredere forståelse af det undersøgte emne, når vi selv kan inkorporere det i henhold til vores specifikke undersøgelse. Med denne forståelse er det således muligt at inkorporere Crime Script som et grundlæggende design, der går igen i flere dele af indeværende speciale. Vi har i indeværende speciale ligeledes læst flere eksisterende studier, hvor Crime Script også er benyttet som tilgang til at forklare en given problemstilling. I disse studier står det klart, at Crime Script typisk anses som værende særligt

praktisk- samt ateoretisk orienteret. Dette ses eksempelvis i studierne *A Crime Script analysis of the online stolen data market* (Hutchings & Holt, 2015) *og A Crime Script Analysis of Child Sexual Exploitation Material Fora on the Darkweb* (van der Bruggen & Blokland, 2021). I specialets senere analyse er det således samme tilgang, vi vil benytte. Dette vil yderligere redegøres for i afsnit 4.11 omhandlende specialets analysestrategi.

For at udforme et Crime Script tager forskere ofte udgangspunkt i det universelle script, der er udarbejdet af Cornish. Dette involverer standardiserede script-scener, eller såkaldte funktioner, som er arrangeret i en specifik rækkefølge. Cornish opstiller i alt ni trin, der lyder som følgende: *Preparation, Entry, Precondition, Instrumental precondition, Instrumental initiation, Instrumental actualization, Doing, postcondition* og *Exit scenes* (Cornish, 1993, s. 40). Crime Scripts er desuden ikke præskriptive, da aktører ligeledes kan improvisere for at opnå det resultat, de ønsker, hvorfor at de ofte handler innovativt i relation til den pågældende forbrydelse (Hutchings & Holt, 2015, s. 598). Lisa Tompson og Spencer Chainey mente, at de ovenstående ni stadier med fordel kunne ændres, således at der blev anvendt et sprog, der var mere alment kendt, samt at hvert stadie kunne tilpasses til den specifikke kriminelle handling. De udarbejdede derfor fire stadier ud fra Cornishs typologi: *Preparation, Pre-activity, Activity* og *Post-activity* (Chainey & Berbotto, 2021, s. 5). De to første udgør forberedelsen af den kriminelle handling, nemlig Preparation, som er identificeringen af en mulig kriminel handling, og Pre-activity, som er de umiddelbare valg og handlinger, der foretages lige op til den kriminelle handling (van der Bruggen & Blokland, 2021, s. 957; Chainey & Tompson, 2011, s. 188-189; Chainey & Berbotto, 2021, s. 8). Dernæst udføres den kriminelle handling, hvilket betegnes som stadiet Activity. Det sidste stadie Post-activity er de logiske trin, der er nødvendige for at afslutte den kriminelle handling uden at blive opdaget (Keatley, 2018, s. 130; van der Bruggen & Blokland, 2021, s. 957; Chainey & Tompson, 2011, s. 189). For at gøre det gennemskueligt for læseren, har vi udarbejdet en overordnet figur med disse fire stadier. Denne omtales *Figur 1: De fire Crime Script stadier* og præsenteres nedenfor. I venstre kolonne fremgår de fire stadier, hvor højre kolonne består af en kort beskrivelse af det pågældende stadie.

Figur 1: De fire Crime Script stadier

Stadie	Beskrivelse
Preparation	Identifikationen af muligheden for at begå kriminalitet.
Pre-activity	Forberedelse, herunder de aktiviteter og adfærd der fører op til den kriminelle handling.
Activity	Udførelsen af den kriminelle handling.
Post-activity	De nødvendige trin for at kunne afslutte den kriminelle handling og undgå at blive opdaget.

(Keatley, 2018, s. 130).

De fire præsenterede stadier er de, som indeværende speciale vil tage udgangspunkt i. De vil derfor fremgå som gennemgående temaer i specialets interviewguide (afsnit 4.7.1), kodningsstrategi (afsnit 4.8.2), analysestrategi (afsnit 4.11) og analyse (afsnit 5).

For at kunne benytte sig af Crime Script kræver det som forsker en dyb og detaljeret forståelse for de faktorer, der gør sig gældende for netop at begå den givne kriminelle handling. Vi har derfor i indeværende speciale foretaget en litteratursøgning, jf. kapitel 1, samt en grundig beskrivelse af uberettiget adgang og ulovlig billeddeling i afsnit 2.2 samt 2.3. Ydermere består den primære empiriindsamling af interviews med eksperter på området, hvilket der argumenteres yderligere for i afsnit 4.5.1. Ud fra det ovenstående, omhandlende Crime Script, har indeværende speciale således til hensigt at undersøge, hvordan en gerningsperson trin for trin planlægger, organiserer og opnår uberettiget adgang til intimt materiale hos det pågældende offer. Ud fra disse scripts kan der ligeledes tillægges et præventivt blik, da viden om de enkelte sekvenser til en vis grad kan forudsige trinnene i andre lignende situationer (Keatley, 2018, s. 133).

4.2 Forskningstilgang

Udover at reflektere over forskningsdesign er det ligeledes relevant at undersøge, hvordan vores forskningsprojekt tilrettelægges, herunder hvordan empirien og teorien anskues og gribes an. Følgende afsnit består således af en forklaring af processen omkring, hvordan indeværende speciale tilgås.

I forskning skelnes der typisk mellem tre forskningstilgange. Den *induktive* tilgang gør sig gældende, når den empiriske analyse tilgås med en åben tilgang, og hvor det således er empirien, der danner de pågældende mønstre og sammenhænge (Andersen et al., 2020, s. 78). Modsat kan der arbejdes ud fra den *deduktive* tilgang, hvor der tages udgangspunkt i teorier, hvortil der udvikles hypoteser, som afprøves på data (Boolsen, 2020, s. 310). Mellem disse to tilgange findes den *abduktive* tilgang, hvor henholdsvis empiri og teori vekselvirker med hinanden. Tilgangen har således den fordel, at den tillader at anskue problemstillingen fra et åbent perspektiv. Ydermere antages det, at vi alle lægger inde med en vis mængde af viden, videnskabelig eller ej, om det pågældende emne, vi ønsker at undersøge. Gennem denne allerede eksisterende viden, er målet således at vekselvirke mellem empiri og teori i en kreativ proces, hvor der søges den bedste forklaring ud fra det undersøgte (Birkler, 2021, s. 93). I indeværende speciale arbejder vi derfor ud fra den abduktive tilgang. Dette valg beror på, at problemformuleringen netop er struktureret på baggrund af Crime Script-tilgangen og ikke på forhånd indeholder en beskrivelse af, hvilke skridt der indgår i kriminalitetsformerne. Vi anerkender hertil, på baggrund af en Crime Script-forståelse, at der indgår konkrete skridt i kriminelle handlinger. Dette perspektiv har derfor tråde til den deduktive tilgang, da vi på forhånd antager, at kriminalitet følger et specifikt manuskript. Hvilke skridt der derimod indgår i de to kriminalitetsformer, uberettiget adgang og ulovlig billeddeling, er dog ikke givet på forhånd. Dette undersøges derfor relativt induktivt, gennem sekundær litteratur, som præsenteres i afsnit 4.3.1, og specialets primære empiri, der fremgår i afsnit 4.5.1. Abduktion kommer yderligere i spil, når der benyttes teoretiske begreber fra specialets teorier jf. kapitel 3, som benyttes til en dybere forklaring af empirien. Der opstår således denne vekselvirkning mellem empiri og teori løbende i den senere analyse, som den abduktive tilgang fordrer (Birkler, 2021, s. 93-94).

En vigtig pointe ift. den abduktive tilgang er, at der ikke sluttes til en endelig konklusion. Dette betyder, at der altid er plads til en endnu bedre forklaring (Birkler, 2021, s. 94). Dette stemmer således godt overens med indeværende speciales fokus på IT-kriminalitet, da vi i kapitel 2, jf. specialets problemfelt, ligeledes argumenterer for, at denne form for kriminalitet konstant er i udvikling. Den åbne konklusion inviterer således til, at senere forskning på området kan nå frem til resultater, der anses som endnu mere relevant, netop på baggrund af den konstante udvikling.

4.3 Triangulering

Triangulering indebærer anvendelsen af flere metoder i en undersøgelse, typisk med formålet om at forbedre gyldigheden og støtte den pågældende undersøgelses empiri. Dog er det en praksis, der gennem tiden er blevet anvendt på forskellig vis (Rahman, 2012, s. 157). Følgende afsnit vil derfor klarlægge, hvordan og hvorfor indeværende speciale anvender triangulering som inspiration i besvarelsen af problemformuleringen.

Norman Denzin har opstillet fire former for triangulering. Den første er *Data triangulation*, hvilket indebærer indhentning af data fra flere forskellige datakilder og sammenfatte det til et enkelt datasæt. Dernæst kan typen *Investigator triangulation* anvendes, hvis der er flere observatører, i stedet for en enkelt i indsamlingen af empiri. *Theoretical triangulation* henviser til anvendelsen af mere end én teoretisk position i undersøgelsen af et fænomen. Sidst præsenteres *Methodological triangulation*, der omhandler brugen af mere end én undersøgelsesmetode. Denzin noterede hertil, at methodological triangulation kan være *Within-method* eller *Between or across-method triangulation* (Fusch, Fusch & Ness, 2018, s. 22). Hvis der inddrages mere end én kvalitativ dataindsamlingsmetode under metodetriangulering, såsom interviews og etnografi, er der således tale om within-method triangulation. Hvis der derimod anvendes både kvalitativ og kvantitativ metode, er det typen between or across-method triangulation, der er i brug (Natow, 2019, s. 161-162). Uanset hvilken fremgangsmåde der anvendes, er methodological triangulation den mest almindelige anvendelse af triangulering (Rahman, 2012, s. 157). Det er dog muligt at benytte flere former for triangulering i den samme undersøgelse. Dette afhænger dog i høj grad af, hvilket formål undersøgelsen har (Rahman, 2012, s. 157).

Vi anskuer de fire præsenterede former for triangulering som idealtypiske fænomener, som kan tilpasses efter den pågældende undersøgelse. Vi er derfor blot inspireret af triangulering i indeværende speciale. Vi anvender hovedsageligt elementer fra data- og methodological triangulation ift. specialets analyseafsnit, da vi benytter baggrundsviden fra sekundær litteratur, som en form for datasæt, der understøtter vores primære empiri. Vi sammensætter derfor ikke flere datakilder til et enkelt men anvender derimod flere sekundære kilder som en måde at undersøge det samme fænomen ud fra forskellige perspektiver. Med inspiration fra methodological triangulation trækkes der udelukkende på kvalitativt data, dvs. akademiske tekster og ekspertinterviews. Ved at trække på inspiration fra triangulering kan vi understøtte vores analyse gennem empiriske studier af de pågældende fænomener. Indeværende speciale arbejder derfor ud fra en within-method triangulation, da der inddrages både ekspertinterviews (afsnit 4.5.1) som primær empiri og eksisterende litteratur som sekundær kilde (afsnit 4.3.1) i specialets analyse (kapitel 5).

Tidligere forskning har endvidere pointeret, at ekspertinterviews kan være begrænset af at eksperterne vildleder, undviger eller udtaler sig om omstændigheder, der gavner dem selv (Natow, 2019, s. 161). Triangulering med forskellige former for empiri kan derfor løse disse problemer ved at bekræfte fundene samt inkorporere yderligere information til, hvad en enkelt ekspert omtaler (Natow, 2019, s. 161). Yderligere kan data- og methodological triangulation give forskeren en række vigtige muligheder, såsom at føle sig mere sikker på den pågældende undersøgelse samt at skabe nye måder at indfange et socialt problem på (Rahman, 2012, s. 159). Hvordan triangulering som inspirationskilde influerer specialets kvalitet uddybes yderligere i afsnit 4.9 omhandlende kvalitetssikring.

4.3.1 Sekundær litteratur

Følgende afsnit indebærer en beskrivelse af det materiale, der udgør specialets sekundære litteratur. For at kunne identificere, hvilken litteratur der var relevant i understøttelsen af specialets analyse i afsnit 5, tog vi udgangspunkt i samme fremgangsmåde som hos litteratursøgningen i kapitel 1.

Den sekundære litteratur består af i alt 30 dokumenter, som benyttes til at underbygge vigtige pointer i specialets analyse jf. afsnit 5. Vi har valgt at opsætte et kriterie omkring, at specialets sekundære empiri som udgangspunkt skal bestå af peer-reviewed artikler, journaler eller bogkapitler. Dette er valgt, da disse peer-reviewed tekster er godkendt ift. specifikke standarder

i diverse akademiske journaler (Natow, 2019, s. 163). Et par sekundære kilder fremstår dog ikke umiddelbart som peer-reviewed, men vi har alligevel valgt, ud fra en kritisk bedømmelse af hver deres udgiver, at de alligevel kan anskues som godkendte akademiske tekster.

Vi har udarbejdet en oversigt med de akademiske tekster, der anvendes som sekundær litteratur. Denne kan tilgås i Bilag 10. Første kolonne præsenterer titel og forfatter på det pågældende materiale. I anden kolonne forekommer årstal og land for publiceringen af materialet. Tredje kolonne referer således til, hvilken type af tekst det pågældende sekundære materiale er. Sidst i fjerde kolonne er der noteret en kort beskrivelse af, hvad teksten har fokus på. Derudover består de fleste sekundære kilder udgivet i andre lande (heriblandt USA og England). Det er valgt at anvende disse udenlandske kilder, da en granskning af litteraturen umiddelbart viste, at dansk litteratur ikke fyldestgørende har kunnet afdække relevante udsagn. Dette ser vi dog ikke som en ulempe, da vi netop kun benytter litteratur fra udlandet, som i udgangspunkt er peer-reviewed og dermed godkendte ift. specifikke standarder.

Den sekundære litteratur kan både understøtte pointerne i den primære empiri men formår også at uddybe de områder, hvor den primære empiri ikke afdækker. På denne måde opnås et grundigere helhedsbillede af, hvordan uberettiget adgang og ulovlig billeddeling opnås og udføres.

4.4 Kvalitativ metode

Kvalitative forskningsmetoder beskrives som værende mangeartede og har indvirkning på de forskellige forskningstraditioner, herunder samfundsvidenskaben. Overordnet set er omdrejningspunktet i kvalitativ forskning at gå i dybden med, hvordan mennesker tilskriver handlinger en mening, og hvordan noget gøres, opleves, siges og forbedres. Interessen foreligger derfor i nuancerne og detaljerne for at kunne forstå, beskrive og fortolke de menneskelige erfaringer (Brinkmann & Tanggaard, 2020, s. 15). En betydelig styrke ved kvalitativ forskning er, at der kan opnås dybdegående viden omkring specifikke begivenheder og situationer på et givent tidspunkt (Bryman, 2016, s. 494). Kvalitativ forskning står derfor også i direkte modsætning til kvantitativ forskning, der i stedet har fokus på at bearbejde data statistisk ud fra talværdier (Brinkmann & Tanggaard, 2020, s. 16). På baggrund af dette vurderes den kvalitative undersøgelsesmetode som fortrinlig i beskrivelsen af specialets emne. Dette skyldes, at vi i indeværende speciale er interesseret i netop en dybdegående viden og

forståelse omkring, hvilke skridt der indgår i udførelsen af uberettiget adgang samt ulovlig billeddeling qua vores problemformulering.

4.5 Interview som undersøgelsesmetode

Det er væsentligt at reflektere over, hvordan der ønskes indsamling af empiri. Formålet er at opnå en detaljeret og dybdegående viden omkring selve udførelsen af uberettiget adgang og ulovlig billeddeling, hvorfor den kvalitative undersøgelsesmetode i indeværende speciale således består af interviews.

Interviews kan anvendes i vidt forskellige kontekster. Overordnet set defineres interviews som *"[...] det at gennemføre en samtale med et bestemt formål*" (Harrits, Pedersen, Halkier & Møller, 2020, s. 180). Lene Tanggaard og Svend Brinkmann mener, at den grundlæggende idé bag interviews er, at forskeren formår at opnå indsigt i informanternes viden om bestemte fænomener. Gennem interviewmetoden er det muligt at koncentrere sig om, hvordan udvalgte informanter forstår bestemte situationer eller fænomener, som de stifter bekendtskab med i deres eget liv (Tanggaard & Brinkmann, 2020a, s. 35-36). Yderligere er det semistrukturerede interview valgt med henblik på at kunne stille uddybende spørgsmål til det sagte og dermed komme dybere ned i konteksten (Tanggaard & Brinkmann, 2020a, s. 42-43). Den semistrukturerede interviewform anses derfor som værende fordelagtig, da det giver intervieweren mulighed for at forfølge spontane beretninger i relation til specialets omdrejningspunkt uden at være fastlåst af en interviewguide.

4.5.1 Ekspertinterviews

Der findes flere forskellige interviewformer, der kan vælges, alt afhængig af undersøgelsens formål (Kvale & Brinkmann, 2015a, s. 197). I dette speciale anvendes ekspertinterviews, da vi på denne måde opnår adgang til empiri, der er baseret på faktuel viden omkring de kriminelle handlinger.

I ekspertinterviews anses informanterne som eksperter inden for et givent område (Kvale & Brinkmann, 2015a, s. 201). Det er således en målgruppe, der har en særlig professionel position, hvor formålet er at indsamle information omkring et specifikt genstandsfelt (Harrits et al., 2020, s. 187). I denne undersøgelse består eksperterne af individer, der til dagligt beskæftiger sig med IT-kriminalitet, eller som har relevant viden inden for feltet.

Dette indebærer en politikommissær, en analytiker, en specialanklager samt to forskere på området. Interviewene omhandler derfor ikke eksperternes eget liv men derimod deres faglige viden og erfaring, som de hver især har i relation til specialets problemstilling.

For at kunne foretage et ekspertinterview kræver det bl.a., at intervieweren har opnået en bred forståelse for specialets emne, således at der kan forberedes relevante spørgsmål, der kan åbne op for den ekspertise og viden, eksperterne har (Kvale & Brinkmann, 2015a, s. 201). Derudover er det vigtigt at være fortrolig med de udvalgte eksperters sociale status, for på denne måde at imødekomme den gensidige respekt interviewer og ekspert imellem (Kvale & Brinkmann, 2015a, s. 201). En primær problematik, der ofte forekommer ved denne form for interview, er netop den asymmetriske magtbalance mellem ekspert og interviewer. Denne problematik var der stort fokus på at imødekomme i indeværende speciale, hvorfor der er sket en granskning af tidligere datamateriale og undersøgelser, inden afholdelsen af interviewene.

Udover en grundig litteratursøgningsproces er eksperternes arbejde ligeledes undersøgt, herunder deres faglige kompetencer, udtalelser til medierne mm. Disse litteratur- og baggrundssøgninger er foretaget med henblik på at stifte bekendtskab med hver enkelt ekspert for at kunne stille ikke-planlagte spørgsmål under interviewet, i så fald at det var relevant med konkretisering af deres faglighed. Ved at benytte en bred vifte af eksperter på området, opnås der flere perspektiver på selvsamme felt, hvilket giver et større grundlag for analysen. Det anses således som værende særligt strategisk netop at benytte sig af en variation af forskellige professionelle positioner, da der på denne måde opnås et bredt grundlag for den senere analyse (Staunæs & Søndergaard, 2005, s. 55). Et eksempel på hvor det kommer til udtryk, at eksperternes faglige viden hovedsageligt var bundet til deres jobmæssige position, er Lene Wacher Lentz, der eksempelvis henviser til NC3 under et spørgsmål: "*[...] hvordan det plejer at være, det er nok NC3, der kan hjælpe lidt mere med det"* (Bilag 9, l. 533-534). Dette eksempel visualiserer således, hvordan den brede vifte af eksperter fordrer, at vi i interviewene opnår en mere facetteret forståelse for vores spørgsmål, samtidig med eksperternes viden kan supplere hinanden.

4.6 Udvælgelse og rekruttering af informanter

Valget af ekspertinterviews som metode fordrer ligeledes en del overvejelser inden gennemførelsen heraf. Én af disse overvejelser er bl.a. valget af antal informanter, der ønskes benyttet. Steinar Kvale og Svend Brinkmann argumenterer for, at antallet af informanter afhænger af den specifikke undersøgelse. Det er således vigtigt at have øje for, hvor meget tid der er til rådighed, samt hvad undersøgelsen opnår ved én eller flere interviews. De postulerer således, at der skal udføres den mængde af interviews, der er nødvendig for at kunne fremskaffe nok viden om undersøgelsens emne (Kvale & Brinkmann, 2015b, s. 166-167). Udvælgelsen af indeværende speciales eksperter skete derfor ud fra den *Formålsbestemte strategi*. Dette begreb dækker over, at eksperterne blev nøje udvalgt ud fra specialets formål, og dermed ikke ud fra et *tilfældighedsprincip*. Eksperterne blev udvalgt ud fra netop deres relevante viden, da dette muliggør et større indblik i det undersøgte emne (Harrits et al., 2020, s. 199). Ligeledes hjalp vores kontaktperson Michael Karpf hos NC3 med at spore os ind på, hvilke relevante eksperter, der med fordel kunne benyttes i indeværende speciale, hvortil han i flere tilfælde også agerede gatekeeper (Karpatschof, 2020, s. 572-573).

Første kontakt til mulige eksperter blev således etableret via e-mail eller en besked på LinkedIn i perioden 14. marts til 15. marts 2022. Løbende som vi modtog svar på, hvorvidt den enkelte ekspert ønskede at deltage i et interview eller ej, sendte vi flere forespørgsler ud til nye eksperter. Vi oplevede også, at eksperter ikke gav svar fra sig, hvorfor vi efter en uges varsel sendte en opfølgende mail eller foretog et opfølgende opkald. Dette gjorde således, vi opnåede større respons, hvor vi ofte blev mødt med, at vores mail var forsvundet i mængden af andre mails i eksperternes indbakker. Det har dermed vist sig at være særligt problematisk at etablere kontakt til relevante eksperter, som havde lyst til og mulighed for at deltage i indeværende speciale. Dette viste sig yderligere, da vi bl.a. blev mødt med svar omkring, at flere eksperter ikke havde tiden til at deltage, eller fordi de er implicerede i verserende sager om digitale krænkelser, hvori der ikke er faldet dom endnu, hvorfor eksperterne ikke måtte udtale sig af habilitetsmæssige årsager. Derudover oplevede vi én informant springe fra, efter vi havde indgået en aftale, da vedkommende alligevel ikke syntes, at hun var den rette ekspert at benytte. Vi endte derfor med at have kontaktet i alt 19 eksperter, hvoraf 9 personer takkede nej, fem ikke svarede og fem sagde ja tak til at deltage. Empirien består derfor af i alt fem ekspertinterviews.

Foruden tidligere nævnte værktøjer til at opnå kendskab til relevante eksperter, har vi ligeledes gjort brug af Snowball-effekten (Thagaard, 2004, s. 55-56). Dette gjorde sig gældende, da vi adspurgte eksperterne, både de der takkede ja og nej, om de kendte til andre interessante eksperter, vi med fordel kunne kontakte. Et eksempel herpå er politikommissær Flemming Kjærside, som gjorde os opmærksom på under interviewet, at Sidsel Harder netop havde forsvaret sin ph.d.-afhandling hos NC3, med titlen *Images with Nudity and Consequences*, hvorfor vi efterfølgende tog kontakt til hende omkring deltagelsen i vores speciale.

På baggrund af den omfattende rekruttering af relevante eksperter, vurderer vi alligevel at opnåelsen af netop fem ekspertinterviews er fortrinlig. Tanggaard og Brinkmann argumenterer nemlig for, at det anses som værende mere fordelagtigt at gennemføre forholdsvis få interviews og dermed kunne gennemarbejde disse, da dette afføder muligheden for at gøre analysen grundig og teoretisk alsidig. Risikoen ved at gennemføre for mange interviews er nemlig, at forskeren kan miste overblikket over empirien (Tanggaard & Brinkmann, 2020a, s. 36-37). Derudover har flere af vores eksperter en bred berøring med sager omhandlende uberettiget adgang og ulovlig billeddeling i deres dagligdag. Eksempelvis udtalte Flemming Kjærside i interviewet, at samtlige anmeldelser omhandlende digitale sexkrænkelser på politi.dk ender hos ham og hans afdeling (Bilag 5, l. 78-87). Vi argumenterer derfor, at vi på baggrund af fem ekspertinterviews formår fyldestgørende at kunne indhente empiri, som kan bidrage til besvarelsen af problemformuleringen.

Derudover efterspurgte tre af eksperterne under rekrutteringen, om de måtte få adgang til specialets interviewguide på forhånd. Dette blev imødekommet, da vi anså det som værende en fordel, da eksperterne på denne måde kunne forberede deres svar på bedste vis. Det vil unægteligt styrke det kommende analysearbejde, hvis de på baggrund af dette vil kunne give udførlige faglige svar under interviewene. Forberedelse kan dog også have den begrænsning, at de kan have forberedt svar, der fremmer de synspunkter, de ønsker videreformidlet (Kvale & Brinkmann, 2015a, s. 202). Dette kunne eksempelvis være, hvis eksperterne har en skjult agenda at tale ud fra, for ikke at kritisere deres egen position, og de derfor får lov at forberede sig herpå. Dette var dog ikke noget, vi i de tre ekspertinterviews lagde mærke til.

Inden påbegyndelsen af interviewene skulle vi desuden sikre os, jf. GDPR, at vores behandling af personoplysningerne havde et lovligt behandlingsgrundlag. Dette har vi sikret ved at sende en samtykkeerklæring til alle eksperter (Bilag 3). Dette samtykke skulle således gives inden

indsamlingen, behandlingen og opbevaringen af personoplysningerne. I samtykkeerklæringen lagde vi vægt på, at det var tilpasset indeværende speciales formål, og at samtykket gives frivilligt. Vi har yderligere understreget, at der ikke vil foreligge nogle ulemper for vores eksperter ved at afvise samtykket. Vi har derfor informeret hver ekspert om, hvilke rettigheder vedkommende har ift. at deltage i indeværende speciale (Aalborg Universitet, s.d.). Vi modtog skriftligt samtykke fra alle fem eksperter inden interviewet.

Nedenfor fremgår en oversigt over de eksperter der indgik i et ekspertinterview i indeværende speciale. Venstre kolonne består af ekspertens navn, hvor anden kolonne er en beskrivelse af deres jobposition, herunder deres arbejdsopgaver og fokusområde.

Figur 2: Oversigt over specialets eksperter

Navn	Jobposition
Flemming Kjærside	Politikommissær fra NSK (NC3) i sektionen for IT-relaterede seksualforbrydelser. Afdelingen hvor Flemming er politikommissær, har bl.a. som kerneopgave at undersøge computere, der er blevet beslaglagt i digitale krænkelsessager. Derudover har sektionen et tæt samarbejde med både EUROPOL samt INTERPOL. Alle former for anmeldelser omkring digitale sexkrænkelser kommer ind til denne afdeling, hvis der anmeldes via politi.dk. Her står de for visiteringen af anmeldelserne at navigere sagerne ud til de respektive politikredse samt at tage kontakt til de pågældende platforme, hvor de kriminelle handlinger finder sted.
Morten Rasmussen	Anklager i mere end 20 år. Har stillingen *National ekspert* i bekæmpelse af cybercrime som indebærer, at han er specialist og specialanklager i cybercrime. Mortens primære fokus er organiseret kriminalitet herunder narkotika og bandekriminalitet. Dog underviser han andre anklagere i cybercrime - herunder også i ulovlig billeddeling.

Christoffer Herlufsen	Arbejder ligeledes i NC3. Christoffer befinder sig i enheden "Hightech crime" som analytiker. Han laver efterforskning samt statistisk analyse på alt det, afdelingen modtager omhandlende traditionel cybercrime (herunder hackingangreb og angreb på virksomheder samt borgere).
Sidsel Kirstine Harder	Sidsel har netop opnået titlen Ph.D. i Sociologi og er nu forsker på Ghent Universitet, juridisk-kriminologisk fakultet. Ph.D. afhandlingen tager udgangspunkt i seks forskellige tekster, hvori der forklares om den digitale udvikling af intime billeder og betydningen af disse i unges hverdagsliv.
Lene Wacher Lentz	Er jurist, underviser på Aalborg Universitet og forsker i cybercrime - herunder rammerne for politiets efterforskning af cybercrime. Særligt er hendes fokus på, hvordan loven stemmer overens med virkeligheden, hvordan lovene passer indbyrdes og på tværs af grænser. Ydermere har Lene tidligere arbejdet som anklager, hvor hun har haft konkrete sager inden for cybercrime.

4.7 Spørgeramme og procedure

I eksisterende litteratur findes der ikke konsensus omkring, hvorvidt forskere opnår et indsnævret syn ved på forhånd at have læst meget om det pågældende emne (Tanggaard & Brinkmann, 2020a, s. 43). Dette argumenterer Tanggaard og Brinkmann dog for er en forfejlet antagelse, da de mener, at ingen forskningsinterviews agerer neutrale, da disse interviews altid vil være bestemt af den pågældende forskers agenda, som bør være teoretisk begrundet (Tanggaard & Brinkmann, 2020a, s. 43). I forlængelse heraf mener Tanggaard og Brinkmann ydermere, at dette grundige forarbejde anses som værende fordelagtigt, da netop dette gør det muligt at kunne målrette interviewspørgsmålene på bedst mulig vis. Derudover viser erfaring ligeledes, at netop de bedste interviews udarbejdes af dem, der har opnået en stor forhåndsviden om det pågældende emne, da de derfor kan formulere de mest fordelagtige spørgsmål

(Tanggaard & Brinkmann, 2020a, s. 43). Tilsvarende i indeværende speciale jf. kapitel 1, omhandlende litteratursøgningsprocessen, startede vi med en dybdegående granskning af tidligere og relevant forskning inden for IT-kriminalitet generelt, samt uberettiget adgang og ulovlig billeddeling. Denne litteratursøgningsproces blev derfor ydermere en væsentlig del af udførelsen af specialets interviewguide.

4.7.1 Interviewguide

Et interview udføres ofte ud fra en form for *guideline*. Dette kan eksempelvis være en interviewguide, der strukturerer forløbet i interviewet. Indholdet i en interviewguide kan være udformet med specifikke spørgsmål eller blot være nogle temaer, der ønskes afdækket (Kvale & Brinkmann, 2015c, s. 185). I indeværende speciale består interviewguiden af opdelte spørgsmål under relevante temaer. Interviewguiden blev som bekendt ydermere udarbejdet ud fra en Crime Script-tankegang, hvorfor interviewguiden blev opdelt efter kategorierne Preparation, Pre-activity, Activity, og Post-activity. Dette kommer bl.a. til udtryk ift. den tidsmæssige rækkefølge; før, under og efter. Dette valg blev taget, da det muliggjorde udarbejdelsen af den senere analyse og desuden dannede et naturligt flow af selve hændelsesforløbene i de respektive kriminalitetsformer under interviewet. Derudover bidrog specialets teorier som inspiration til udvalgte interviewspørgsmål. Dette forekom eksempelvis i relation til læringsperspektivet under spørgsmålet: *"Hvordan opnår gerningspersonen viden omkring at kunne opnå uberettiget adgang?"* (Bilag 4).

Som argumenteret for i afsnit 4.5, omhandlende interview som undersøgelsesmetode, blev indeværende speciales spørgeramme udarbejdet ud fra den semistrukturerede interviewform for på bedst mulig vis at opnå adgang til eksperternes viden (Tanggaard & Brinkmann, 2020a, s. 42-44). Afhængig af hvad eksperten fortalte, blev der således sprunget rundt i rækkefølgen af de etablerede spørgsmål. Foruden interviewspørgsmålene var der ligeledes udarbejdet forskningsspørgsmål til hvert tema. Dette blev gjort, da forskningsspørgsmål ikke just fungerer som gode interviewspørgsmål. Derudover er målet med forskningsspørgsmål sædvanligvis at søge forklaringer på specifikke fænomener, processer og/ eller sammenhænge, hvorimod interviewspørgsmål i stedet søger bestemte beskrivelser af disse (Tanggaard & Brinkmann, 2020a, s. 48). Et eksempel på et forskningsspørgsmål i indeværende interviewguide er: *"Hvilke overvejelser ligger forud for opnåelsen af uberettiget adgang?"* (Bilag 4).

Der findes flere forskellige typer af interviewspørgsmål, som kan anvendes i et interview, alt afhængig af den information der søges (Harrits et al., 2020, s. 192). I indeværende speciales interviewguide er der blevet anvendt flere typer af spørgsmål. Dog bliver der i det følgende præsenteret de væsentligste. Grundlæggende set består de fleste interviewspørgsmål af typen *Informationssøgende spørgsmål* (Harrits et al., 2020, s. 193). Årsagen til dette er, at hele interviewet er opsat efter et ønske om adgang til eksperternes fagkyndige viden. Spørgsmål relateret hertil er eksempelvis: *"Kan du give to eksempler på, hvilke udfordringer online kriminalitet kan have i forhold til offline kriminalitet?"* (Bilag 4) i relation til deres jobmæssige position. Yderligere præges interviewguiden i høj grad af *Strukturerende spørgsmål* for at strukturere samtalen (Harrits et al., 2020, s. 194). Dette udfolder sig på baggrund af Crime Script-tilgangen, med fokus på før, under og efter handlingen i form af: *"De næste par spørgsmål relaterer sig til det der sker efter, der er opnået uberettiget adgang"* (Bilag 4). Afslutningsvist er det væsentlig at fremføre at alle interviewspørgsmål var, uanset type, udfærdiget i et letfatteligt sprog for på bedst mulig vis at kunne skabe et positivt samspil interviewer og ekspert imellem (Kvale & Brinkmann, 2015c, s. 186; Tanggaard & Brinkmann, 2020a, s. 48-49).

4.7.2 Interviewsituation

De fem ekspertinterviews blev udført i perioden d. 24. marts til d. 1. april 2022 og blev alle afviklet over kommunikationsplatformen Microsoft Teams. Der er derfor tale om *synkron online-interviews*, en dataindsamlingsmetode som efterhånden har vundet indpas blandt forskere (Deakin & Wakefield, 2013, s. 604). En stor fordel ved interviews der foregår online, er den fleksible og innovative måde, der kan indsamles data på (Żadkowska, Dowgiałło, Gajewska, Herzberg-Kurasz & Kostecka, 2022, s. 2; Deakin & Wakefield, 2013, s. 605). Der kræves eksempelvis ikke en specifik geografisk placering for udførelsen af interviewet, hvorfor det har været muligt at opnå interviews med eksperter fra forskellige steder i Danmark og uden for landets grænser. Eksempelvis befandt ekspert Sidsel Harder sig i Belgien under det respektive interview (Bilag 8, l. 644). Et væsentligt kritikpunkt, der dog ofte relaterer sig til denne form for indsamlingsmetode, er den manglende fysiske tilstedeværelse af interviewperson, da non-verbale signaler ofte er med til at kontekstualisere situationen (Deakin & Wakefield, 2013, s. 605). Dette har vi dog forsøgt at imødekomme i form af webcam, således at det var muligt at se den pågældende eksperts mimik mm., for derved lettere at forstå det

sagte. Online interviews kan derfor anses som et velset supplement eller erstatning for ansigt-til-ansigt interviews (Deakin & Wakefield, 2013, s. 603).

Under interviewene var der to interviewere til stede. Når den ene interviewer agererede frontinterviewer, agererede den anden således som observatør. Det var frontintervieweren, der stod for at styre det pågældende interview ved at stille de udarbejdede spørgsmål, hvor observatøren havde til formål at sikre, at interviewguiden blev fulgt, og at specialets forskningsspørgsmål blev afdækket. På baggrund af denne opdeling muliggør det, at intervieweren bedre kan sørge for at producere ny viden om specialets omdrejningspunkt, samtidig med at vedkommende ligeledes skal forfølge det nye og uventede, som eksperten fortæller om undervejs (Staunæs & Søndergaard, 2005, s. 56). Dette taler ydermere også ind i fordelen ved at benytte sig af den semistrukturerede interviewmetode, som indeværende speciale som bekendt har anvendt. Et eksempel fra interviewene, hvor det gjorde sig gældende, at intervieweren skulle omstrukturere den i forvejen opstillede interviewguide var i tilfælde, hvor det tidsmæssige aspekt qua Crime-Script ikke blev fulgt stringent. Det hændte således, at eksperternes fortællinger sprang imellem før, under og efter handlingerne i de to kriminalitetsformer.

Selve interviewene forløb således, at der blev startet ud med småsnak med den pågældende ekspert for på bedst mulig vis at skabe en behagelig samt indbydende stemning (Kvale & Brinkmann, 2015c, s. 183). Herudover blev hver ekspert orienteret om henholdsvis formålet med interviewet, rammerne herfor samt deres rettigheder i forbindelse med hver deres medvirken i interviewet i form af samtykkeerklæringen (Bilag 3). Da hvert interview var nået til vejs ende, blev de ligeledes adspurgt, hvorvidt der var opstået nogle spørgsmål eller tilføjelser til interviewet undervejs. I alt varede hvert interview mellem 45-60 minutter.

Da interviewene blev afholdt, viste det sig, at det ikke var alle vores i forvejen opstillede spørgsmål, der var lige relevante. Nogle af interviewspørgsmålene var for generelle og dermed ikke specificeret nok til hver enkelt eksperts faglighed. Det blev dog vurderet undervejs, at det ville være vanskeligt at udforme nye forskellige interviewguides, eftersom eksperterne ofte tog udgangspunkt i særskilte sager, som de fandt relevante i selve interviewsituationen. Det var dog stadig muligt gennem en vekselvirkning af åbenhed og de opstillede spørgsmål, qua den semistrukturerede interviewform, at indfange relevant og tilstrækkelig viden i henhold til specialets emne.

4.8 Bearbejdning af empiri

Efter gennemførelsen af interviewene påbegyndte vi bearbejdningen af den empiri, der blev indsamlet. Alle interviews blev audiooptaget ved brug af Microsoft Teams. Dette gav den pågældende interviewer muligheden for at kunne koncentrere sig om selve interviewet samt dynamikken heri, uden at skulle nedskrive det sagte undervejs. Ved at interviewene netop er optaget, forefindes de i en permanent form, hvilket gav muligheden for at kunne lytte til dem på ny og ad flere omgange (Kvale & Brinkmann, 2015d, s. 236-237). Efter de respektive optagelser blev downloadet fra Microsoft Teams, blev de således overført til AAU's lokale opbevaring af data *Fileshare*, hvor kun indeværende specialegruppe har adgang til. Efter overførelsen hertil blev hver fil slettet fra computeren, hvilket har gjort, at lydfilerne er udvekslet på en forsvarlig måde jf. GDPR. Disse lydoptagelser blev transskriberet efterfølgende.

4.8.1 Transskription

Ved at transskribere de pågældende interviews fra lydoptagelse til skriftlig form, egner materialet sig således til den videre analyse (Kvale & Brinkmann, 2015d, s. 237-238). Transskriberingen kan dog fordre, at en fortolkningsproces opstår, hvor forskellen mellem det sagte og det skrevne kan udlede problematikker. Disse problematikker er bl.a., at der går elementer tabt, når netop materialet skriftliggøres. Dette kan eksempelvis omhandle stemningen, kropssproget samt tonelejet (Kvale & Brinkmann, 2015d, s. 236).

Eftersom det var alle gruppemedlemmerne der var inde over transskriptionsprocessen af interviewene, var det nødvendigt på forhånd at opstille skriftlige instruktioner på, hvorledes transskriptionen skulle udføres (Kvale & Brinkmann, 2015d, s. 239). Der blev bl.a. taget et valg om, at udtalelserne i interviewene skulle transskriberes ordret for at bevare meningsindholdet i det sagte. Dog var dette med undtagelse af ord såsom "hmm" samt "øh" for at opretholde en mere formel skriftsproglig stil for læserens skyld (Kvale & Brinkmann, 2015d, s. 239-240). I transskriptionen tydeliggøres det desuden, ved at anvende forkortelser, hvem der udtaler hvad i interviewene: *IP* referer til interviewpersonen, *I* til intervieweren og *O* til observatøren. Derudover markeres tænkepauser, emneskift eller afbrydelser med [...] (Tanggaard & Brinkmann, 2020a, s. 52). Ved at bruge samme skriveprocedure fremstår transskriptionerne så gennemskuelige som overhovedet muligt, hvilket ligeledes lettede

sammenligningerne af elementerne i interviewene (Kvale & Brinkmann, 2015d, s. 239). Yderligere er der kun inddraget én skriftlig briefing (Bilag 5) i transskriptionerne, da det blev vurderet unødigt at gentage samme procedure i alle transskriberinger, da briefingen var ens i samtlige interviews. Alle interviewpersoner har ikke desto mindre fået den mundtlige briefing jf. afsnit 4.7.2 omhandlende interviewsituationerne.

Derudover oplevede vi lydproblemer i interviewet med Sidsel Harder, hvilket gjorde transskriberingen af netop disse pågældende tidspunkter vanskeligt. Konkret har alle tre studerende i indeværende speciale forsøgt at lytte til disse tidspunkter for at give sit besyv på, hvad der oprindeligt bliver sagt. Det er dog ikke lykkedes alle gange at lytte sig frem til, hvorfor disse tidspunkter er markeret med *utydelig lyd* i transskriberingen.

Alle citater, der benyttes i indeværende speciale, vil fremstå med, hvilket bilag samt linjenummer, der refereres til. De fulde transskriptioner kan tilgås i bilag 5-9. Når vi henviser til disse bilag, er det med udgangspunkt i linjenumre, da dette fordrer, at der kan refereres præcist tilbage til transskriptionerne (Kvale & Brinkmann, 2015e, s. 371).

4.8.2 Kodningsstrategi

For på bedste vis at danne et overblik over specialets indsamlede empiri i form af ekspertinterviews, og dermed at imødekomme det senere analysearbejde, blev der efter udarbejdelsen af transskriptionerne benyttet en kodningsstrategi.

Kodning bidrager til at skabe struktur og få et overblik over et ellers omfattende tekstmateriale (Kvale & Brinkmann, 2015f, s. 262). Måden, hvorpå transskriptionerne blev kodet, var i form af læsning af det transskriberede materiale og undervejs identificere én eller flere udtalelser, som passede under det pågældende tema. Koderne er derfor udarbejdet ud fra den *begrebsdrevne*-tilgang (Tanggaard & Brinkmann, 2020a, s. 56), da tematikkerne er på baggrund af de fire stadier Preparation, Pre-activity, Activity og Post-activity af Tompson og Chainey jf. afsnit 4.1 omhandlende Crime Script som forskningsdesign.

Vi har anvendt programmet Nvivo 12 til at udarbejde kodningen. Dette program fordrer nemlig, at alle gruppemedlemmer kan kode i den samme transskription. I praksis gjorde det sig gældende, at alle gruppemedlemmer fik til opgave at kode hver enkelt af de fem transskriptioner under de førnævnte tematikker. Dernæst blev de færdigkodede transskriptioner

diskuteret indbyrdes for eventuelle manglende pointer samt for at danne et fælles overblik over empirien. Det er ydermere vigtigt at have in mente, at det ikke har været til hensigt at opnå en fuldkommen overensstemmelse mellem alle kodninger i alle transskriptionerne men til gengæld at have fokus på, hvad der indgik i hver eksperts forklaring og viden.

Oprindeligt havde vi påtænkt at kode det sekundære litteratur, jf. afsnit 4.3.1 omhandlende sekundær litteratur, på samme måde som det ovenstående primære empiri. Dog fandt vi frem til under denne litteratursøgning hertil, at litteraturen oftest kun indebar én af de fire stadier. Vi vurderede det derfor unødigt at kode det sekundære litteratur i Nvivo, hvorfor vi i stedet blot valgte at notere de relevante passager. Dette viste sig at være tilstrækkeligt og gav et fyldestgørende overblik over den sekundære litteratur.

4.9 Kvalitetssikring

Ofte sker det, at de gældende kvalitetskriterier fra den kvantitative forskningstradition overføres til den kvalitative forskningstradition. Disse kvalitetskriterier er henholdsvis *Reliabilitet, Validitet* samt *Generalisering.* Der foreligger dog ikke enighed omkring, hvorvidt disse begreber direkte kan benyttes i kvalitativ forskning, som begreberne kan i kvantitativ forskning. Kritikere argumenterer for, at ved at overtage disse begreber direkte, vil den kvalitative forskning således underkendes (Tanggaard & Brinkmann, 2020b, s. 658). Tove Thagaard anbefaler i forlængelse heraf, at Reliabilitet skiftes ud med *Transparens*, Validitet udskiftes med *Gyldighed*, og *Genkendelighed* skal stå i stedet for Generalisering (Tanggaard & Brinkmann, 2020b, s. 658). Det er derfor disse tre begreber, Transparens, Gyldighed og Genkendelighed, der vil være omdrejningspunktet i indeværende afsnit.

Transparens som kvalitetskriterium i kvalitative studier opnås ved en høj grad af metodologisk refleksion og dermed at velbegrunde sine valg ift. metodisk litteratur. Dette resulterer i, at læseren bedst muligt formår at kunne "*kigge forskeren over skulderen for at kunne gennemskue vejen fra design af undersøgelsen til udførelse, analyse og resultater"* (Tanggaard & Brinkmann, 2020b, s. 660). Når dette er muligt, vil læseren derfor både kunne stille sig kritisk over for undersøgelsens endelige resultater, samtidig med at specialet i højere grad kan inspirere til at udføre lignende studier i både samme og andre sammenhænge (Tanggaard & Brinkmann, 2020b, s. 660). Reliabilitet, som efterstræbes i den kvantitative forskning, søger efter målet om at kunne gentage og opnå samme resultater i anden forskning. Dette er der ikke

fokus på i den kvalitative forskning. Det vurderes derfor, at det anses som værende absurd at forlange, at andre forskere vil kunne gentage et interview, og dermed opnå præcis samme udtalelser fra informanten og samtidig at tro, at observatøren vil se, opleve og mærke det samme under interviewet. Målet er derimod, at gennemførelsen og designet er så transparent som muligt, for at læseren kan vurdere sammenhængen, som de pågældende resultater skal betragtes ud fra (Tanggaard & Brinkmann, 2020b, s. 660). Vores værdier, interesser og antagelser i indeværende speciale skal derfor gøres eksplicitte, da læseren på denne måde kan fortolke det givne data samt muligheden for at overveje eventuelle alternativer. Triangulering muliggør, at vi kan analysere facetteret empiri og præsentere resultaterne til andre på en grundig måde, så de kan forstå, hvordan uberettiget adgang og ulovlig billeddeling udspiller sig i praksis. Ydermere er vi løbende i analysen eksplicitte omkring, hvilken sekundær litteratur vi trækker på de enkelte steder, samtidig med vi udførligt har opstillet en tabel, der indeholder specialets sekundære empiri og information herom (Bilag 10). Alt dette imødekommer ligeledes ønsket om transparens i indeværende speciale. Derudover argumenteres der for, at en grundig beskrivelse af rekrutteringen af eksperterne samt de pågældende interviewsituationer er at foretrække ift. transparensen. Foregik deltagelsen af interviewene frivilligt? Hvordan var interviewsituationerne, og hvad er begrundelsen for antallet af informanter og kriterier for netop valget af pågældende informanter? (Tanggaard & Brinkmann, 2020b, s. 661-662). Dette er imødekommet i afsnit 4.6 omhandlende udvælgelse og rekruttering af informanter samt afsnit 4.7.2 omhandlende interviewsituationerne. Ydermere vil det gøre sig gældende, at specialets data vil gøres eksplicit i form af eksempler i den kommende analyse for på bedst mulig vis at kunne vurdere sammenhængen af data og forskerens forståelse heraf. Der er ligeledes markeret tydeligt ved hvert citat fra den primære empiri, i hvilket bilag (5-9) og linjenumre citatet kan tilgås, jf. afsnit 4.8.1 omhandlende transskription. Dette giver ligeledes læseren mulighed for at anskue konteksten, hvori citatet er udtaget fra.

Gyldigheden i pågældende undersøgelse sikres ved, at de endelige resultater kontrolleres så udtømmende som muligt ved at samtlige gruppemedlemmer deltager heri. Dette imødekommer nemlig eventuelle diskrepanser, fejl eller deciderede overdrivelser. Et konkret eksempel fra indeværende speciale er, at vi alle deltog i kodningerne af samtlige transskriptioner jf. afsnit 4.8.2. Tanggaard og Brinkmann argumenterer ydermere for, at ingen forskning, såvel som forskere, kan agere fuldstændig neutral, hvorfor dette bør indgå i en reflekterende tilgang til analysens data. Det skal derfor fremstå tydeligt, at konklusionerne er på baggrund af

informanternes udtalelser og ikke forskeren selv. Derudover bør alle analysedele være så empirinære som overhovedet muligt (Tanggaard & Brinkmann, 2020b, s. 662). Yderligere kan der argumenteres for, at triangulering, jf. afsnit 4.3, øger sandsynligheden for at specialets fund er så præcise og pålidelige som muligt, i det at der inddrages flere forskellige datakilder.

Genkendelighed kommer af, at den kvalitative forskning ofte kritiseres for at indeholde for få individer, for at de endelige resultater vil kunne generaliseres, som det er muligt at gøre med kvantitative data (Kvale & Brinkmann, 2015g, s. 332). Generalisering er heller ikke den kvalitative forsknings formål men derimod at kunne påpege specifikke tilfælde - i form af specialets udvalgte eksperter - til at kunne sige noget mere generelt om omdrejningspunktet for specialet (Bryman, 2016, s. 399; Åkerstrøm & Wästerfors, 2018, s. 145). Kvale og Brinkmanns begreb om *Analytisk generaliserbarhed* kan derimod bruges til at imødegå netop kritikken om den manglende generaliserbarhed i kvalitativ metode. Begrebet dækker over, hvorledes specialets resultater kan benyttes i lignende sammenhænge. Eftersom specialets sekundære litteratur omtaler og underbygger de samme fænomener som specialets primære empiri, må dette således også betyde, at andre studier kan anvende vores analytiske fund. Den analytiske generaliserbarhed opnås således gennem relevans, detaljeniveau samt præcision angående specialets beskrivelser. Som redegjort for i afsnit 4.2, jf. specialets forskningstilgang, opstilles der ikke en endelig konklusion, når der arbejdes ud fra den abduktive tilgang (Birkler, 2021, s. 94). Dette fordrer derfor, at indeværende speciale er åben for, at fremtidige interesserede kan arbejde videre på fundene, der vil ekspliciteres senere. Analytisk generaliserbarhed anses derfor som en vejledning til, hvad der kan opnås i tilsvarende specialer (Kvale & Brinkmann, 2015g, s. 334-335).

4.10 Etiske overvejelser

Ønsket med indeværende speciale er som bekendt at videregive forskningsresultater til specialets samarbejdspartner NC3, sådan at materialet kan agere som nyttigt værktøj i kriminalpræventivt regi. Dog er det stadig hensigtsmæssigt at reflektere over, hvilken data der bliver produceret, og hvordan dette håndteres på forsvarlig vis, når problemstillingen netop omhandler kriminalitet.

Hvilke værdier der er på spil i kvalitativ forskning, afhænger i høj grad af det konkrete forskningsprojekts erkendelsesinteresse (Brinkmann, 2020, s. 587). Ofte angår de etiske

overvejelser menneskets personlige liv og erfaringer i kvalitativ forskning (Brinkmann, 2020, s. 581). Her er der således ofte tale om mikroetiske problematikker, hvor der skal tages vare på de personer, der er en del af forskningen (Brinkmann, 2020, s. 593). I indeværende speciale er fokusset derimod på den makroetiske dimension, der indebærer forskningens placering i en samfundsmæssig sammenhæng (Brinkmann, 2020, s. 593). Den indsamlede empiri består som bekendt af ekspertviden om uberettiget adgang til intimt materiale og videredeling af dette, hvorfor det ikke omhandler eksperternes egen livsverden. Den viden, der bliver tilgængelig, indebærer derfor udførelsen af en kriminel handling. Det var derfor nødvendigt at overveje publiceringen af bestemte resultater, da nogle individer kan have et ønske om at misbruge denne information. Både ekspertudtalelser samt vores litteratursøgning beror dog på, at der i forvejen foreligger let tilgængeligt materiale om udførelsen af flere forskellige IT-kriminalitetsformer på internettet. Dette kommer bl.a. til udtryk i interviewet med Christoffer Herlufsen:

> *"Man kan sige, at før i tiden krævede det meget teknisk kunnen at lave IT-kriminalitet, hvorimod i dag er det meget mere tilgængeligt for normale mennesker, også fordi at der ligger så meget viden ude på nettet. Så, det behøver ikke en speciel mobil, men bare en forståelse for, hvordan sociale medier er skruet sammen på"* (Bilag 7, l. 152-157).

Vi vurderer således, at specialets publicering ikke består af enestående sensitiv information, som gerningspersoner ikke i forvejen kan finde på internettet, hvis vedkommende er motiveret herfor.

4.11 Analysestrategi

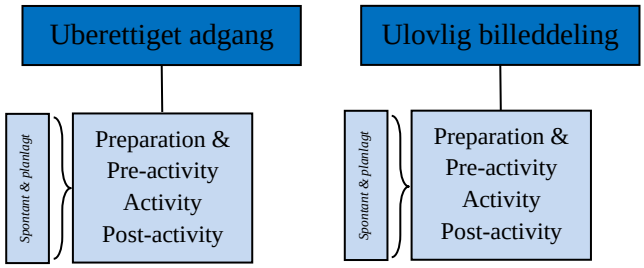
Følgende afsnit består af en beskrivelse af, hvordan indeværende speciales analyse udarbejdes. Afsnittet vil således indeholde analysens opbygning, og hvordan den primære og sekundære empiri samt de identificerede teorier løbende bliver inddraget.

Da indeværende speciale som bekendt er udarbejdet på baggrund af en Crime Script-tilgang, opbygges analysen ligeledes herefter. Selvom eksperterne i specialets primære empiri ofte berettede om gerningspersonens motivation[4] til at begå kriminalitet, er dette ikke noget der

[4] To af specialets eksperter benytter adjektivet "ond", når de forklarer om motivationen bag disse kriminalitetstyper (Bilag 5, l. 479, 486-487, 581; Bilag 9, l. 687). Derudover beskriver tre af eksperterne motivation i form af at fremstå sej, at det er sjovt, spændende og frækt at dele intimt materiale, samt at det giver status og respekt i vennegruppen (Bilag 5, l. 403-405; Bilag 6, l. 499-504, 546-554; Bilag 7, l. 430-440).

bliver inddraget i analysen. For at klarlægge hvilke skridt, der indgår i anskaffelsen af uberettiget adgang til intimt materiale og ulovlig billeddeling, bliver analysen i stedet opdelt i disse to kriminalitetsformer. Dette gøres for at kunne identificere de enkelte sekvenser, der forefindes fra start til slut under hver kriminalitetsform. For at overskueliggøre analyseopsætningen har vi udarbejdet en visualisering i *Figur 3: Analyseopsætning*. Som det fremgår af denne, er første delanalyse uberettiget adgang og anden delanalyse ulovlig billeddeling. Som nævnt i afsnit 4.1, omhandlende Crime Script som forskningsdesign, opstiller Tompson og Chainey fire forskellige stadier, der indgår i et Crime Script. Disse stadier udfoldes derfor under den enkelte kriminalitetsform, hvortil der under hvert stadie skelnes mellem en spontan og planlagt udgave. Disse to udgaver bliver uddybet yderligere i analysen (afsnit 5).

Figur 3: Analyseopsætning



Som det fremgår af ovenstående figur, har vi valgt at sammenfatte stadierne Preparation og Pre-activity, således at de går under én fase. Dette skyldes bl.a., at de begge udgør opsætningen af den kriminelle handling (van der Bruggen & Blokland, 2021, s. 957). Yderligere var det fremtrædende i specialets primære empiri, at de to stadier ofte overlappede hinanden, hvorfor de ofte var svære at skelne mellem. Vi anser derfor Preparation og Pre-activity som én samlet betegnelse for de forberedelser, overvejelser og beslutninger, der er nødvendige at foretage før den identificerede kriminelle handling udføres. Som beskrevet i afsnit 4.1, omhandlende Crime Script som forskningsdesign, anses Crime Scripts ikke som værende præskriptive, hvorfor sammensætningen af de pågældende to trin vurderes muligt. De tre stadier, Preparation & Pre-activity, Activity og Post-activity, vil således indgå som de overordnede tematikker i den kommende analyse. Dette muliggør en klar forståelse af hvilke aktører, overvejelser, handlinger og kontekst, der indgår i anskaffelsen af uberettiget adgang til intimt materiale samt videredelingen heraf.

Undervejs i analysen bliver der inddraget relevant eksisterende litteratur qua specialets triangulering. Formålet med dette er som bekendt at supplere med tilstrækkelig viden, der kan understøtte specialets primære empiri. På denne måde kan de relevante pointer fremstå tydeligere, og der kan dannes en sammenhæng mellem de forskellige udsagn. Derudover anlægger vi et teoretisk perspektiv, jf. Social læringsteori og Rutineaktivitetsteori, på de fire stadier under de opsummerende afsnit i analysen, hvilket forekommer sidst under det hvert enkelt stadie. At vi således har valgt at knytte væsentlige teoretiske forklaringer i opsummeringerne, gør at vi stringent holder os til *hvordan*-spørgsmålet, som Crime Script fordrer. Ligeledes argumenterer vi for i afsnit 4.1, omhandlende Crime Script som forskningsdesign, at netop Crime Script anskues som en ateoretisk tilgang, hvorfor valget om at beholde teori i opsummeringerne synes fordelagtigt.

Slutteligt er det vigtigt at pointere, at de scripts der bliver udarbejdet ikke er perfekt lineære, da nogle gerningspersoner ikke følger alle opstillede trin. Som vi ydermere argumenterer for i afsnit 4.1, findes der ikke ét særligt script til hver kriminalitetsform, men derimod forekommer der variationer i scriptene afhængig af den pågældende gerningsperson og målet. Grundet at disse scripts ikke forekommer perfekt lineære gør således, at vi qua vores abduktive tilgang er åbne for yderligere scripts samt fortolkninger af de respektive kriminalitetsformer. De scripts der forekommer i indeværende speciale er således udarbejdet på baggrund af specialets fem ekspertinterviews samt eksisterende litteratur, hvorfor andre undersøgelser med andre informanter således kan nå frem til andre scripts.

Kapitel 5
Analyse

5. Analyse

Følgende kapitel består af specialets analyse. Flere af eksperterne i specialets primære empiri har i deres fagfelt observeret to forskellige "grupper" i relation til uberettiget adgang til intimt materiale og ulovlig billeddeling (Bilag 5, l. 305-327; Bilag 6, l. 92-113; Bilag 7, l. 50-104). Disse påtales som en *planlagt* og *spontan* udgave. Vi anser således de planlagte sager som en kompleks udgave af de sager, der forekommer spontant. Den planlagte består af motiverede gerningspersoner, der udførligt forbereder, planlægger og gennemtænker hver enkelt skridt for at kunne fuldføre den kriminelle handling. Den spontane udgave er derimod gerningspersoner, der for det meste allerede har adgang til det intime materiale, og som udgangspunkt deler dette relativt impulsivt. På baggrund af kapitel 2 jf. specialets problemfelt samt to af eksperternes fortællinger er det ofte unge mennesker, der dominerer den spontane gruppe (Bilag 6, l. 309-315, 351-353; Bilag 7, l. 76-82, 266-267, 459-464). Det er denne spontane gruppe, der forekommer flest sager af ifølge flere eksperter i den primære empiri (Bilag 5, l. 435-439; Bilag 6, l. 214-217; Bilag 7, l. 68-73), hvorimod det er i den planlagte gruppe, at der typisk forekommer flest forurettede (Bilag 5, l. 687-689, 768-771; Bilag 6, l. 215-226). For at specificere disse to grupper kan der nævnes to velkendte sager, hvor både uberettiget adgang samt ulovlig billeddeling indgår. En sag som knytter sig til den spontane gruppe er Umbrella-sagen, som der i indeværende speciale refereres til i afsnit 2.3 omhandlende ulovlig billeddeling. En sag der knytter sig til den planlagte gruppe er Herning-sagen, som refereres til i afsnit 2.2.1 omhandlende Social Engineering.

5.1 Uberettiget adgang

Første delanalyse omhandler uberettiget adgang af intimt materiale. Det er således kriminelle aktiviteter, som udspiller sig inden den ulovlige billeddeling. Følgende indebærer en beskrivelse af både før, under og efter anskaffelsen af uberettiget adgang.

5.1.1 Preparation & Pre-activity

Stadierne Preparation og Pre-activity dækker over gerningspersonens forberedelser, valg og handlinger op til den specifikke kriminelle handling. Det vil altså sige, at dette stadie omfatter det, der er nødvendigt at gøre inden den uberettigede adgang igangsættes.

Som nævnt skelner eksperterne løbende mellem en spontan og en planlagt udgave af uberettiget adgang. Dette er en væsentlig distinktion, da eksperterne beretter om, at der i den spontane udgave ikke nødvendigvis er tale om *uberettiget* adgang. I stedet er der tale om, at det pågældende individ ofte allerede er i besiddelse af det intime materiale, typisk fra tidligere intime forhold (Bilag 7, l. 69-73; Johansen, Pedersen & Tjørnhøj-Thomsen, 2019, s. 1034). Det fremgår nemlig af ekspertinterviewene med politikommissær Flemming Kjærside, specialanklager Morten Rasmussen og forsker i IT-kriminalitet Lene Wacher Lentz, at det at sende nøgenbilleder til sin kæreste, i form af sexting[5], anses som en normal del af et parforhold i nutidens samfund (Bilag 5, l. 437-439; Bilag 6, l. 849-851; Bilag 9, l. 154-155). En del af forberedelsen til sexting er derfor som minimum en digital enhed, f.eks. mobiltelefon eller computer, med internetforbindelse (Bilag 5, l. 824-827; Bilag 6, l. 155-160). Derudover er tillid en væsentlig forudsætning for at ville deltage i denne handling. Tillid opnås dér, hvor vedkommende potentielt er i risiko for at blive eksponeret men alligevel vælger at tro på, at modparten kun handler ud fra gode intentioner. Tillid tolkes derfor som en opdyrket forventning om, at modtageren af det intime materiale vil respektere afsenderen af det og dermed ikke har i sinde at videresende materialet til andre (Chatzinikolaou & Lievens, 2020, s. 39, 41). Tali Hatuka og Eran Toch påpeger derudover, at mobiltelefonen er en yderst personlig digital enhed, der inkluderer individets online relationer og de sociale kontekster, vedkommende er en del af. De skaber på baggrund heraf fænomenet *Portable private-personal territory*. Dette indikerer et personligt rum, som individet udvikler på baggrund af teknologien, og som karakteriserer en række af sociale relationer, som vedkommende indgår i (Hatuka & Toch, 2014, s. 2194, 2203; Mandau, 2019, s. 76). Disse teknologiske muligheder for socialt samvær må derfor ligge forud for videregivelsen af intimt materiale, da de er med til at præge individets seksuelle og romantiske forhold (Mandau, 2019, s. 73, 76). Michelle Ybarra og Kimberly Mitchell italesætter yderligere, at denne teknologidrevne adfærd (at videregive nøgenbilleder af sig selv) er en ny måde at udtrykke seksualitet på (Ybarra & Mitchell, 2014, s. 757, 760-762). Udviklingen og brugen af digitale medier, og dertilhørende normer og værdier, har derfor medbragt en række nye koncepter og fænomener, heriblandt netop sexting. Denne måde at udtrykke sig på i et forhold, vurderes dog alligevel som forholdsvis spontan, da det er relativt let og simpelt at tage et billede af sig selv og sende det til den pågældende

[5] Sexting er en sammentrækning af ordene "sex" og "texting", og er når en person kreerer, deler eller poster seksuelt materiale af sig selv via mobiltelefoner, herunder sociale medier såsom Facebook og Snapchat (Johansen, Pedersen, Tjørnhøj-Thomsen, 2019, s. 1029; Dahl, Henze-Pedersen, Østergaard & Østergaard, 2018, s. 37; Mandau, 2019, s. 73).

modtager. Der findes dog alligevel en række omstændigheder, som indirekte er med til at influere det at anskaffe intimt materiale på. Eftersom fænomenet sexting er selve udførelsen af anskaffelsen af intimt materiale, udfoldes dette yderligere i stadiet Activity i afsnit 5.1.2.

Hvad der indgår under Preparation og Pre-activity stadiet hos den planlagte form for uberettiget adgang kan derimod variere alt efter, hvilken metode gerningspersonen vælger at anvende. Der findes en del tilgængelig information på internettet omkring dette, som gerningspersonen kan udnytte (Bilag 5, l. 227-229; Bilag 7, l. 124-138). Morten Rasmussen nævner i relation til dette:

"Det der er problemet med det her, det er jo, at man kan finde utroligt meget på nettet både i form af måder, hvor der er beskrevet: "Sådan her kan du gøre det", men også værktøjer, hackerværktøjer, som man jo kan købe mere eller mindre frit. Der behøver man ikke engang at gå på dark web, men det kan man jo gøre" (Bilag 6, l. 140-145).

Det er derfor ikke særlig kompliceret at finde frem til, hvilke muligheder der er for at anskaffe intimt materiale uberettiget. Lene Wacher Lentz udtaler ydermere, at vedkommende derudover kan finde inspiration fra tidligere offentlige sager, herunder hvordan den daværende gerningsperson blev opdaget. Dette kan vedkommende derfor bruge til at mindske sin egen opdagelsesrisiko og dermed forberede sig bedre (Bilag 9, l. 687-709).

I fire ud af fem af specialets ekspertinterviews blev Social Engineering omtalt som den fremgangsmåde, der oftest bliver anvendt i digitale sexkrænkelsessager i Danmark (Bilag 5, l. 42-47; Bilag 6, l. 152-155; Bilag 7, l. 92-99; Bilag 9, l. 594-598). Eksempelvis forklarer Flemming Kjærside, at "traditionel hacking" anses som en forældet forståelse af uberettiget adgang, og at det nu er Social Engineering, der dominerer:

"[...] den traditionelle hacking er ikke det, vi ser i disse sager. Det er uberettiget adgang, og det er Social Engineering, hvor man narrer nogen til noget. Så det der med at nogle hacker sig ind og kommer om natten og skaffer sig adgang til computeren udefra, det er ikke det, vi ser" (Bilag 5, l. 42-47).

At Social Engineering er en af de mest anvendte metoder til at opnå uberettiget adgang, er en opfattelse der ligeledes gør sig gældende hos andre studier (Abraham & Chengalur-Smith, 2010, s. 183; Lohani, 2019, s. 385). Ifølge Sherly Abraham og Indushobha Chengalur-Smith er Social Engineering-angreb konstant i udvikling og bliver kun mere komplekse og sofistikerede (Abraham & Chengalur-Smith, 2010, s. 194). Ifølge Abraham og Chengalur-

Smith er det nødvendigt for gerningspersonen at kunne manipulere følelser såsom frygt, nysgerrighed og empati hos offeret og samtidig have tilstrækkelig viden omkring, hvordan der skabes et vellykket Social Engineering-angreb (Abraham & Chengalur-Smith, 2010, s. 185-186). Indsamlingen af informationer kræver hertil, at gerningspersonen undersøger relevant information om det pågældende offer, hvilket eksempelvis kan ske gennem diverse sociale medier (Ozkaya, 2018a, s. 16).

Yderligere påpeger Abdullah Algarni, Yue Xu og Taizan Chan, at gerningspersonen helst skal opfattes som oprigtig, kompetent, attraktiv og værdig, for at offeret føler sig tilpas nok til at udlevere privat information (Abdullah, Xu & Chan, 2017, s. 665). Det kræver derfor en del forarbejde i henhold til at fremstå på en bestemt måde. Disse psykologiske taktikker er en vigtig del af et Social Engineering-angreb, da ingen computerkomponenter eller software kan forhindre angrebet (Lohani, 2019, s. 385; Koyun & Janabi , 2017, s. 1). Gerningspersonen må derfor forstå, inden udførelsen af angrebet, hvem deres offer er, og hvordan vedkommende tænker (Hadnagy, 2010a, s. 103). Hvis gerningspersonen kender offeret i forvejen, er det derfor også lettere at spore sig ind på, hvordan der kan opbygges tillid: "*It has been shown through research that most people are drawn closer to individuals they are fond of and they end up developing trust for them"* (Abdullah et al., 2017, s. 666). Derudover er det ligeledes væsentligt at nævne, at denne tillid ydermere allerede kan være etableret forinden, netop gennem relationen mellem gerningsperson og offer. Dette fordrer derfor, at gerningspersonen i disse tilfælde kan springe dette skridt over. Ved at opnå viden omkring offeret og vedkommendes interesseområde, jf. afsnit 2.2.1, omhandlende Social Engineering, kan gerningspersonen derfor planlægge den bedste måde at snyde og lokke offeret på (Hasan, Prajapati & Vohara, 2010, s. 19).

Selvom at det kan lette gerningspersonens forberedelse, hvis de allerede har et forhold til offeret, kan det ligeså vel være et tilfældigt offer, gerningspersonen udvælger (Bilag 7, l. 99-100). Dette kræver formentlig en længere informationsindsamling omkring det pågældende offer, da de personlige oplysninger ikke er velkendte fra start af. Det er dog stadig muligt at udføre et angreb, ligesom hvis det var en bekendt, men det vurderes dog nemmere at opnå tillid til et offer, gerningspersonen i forvejen kender.

Opsummering af Preparation & Pre-activity

Når der er tale om de spontane situationer, fremgår det, at især tillid er essentiel i parforhold, hvor nøgenbilleder er en del af den seksuelle adfærd. Der medfølger således bestemte normer og værdier på baggrund af de relationer, individet er en del af i både den offline og online verden. Dette inkluderer eksempelvis en forventning om gensidige nøgenbilleder fra modtageren og en generel fælles forståelse af håndteringen af det intime materiale. Dette lærer de eksempelvis gennem tidligere erfaring i parforhold og indbyrdes kommunikation omkring, hvad der er tilladt og fortrinlig adfærd (Akers, 2011[1994], s. 132-134; Akers & Jennings, 2019, s. 115, 117- 118; Cohen & Felson, 2013, s. 469-470). Derudover har den teknologiske udvikling i samfundet, qua forandrede rutineaktiviteter, ligeledes præget, hvordan der interageres og kommunikeres i disse intime forhold. Digitale enheder, såsom mobiltelefoner, udspiller sig i højere grad i sociale- og online sammenhænge. Nøgenbilleder anses derfor som en måde at udtrykke seksualitet og kærlighed på, hvorfor det er muligt, at flere personer besidder intimt materiale uden en egentlig uberettiget adgang har fundet sted. Opsummerende omhandler Preparation og Pre-activity stadiet ift. den spontane udgave, at der opbygges en form for tillid mellem de respektive parter inden sexting, hvorfor der forekommer berettiget adgang til det intime materiale.

I de planlagte situationer forekommer der mere udførlige forberedelser og overvejelser, inden den uberettigede adgang bliver forsøgt opnået. Gerningspersonen skal bl.a. træffe en beslutning omkring, hvilken metode der skal benyttes for at opnå uberettiget adgang. Social Engineering er en af de metoder, som motiverede gerningspersoner har lært om gennem online kilder, heriblandt offentlige sager, andre kriminelles beretninger samt eventuelt tidligere individuel erfaring, hvorfor der også her forekommer et element af social læring. Denne læring gør også, at den pågældende motiverede gerningsperson opnår viden omkring, at der i Social Engineering-angreb typisk er et fravær af kapable vogtere. I et traditionel hackingangreb består kapable vogtere ofte af diverse computerkomponenter eller softwareprogrammer. Disse kan dog ikke forhindre et Social Engineering-angreb. Denne viden vil uden tvivl være til gavn ift. gerningspersonens valg af metode og den videre forberedelse (Felson & Clarke, 1998, s. 4). Derudover kan det udledes, at jo hyppigere gerningspersonen opnår uberettiget adgang med den samme metode, desto mindre forberedelse og færre spekulationer kræves det fremover. Ifølge indeværende speciales Crime Script-tilgang lagres disse manuskripter nemlig i individets hukommelse, hvorfor den specifikke modus huskes som værende en standardiseret

samt generaliseret episode (Haelterman, 2016b, s. 8). Denne Crime Script tanke kan således sættes lig med Akers læringsteoretiske begreb omhandlende Differential reinforcement (Akers, 2011[1994], s. 133-134; Akers & Jennings, 2019, s. 117). Akers påpeger nemlig med dette begreb, at gerningspersonen vil genoptage den pågældende adfærd, når der forekommer en form for belønning. Gerningspersonen lærer altså på baggrund af disse lagrede manuskripter, hvad der udløser henholdsvis positive- og negative reinforcement.

5.1.2 Activity

Følgende stadie omhandler Activity, som er selve udførelsen af uberettiget adgang. Dette indebærer, at gerningspersonen lykkes med den kriminelle handling og dermed får fat i det intime materiale.

Som præsenteret i forrige afsnit er der ikke tale om uberettiget adgang i de tilfælde, hvor en person har opnået adgang til det pågældende materiale med samtykke fra ophavsmanden. Analytiker Christoffer Herlufsen påpeger netop dette: *"Men i rigtig rigtig mange af sagerne er det billeder, de allerede har fået tilsendt, ikk'? Uberettiget adgang behøver ikke engang at være benyttet i mange af sagerne"* (Bilag 7, l. 218-221). Det er derimod ofte anskaffet gennem sexting, hvorfor der ikke er tale om en kriminel handling, men derimod en handling, der udspiller sig i parforhold, hvor parterne ønsker at imponere ved at sende intime billeder til hinanden (Jaishankar, 2009, s. 21-22). Sexting anses derfor som et resultat af den digitale teknologis udvikling (Strasburger, Zimmerman, Temple & Madigan, 2019, s. 1). Når sexting udspiller sig, er det som bekendt med samtykke og tillid fra begge parter. Handlingen udspiller sig derfor, så længe parterne indgår i et tillidsfuldt forhold. Udførelsen af berettiget adgang foregår desuden relativt simpelt grundet de digitale muligheder, der foreligger i nutidens samfund. Dog foreligger der stadig en risiko for en fremtidig formidling af det seksuelle materiale (Johansen et al., 2019, s. 1029; Strasburger et al., 2019, s. 3; Harder, 2022, s. 187). Dette uddybes yderligere i afsnit 5.5.2 jf. afsnittet omhandlende Activity i ulovlig billeddeling.

Sekundær litteratur peger på, at der også findes *ufrivillig sexting.* Dette begreb dækker over, når personer får tilsendt intimt materiale uden at have bedt om dette. I undersøgelsen "*Unges opfattelser af køn, krop og seksualitet"* fra 2018 beskrives begrebet helt konkret:

"Sexting finder dog ikke kun sted i konteksten af flirt eller kæresterelationer. Fra flere af pigerne i denne undersøgelse hører vi, at de har fået tilsendt såkaldte "dickpics", dvs. billeder af mandlige kønsdele, på Snapchat – billeder, de får tilsendt fra fremmede personer, uden at de har bedt om det" (Dahl, Pedersen-Hentz, Østergaard & Østergaard, 2018, s. 39).

Denne ufrivillige sexting nævner post doc forsker Sidsel Harder ligeledes: *"[...] og der er jo også forskel på, hvis du sender et dickpic, er det tit uden, at du er blevet spurgt, om du vil have det [...]"* (Bilag 8, l. 225-227). I skiftet fra sexting til ufrivillig sexting opstår der således en kriminel handling, da et utilsigtet dickpic ifølge Straffelovens § 232 omfatter krænkelse af blufærdigheden. Det som de to sexting-varianter derimod har tilfælles er, at modtageren i princippet er berettiget til at have adgang til det intime materiale, da afsenderen netop har sendt det med samtykke. Når modtageren dog utilsigtet bliver udsat for seksuelle billeder i form af dickpics, udgør det en form for seksuel krænkelse eller chikane (Mandau, 2019, s. 73, 80).

Selve udførelsen af Social Engineering under den planlagte form for uberettiget adgang sker bl.a. i form af bedrageri, løgne og snyd. På denne måde kan gerningspersonen opnå den ønskede information, som gør, at vedkommende får adgang til det intime materiale (Bilag 5, l. 550-554; Hadnagy, 2010b, s. 9). I disse Social Engineering-angreb, hvor målet er uberettiget at opnå adgang til intimt materiale, gør begrebet *Human based* sig oftest gældende. Begrebet dækker over, når angrebene gennemføres via direkte kommunikation mellem gerningspersonen og offeret. Denne direkte kommunikation fordrer således, at der ikke forekommer et stort antal af ofre, som der ville gøre, hvis angrebet skete på baggrund af software, der opsnapper information (Koyun & Janabi, 2017, s. 7534). Et eksempel på hvordan et human based Social Engineering angreb udfolder sig, er ved at gerningspersonen udgiver sig for at være en veninde eller ven for derved at opnå tillid til, at offeret vil udlevere sin adgangskode. Flemming Kjærside beskriver bl.a.:

" [...] så jeg skal have verificeret min konto, kan man så ikke lige låne din til at logge ind, for så kan jeg måske gøre nogle ting. Man kommer med en eller anden plausibel forklaring omkring, at man har behov for at logge ind på den platform, for man har mistet sin adgang, eller eksemplet med Netflix, så man kan se en serie, eller din spillekonto, hvor man ikke lige tænker over, at nogen har et ondt sind. Vi vil jo gerne hjælpe vores venner og veninder, havde jeg nær sagt, og så viser det sig bagefter, at det var altså ikke en veninde, man hjalp, men én der udgav sig for at være din veninde" (Bilag 5, l. 575-584).

og

"Hvis jeg kan overtale dig ved at sige: "For fanden, jeg har mistet adgangen til min Facebook. Kan jeg ikke lige låne dit login eller sådan noget, ikke? For så kan det være med til at genskabe min, og vi er jo gode venner, så kan du ikke gøre det?", og så lige pludselig har jeg fået dit password, og så kan jeg skaffe mig adgang til din computer" (Bilag 5, l. 132-138).

Flemming Kjærside beskriver således denne metode som værende aktuel i planlagte sager om uberettiget adgang i Danmark. Han bruger ligeledes sagen fra Herning som eksempel, hvilken vi har redegjort for tidligere i afsnit 2.2.1, omhandlende Social Engineering: *"Han har snydt sig til adgang og har udnyttet, at han har kendt nogle af pigerne i forvejen, eksempelvis udgivet sig for at være dem og sådan noget for at få adgang til andre computere og sådan"* (Bilag 5, l. 105-108). Ved at narre og snyde offeret kan gerningspersonen derfor skabe en vis form for tryghed og tillid, som hos nogle resulterer i frivillig videregivning af sin adgangskode (Bilag 5, l. 242-245, 373-378). Ydermere anses adgangskoder af flere af eksperterne, som værende den mest essentielle information, som gerningspersonen kan bruge til at få adgang til offerets intime materiale (Bilag 5, l. 244-245; Bilag 7, l. 214-218). Dette skyldes, at en del mennesker anvender det samme kodeord til flere forskellige digitale enheder, eksempelvis Facebook og Netflix (Bilag 5, l. 521-524; Bilag 6, l. 94-98, 872-873; Bilag 7, l. 88-92; Hadnagy, 2010a, s. 103; Hadnagy, 2010b, s. 12).

Hvis det lykkes for gerningspersonen at udgive sig for at være en ven eller veninde, kan det være et væsentligt middel til at skaffe sig yderligere adgang til andre konti. Med fortsat udgangspunkt i ekspertinterviewet med Flemming Kjærside, kan dette foregå således:

"Har jeg først fået adgang til én, så kan jeg jo bruge hendes oplysninger til at få adgang til den næste og næste, ikke? Det er samme modus, man bruger. Nu har jeg fået adgang til din konti, så nu udgiver jeg mig for at være dig, som skriver til en af dine veninder, at "jeg har mistet mit password", og så får jeg passwordet der, og så får jeg den profil til at komme videre og den profil til at komme videre osv." (Bilag 5, l. 388-395).

Sekundær litteratur peger således også i denne retning. Social Engineering kan forekomme i et *single-stage-attack*, hvor gerningspersonen blot vil opnå adgang til én konti, dvs. hvor det ikke er hensigten at benytte sig af denne Snowball-effekt ift. at opnå uberettiget adgang til flere

forskellige ofre. Det kan derimod også udspille sig som et *multi-stage-attack*, hvor opnåelsen af ét offers kodeord benyttes til at få adgang til et bredere spektrum af forurettede (Airehrour, Nair & Madanian, 2018, s. 4). Ovenstående citat fra Flemming Kjærside understøtter derfor fænomenet multi-stage-attack, da dette ofte er noget, han oplever i praksis hos de planlagte tilfælde af uberettiget adgang. Første skridt kan således defineres som at få adgang til forurettedes oplysninger til én platform. Næste skridt kan i forlængelse heraf så blive at forsøge at skaffe sig uberettiget adgang til næste offers ved at udgive sig for at være en veninde eller ven til vedkommende. Hvis gerningspersonen ikke stoppes, kan denne fremgangsmåde således som udgangspunkt fortsætte frit, og der vil altså opstå en Snowball-effekt, som resulterer i netop et multi-stage-attack.

Opsummering af Activity

Ud fra eksperternes beretninger om socialt samvær, opnås der nemt intimt materiale gennem sexting. Dette er dog ikke ulovligt, da materialet blev tilsendt med samtykke. Yderligere indebærer denne handling belønning i form af gengældte intime billeder. Hvordan sexting således foregår, kan parterne bl.a. have imiteret fra sine intime forhold eller den omgangskreds, vedkommende er en del af. Måden hvorpå der bliver kommunikeret om adfærden influerer dermed individets værdier og heraf handlinger. Særligt anses det som socialt lærerigt at imitere andres adfærd ved at anskue, hvilke positive reaktioner som dette medfølger. Denne indflydelse påvirker i højere grad de, som endnu ikke selv har prøvet sexting før (Akers & Jennings, 2019, s. 118). Jf. afsnit 4.1 omhandlende Crime Script som forskningsdesign indsamler individer kontinuerligt viden for at kunne udføre bestemte handlinger, hvorfor denne viden lagres i vedkommendes hukommelse (Haelterman, 2016b, s. 9). Denne pointe kan således underbygge Akers pointe omkring, at en given adfærd har størst indflydelse på dem, som ikke før har gjort brug heraf. Distribueringen af dickpics er ligeledes en form for sexting, dog ufrivilligt i henseende til modtageren. Modtageren reagerer typisk med negative følelser, såsom afsky, da flere opfatter denne handling som krænkende. Afsenderen af det ufrivillige materiale vil derfor opnå negative reinforcement, og dermed ikke den positive reinforcement, som der ofte ses hos den gensidige sexting.

Udførelsen af den planlagte form for uberettiget adgang sker typisk gennem et Social Engineering-angreb. Efter nok indsamling af viden omkring, hvordan dette gøres, qua Preparation og Pre-activity stadiet, kan gerningspersonen udnytte offerets grundlæggende tillid

til andre. At dette er en hyppig måde at bedrage et offer, må gerningspersonen have imiteret fra andre kriminelle, som har anvendt Social Engineering, og hvor det netop er lykkedes dem at fuldføre handlingen (Akers, 2011[1994], s. 134; Akers & Jennings, 2019, s. 118). Social Engineering indgår derfor under Cyber deception and theft, jf. Walls typologi i afsnit 2.1.1 omhandlende kriminalitetsformer, eftersom der opnås adgang til et individs private platform, hvorved der bliver stjålet intimt materiale. Ydermere vil gerningspersonen have hentet inspirationen fra (virtuelle) fællesskaber, hvor Social Engineering-metoden er imiteret fra (Akers, 2011[1994], s. 132; Akers & Jennings, 2019, s. 115). Foruden Akers begreb om Imitation, vil begrebet Differential Association ligeledes kunne bidrage til forståelsen af, hvordan den uberettigede adgang tillæres gennem den sociale gruppe, individet hovedsageligt er en del af. Igennem disse fællesskaber har de eksempelvis lært, at det at foregive sig for at være en veninde/ ven til offeret er en fortrinlig måde at opnå tillid på, da gerningspersonen herigennem hurtigere kan tilegne sig offerets adgangskode. Desuden peger flere eksperter på, at vi mennesker ofte genbruger det samme kodeord på flere virtuelle platforme. Dette er et faktum, som de motiverede gerningspersoner bl.a. kan have lært om i de fællesskaber, vedkommende er en del af, jf. Differential association (Akers, 2011[1994], s. 132; Akers & Jennings, 2019, s. 115). Derudover giver et multi-stage-attack et større udbytte, da de på denne måde kan anskaffe sig en større mængde af intimt materiale fra flere forskellige ofre og platforme. Dette peger altså på, at gerningspersonerne lærer specifik adfærd og handlinger gennem sociale sammenhænge, herunder hvilke fremgangsmåder der giver den største belønning, og hvordan de kan undgå eventuelle kapable vogtere (Akers & Jennings, 2019, s. 117).

5.1.3 Post-activity

Følgende afsnit omhandler stadiet Post-activity, som indebærer de nødvendige logistiske trin, gerningspersonen skal tage for at afslutte den kriminelle handling uberettiget adgang.

Sexting afsluttes helt logisk, når det intime forhold ophører. Den indbyrdes deling af de berettigede tilsendte billeder stopper, men modtageren vil dog stadig have materialet i sin varetægt, hvis ikke vedkommende sletter det. Skridtene i post-activity stadiet, i de spontane sager, forekommer derfor forholdsvis enkle. Der forekommer ingen logiske trin for at undgå at blive opdaget i sin handling, som Crime Script fordrer, da der som bekendt ikke er et kriminelt element til stede i sexting. Desuden forekommer sexting relativt impulsivt og spontant.

Ligeledes gør dette sig gældende i ufrivillig sexting i form af eksempelvis dickpics, på trods af det kriminelle element - netop fordi denne handling også forekommer spontant.

I forhold til den planlagte form for uberettiget adgang er et vellykket Social Engineering angreb, når gerningsperson uden at vække opsigt får anskaffet uberettiget adgang til offerets materiale. For at afslutte handlingen skal gerningspersonen lave et *clear exit*, så der ikke efterlades beviser, som kan føres tilbage til vedkommendes identitet (Chinta, Alaparthi & Kodali, 2016, s. 226). Hvis offeret dog har aktiveret et sikkerhedssystem, hvor de bliver notificeret omkring mistænkeligt login fra en anden enhed, vil dette i princippet stoppe gerningspersonen i den kriminelle handling. Vedkommende kan derfor blive opdaget i forsøget på at logge ind på offerets konti. Christoffer Herlufsen nævner i ekspertinterviewet: *"[...] så mit indtryk er ikke, at det er IT-delen, at de her ting bliver opdaget. Så skulle det være fordi, at platformen gør opmærksom på, at der bliver logget ind et eller andet sted, og man så opdager det"* (Bilag 7, l. 368-372)

og

"Der er nogle tilfælde, hvor personen måske kan lægge mærke til, at nogen prøver at skifte deres passwords, hvor man får de her e-mails osv., med at der er blevet prøvet at logge ind, men det er ofte i tilfælde, hvor det ikke er lykkedes" (Bilag 7, l. 340-344).

Såfremt gerningspersonen alligevel lykkes med at logge uopdaget ind på offerets e-mail, sociale medier mm., kan vedkommende i princippet fortsætte med at anskaffe intimt materiale. Planlagt uberettiget adgang afsluttes derfor nødvendigvis ikke, især ikke i de tilfælde, hvor målet er at udføre et multi-stage-attack. Gerningspersonen kan blive ved med at anskaffe intimt materiale, så længe vedkommende ikke bliver opdaget i sit foretagende. Christoffer Herlufsen forklarer ud fra sin faglige ekspertise:

"Ja, altså generelt hvis vi snakker folk, der er dygtige til at lave Social Engineering, så hvis de er gode nok jo, så er det jo, at man ikke opdager det før, at materialet er ude, eller at skaden er sket på en eller anden måde" (Bilag 7, l. 334-337).

Ovenstående citat tydeliggør således, at hvis gerningspersonen er dygtig nok til at begå Social Engineering-angreb, heriblandt forberedt sig tilstrækkeligt, vil disse angreb ikke opdages før, at det opnåede intime materiale eksempelvis er blevet videredelt til andre personer, såkaldte

barmhjertige samaritanere, som vælger at berette om hændelsen til det pågældende offer (Bilag 8, l. 394-399).

Opsummering af Post-activity

Opsummeret omhandler Post-activity stadiet i de spontane sager, at sexting ofte ophører, hvis det intime forhold stopper. Fundet i indeværende stadie er derfor, at der foregår mere simple afslutninger. Når det intime forhold ophører, vil der således opstå en forventning om, at fremtidig sexting ikke vil blive modtaget med positiv respons længere. Hvis en af parterne således fortsætter med at sende billeder, eksempelvis i form af ufrivillige dickpics, jf. ufrivillig sexting, vil vedkommende blive mødt med uønskede reaktioner, hvilket således vil agere som en form for negative reinforcement (Mandau, 2019, s. 80; Akers, 2011[1994], s. 133-134; Akers & Jennings, 2019, s. 117).

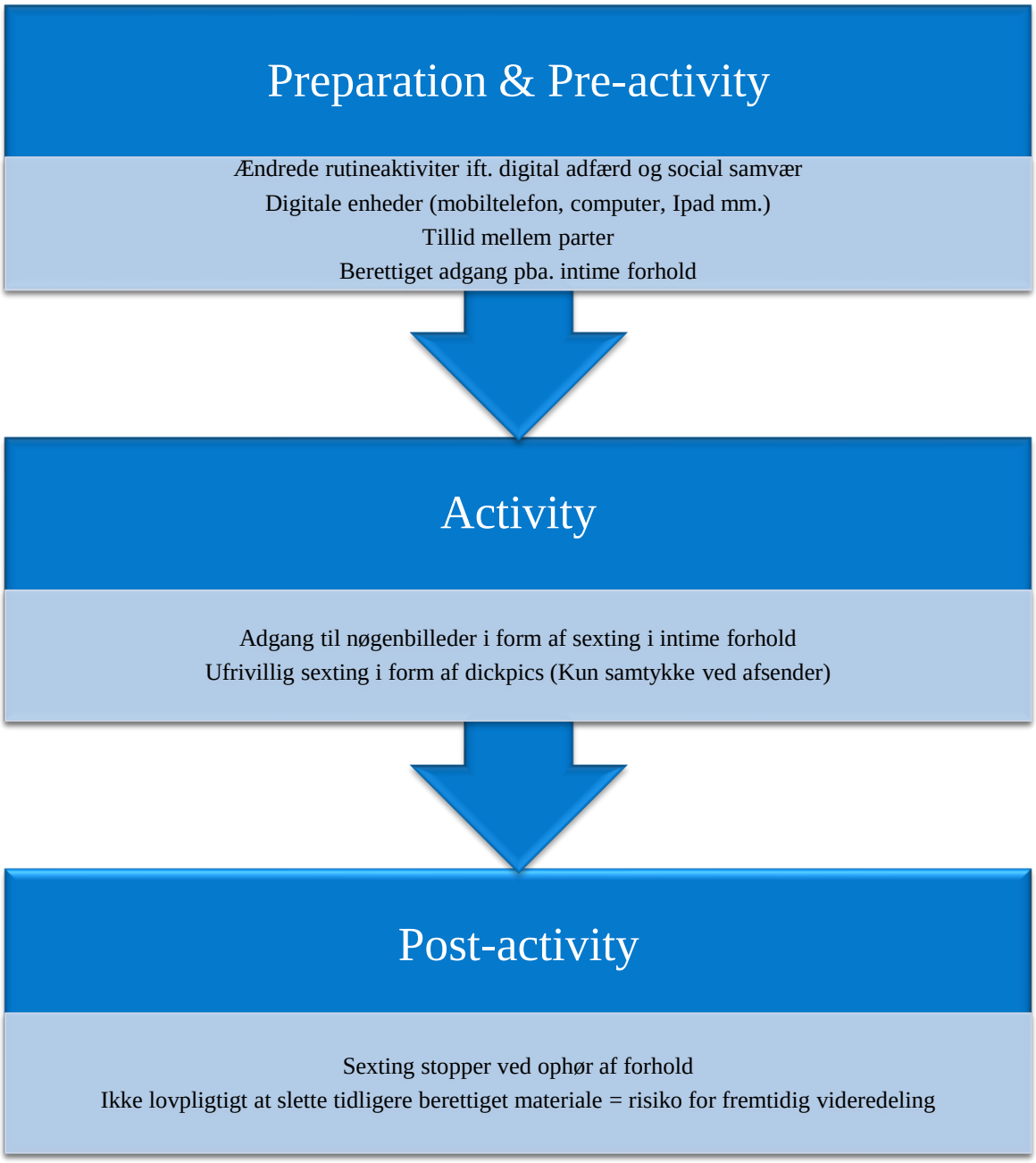
I de planlagte sager vil en logisk og foretrukket afslutning være, når gerningspersonen formår at lave et clear-exit uden at efterlade beviser omkring vedkommendes identitet eller tilstedeværelse på den pågældende digital platform. På baggrund af manglende kapable vogtere har den uberettigede adgang kunne finde sted, samtidig med at clear-exit netop kan forekomme. Derudover, som opsummeret i afsnittet omhandlende Preparation og Pre-activity, har den motiverede gerningsperson opnået viden omkring, hvordan vedkommende bedst mulig forbereder sig på at opnå og ikke mindst udføre den uberettigede adgang jf. Akers begreber omhandlende Imitation og Differential Association.

Gennem offentligt tilgængeligt materiale, såsom offentlige sager i medierne eller en manual for udførelsen af Social Engineering, vil vedkommende dermed kunne navigere i, hvordan clear-exit opnås. Scriptet, vi i indeværende analyse har præsenteret omhandlende planlagt uberettiget adgang, stemmer ligeledes overens med mønsteret, der præsenteres i eksisterende litteratur jf. afsnit 2.2.1 omhandlende Social Engineering. Her viser litteraturen som bekendt, at der indgår fire faser i et Social Engineering-angreb: 1. Indsamling af oplysninger om målet, 2. Udvikling af et forhold til målet, 3. Udnytte den tilgængelige information og herefter udføre selve angrebet, og 4. Forlade uden nogle spor (Salahdine & Kaabouch, 2019, s. 2; Chantler & Broadhurst, 2008, s. 4-5).

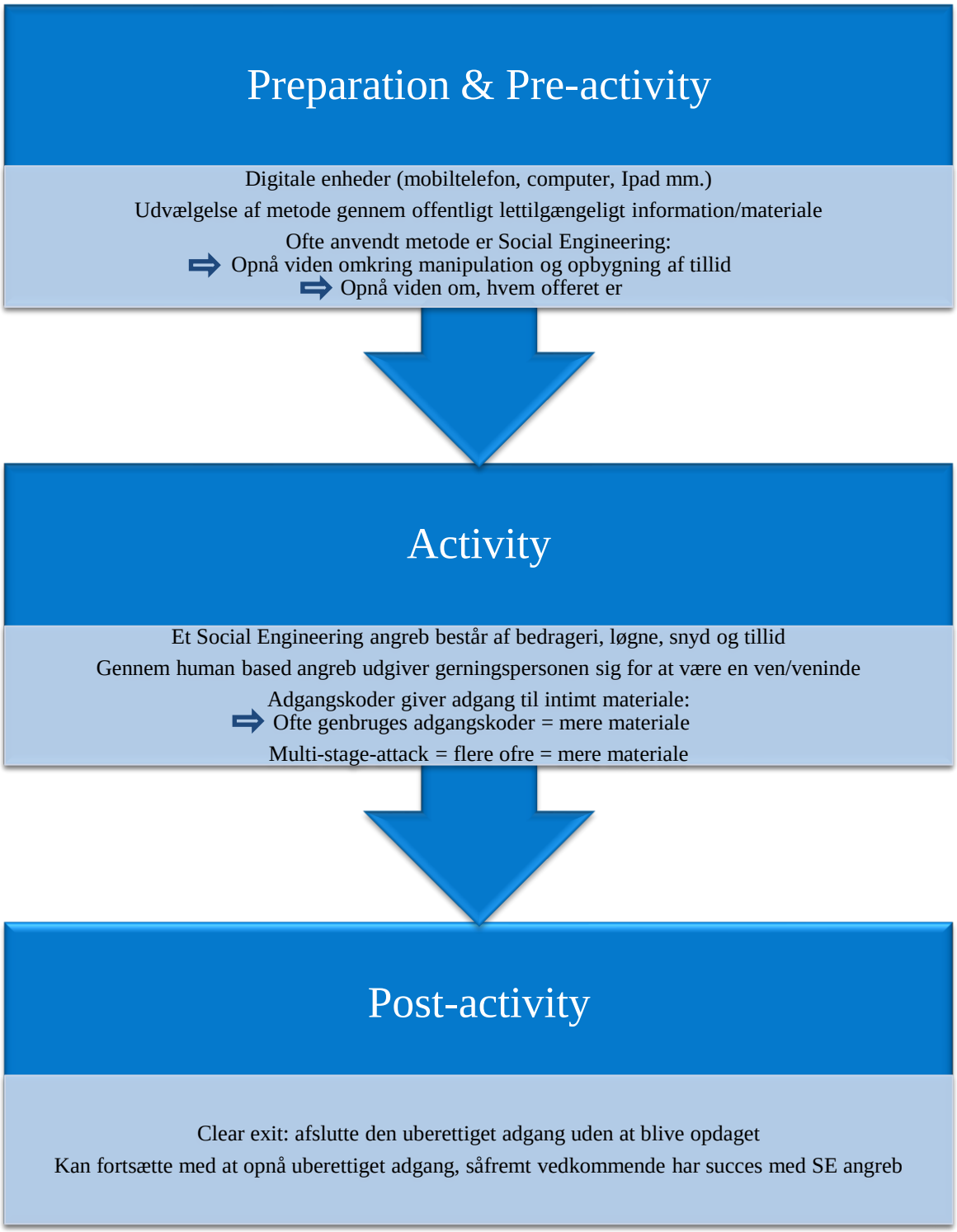
I nedenstående figurer er således en visualisering af de præsenterede Crime Script stadier. Disse er således fundene i ovenstående delanalyse 5.1. Eftersom der er en tydelig forskel mellem den

spontane og planlagte udgave af uberettiget adgang, forekommer der ligeledes en distinktion mellem disse, hvorfor der fremstår en Figur 4 (Spontan) og en Figur 5 (Planlagt).

Figur 4: Crime Script af *spontan* uberettiget adgang til intimt materiale



Figur 5: Crime Script af *planlagt* uberettiget adgang til intimt materiale



5.2 Ulovlig billeddeling

Anden delanalyse omhandler kriminalitetsformen ulovlig billeddeling. Gerningspersonen har således intimt materiale i sin varetægt, som vedkommende ønsker at videredele ulovligt til andre motiverede gerningspersoner. Afsnittet belyser derfor de skridt, der indgår før, under og efter den ulovlige billeddeling.

5.2.1 Preparation & Pre-activity

Stadierne Preparation og Pre-activity vil i følgende underafsnit præsenteres ift. ulovlig billeddeling. Der er som bekendt tale om de overvejelser, handlinger og beslutninger, der er nødvendige for at kunne udføre den kriminelle handling.

Der hersker en fælles konsensus hos flere af eksperterne om, at især unge mennesker ikke er klar over, at billeddeling er ulovligt (Bilag 6, l. 351-353; Bilag 7, l. 264-267; Bilag 9, l. 322-328, 341-345). I disse tilfælde er det således ikke relevant for gerningspersonen at overveje handlingen på forhånd. Lene Wacher Lentz udtaler eksempelvis, at det er relativt nemt at dele et billede, og at det ikke kræver særlige kompetencer eller planlægning for at lykkes, da det er en relativ simpel handling: *"Jeg tror, der er noget omkring den her digitale kriminalitet som simpelthen er for nemt, på en eller anden måde […] det er jo egentlig bare at klikke"* (Bilag 9, l. 320-322). Denne spontanitet understøttes yderligere af de andre eksperter i specialets empiri (Bilag 5, l. 201; Bilag 6, l. 496-511, 314-315; Bilag 7, l. 263-267, 276-279). Delingen kræver dog en basal viden omkring, hvorledes dette rent faktisk gøres. Nutidens unge mennesker er eksempelvis vokset op med sociale medier, hvorfor denne viden og erfaring anses som gældende for langt de fleste unge (Bilag 7, l. 620-621; Holst, 2018, s. 155). Vi vurderer derfor, at forberedelsen forekommer mere simpel i de tilfælde, hvor materialet bliver delt spontant.

Modsat spontan ulovlig billeddeling består den planlagte form af en mere udførlig forberedelsesproces. Det første egentlige skridt er som bekendt, at gerningspersonen har opnået uberettiget adgang til intimt materiale, som vedkommende har i sinde at videredele ulovligt. Herefter foretages en vurdering af, hvilke remedier der skal til for at videredele, og om der er nogle specifikke omstændigheder, som der skal tages forbehold for (Bilag 7, l. 283-288). Det kræver eksempelvis ikke en specifik fysisk lokation at kunne videredele intimt materiale. Med teknologiens udvikling kan det gøres både i hjemmet, på skoler, offentlige steder mm., så længe

vedkommende har internetforbindelse, samt eksempelvis en mobil eller computer. Der findes derfor ikke længere fysiske begrænsninger for gerningspersonen (Bilag 5, l. 259-266, 824-827; Bilag 6, l. 157-158).

Gerningspersonen opnår viden om de specifikke online fora, som der typisk deles materiale på, gennem bekendte eller ved at søge sig frem til det via enten mørkenettet eller det almene internet (*clear net*) (Bilag 5, l. 291; Martin, Cunliffe & Munksgaard, 2019, s. 13). Hvis ikke gerningspersonen kender til Tor (The Onion Router) og VPN (Virtual Private Network) inden da, er det formentlig i denne søgningsproces, at vedkommende støder på dem. Morten Rasmussen peger bl.a. på, at dette er nogle af de typiske teknikker, der benyttes i de planlagte sager omhandlende ulovlig billeddeling (Bilag 6, l. 316-318). Mørkenettet kan nemlig ikke tilgås lige så simpelt som almene hjemmesider, hvorfor der er behov for specialiseret software. Vi afgrænser således mørkenettet til hjemmesider *hostet* på Tor (Martin et al., 2019, s. 13). Dog er det væsentligt at pointere, at ikke alt materiale på mørkenettet er ulovligt (Martin et al., 2019, s. 14), hvorfor det at begå sig på herpå i sig selv ikke anses som værende ulovligt. Eftersom indeværende delanalyse omhandler ulovlig billeddeling, er det således de kriminelle aktiviteter, der er i fokus, når mørkenettet omtales.

Tor er et populært privatlivs- og anonymitetsnetværk, der er gratis og nemt at downloade (Cole, Latif & Chowdhury, 2021, s. 3; Martin et al., 2019, s. 13). Lene Wacher Lentz beskriver følgende: *"Altså det skulle være ganske let at gå på Tor netværk, og det er også meget nemt at skjule IP-adressen, man kommunikerer fra"* (Bilag 9, l. 289-290). Det er sværere at spore de kriminelle aktiviteter på en Tor browser ift. det almene internet. Dette skyldes netop den anonymitet, som Tor fordrer (Cole et al., 2021, s. 4). Morten Rasmussen påtaler i relation til dette, hvordan nogle gerningspersoner anvender både VPN og Tor, når de ulovligt deler intimt materiale (Bilag 6, l. 315-318, 413-420). Et VPN-netværk muliggør, at brugeren kan ændre sin originale IP-adresse til at være en anden lokation og herved skjule sin virtuelle placering (Sardá, Natale, Sotirakopoulos & Monaghan, 2019, s. 559). Ved at forbinde VPN med Tor, kan det således styrke gerningspersonens online sikkerhed (Cole et al., 2021, s. 3). Selvom disse netværk er en del af gerningspersonens overvejelser og forberedelser, dvs. Preparation og Pre-activity stadiet, er det værktøjer som vedkommende bruger under hele hændelsesforløbet omkring ulovlig billeddeling.

Når sikkerheden og anonymiteten er på plads for gerningspersonen, er det nødvendigt at spore sig ind på de pågældende regler og formål, der gør sig gældende på den specifikke virtuelle platform, som gerningspersonen vil dele det intime materiale på (Otteren & Gynnild, 2021, s. 7). Hvis gerningspersonen ønsker at få adgang til et online fællesskab, kræver det til tider, at vedkommende viser sit værd ved at dele sine stjålne billeder på forhånd:

"Der er nogle af de her sager, de mere organiseret sager, hvor at der bliver oprettet et forum eller en hjemmeside, hvor der bliver delt masser af billeder og videoer, og der kan man sige, at der ligesom er flere aktører inde over, og der er også nogle sider, hvor folk ligesom selv sender billeder ind til for at få adgang til billeder selv osv." (Bilag 7, l. 166-172).

Hvis den motiverede gerningsperson således bliver godkendt på det sociale forum, kan vedkommende interagere med andre motiverede gerningspersoner, som har samme mål og interesser. Ved at engagere sig i netværket, er det desuden muligt at opnå adgang til andre fora og andet ulovligt billedmateriale: *"Building a quality network helps a user to gain access to other networks with more exclusive images, granting access to more exclusive forums, websites, and conversations that are password protected"* (Otteren & Gynnild, 2021, s. 7). De kan derfor indbyrdes inspirere hinanden til, hvordan delingen af intimt materiale kan udføres bedst muligt og på hvilke platforme. Der er dog ikke en fælles konsensus omkring, hvilket materiale der skaber mest værdi, da dette afhænger af den pågældende gerningspersons præferencer. Hilde Otteren & Astrid Gynnild beskriver eksempelvis, hvordan indhentet materiale i flere år og fra forskellige lande anses som værende dét, der skaber værdi, hvor to af eksperterne i indeværende speciale i stedet peger på, at det er materiale af ny karakter, der skaber høj status i det kriminelle miljø (Bilag 6, l. 180-183, 562-568; Bilag 7, l. 422-428).

Udover anvendelsen af Tor-netværket og VPN-tjenester er det ligeledes favorabelt for gerningspersonen at udforme et falsk navn på den virtuelle platform. Dette kan både være på mørkenettet, men kan ligeså vel være på sociale medier såsom Facebook eller Snapchat. Ved at fokusere på disse sikkerhedsforanstaltninger, kan gerningspersonen minimere opdagelsesrisikoen yderligere:

"I de højprofilerede sager, bliver der taget nogle sikkerhedsforanstaltninger og brugt falske navne og sådan noget, hvis der bliver delt noget på Snapchat grupper, der bliver brugt en lille smule i hvert fald ja, men det kommer an på, hvilken type sag det er, og hvor organiseret det er [...]" (Bilag 7, l. 279-284).

Gerningspersonen skal derudover kalkulere, hvilken risiko der kan være forbundet med den ulovlige billeddeling. Denne risikokalkulering påpeger Otteren og Gynnild ligeledes i deres studie af anonyme brugere på et stort online forum. Her skal brugerne bl.a. informere andre om de mulige konsekvenser, som aktiviteterne kan medføre (Otteren & Gynnild, 2021, s. 13). Denne modus er meget lig det, der foregår ved CSAM[6] (Child Sexual Abuse Material). Der anvendes ligeledes ofte Tor i forbindelse med CSAM, da det som bekendt mindsker risikoen for, at den kriminelle online adfærd bliver opdaget (Leclerc, Drew, Holt, Cale & Singh, 2021, s. 3). På denne måde kan der med minimal risiko blive produceret og distribueret materiale til et større antal af motiverede gerningspersoner, hvor de kan få adgang til flere forskellige børn (Leclerc et al., 2021, s. 2-3). Dette store antal af ofre pointerer Morten Rasmussen ligeledes i ekspertinterviewet: *"[...] de her mennesker ligger jo sjældent inde med under 2000 billeder, og det er jo meget tit af forskellige børn, så der er utrolig mange ofre i sagerne"* (Bilag 6, l. 221-223). Det lader til, at der ligeledes er et sammenfald i modus omkring "samlere" online, omend det er intimt materiale generelt eller CSAM. Leclerc et al. nævner yderligere under det de kalder *The crime set-up phase,* at for at CSAM-gerningspersoner kan begå sig på mørkenettet, kræver det adgang til internettet og evnen til overhovedet at kunne navigere på det almene internet. Ligesom hos ulovlig billeddeling af intimt materiale generelt, er det nemlig sjældent, at gerningspersoner tilgår mørkenettet uden først at navigere på det almene internet (Leclerc et al., 2021, s. 6). Det er igennem søgningen af CSAM-materiale, at de sporer sig ind på eksistensen af mørkenettet, og hvordan de således kan få adgang hertil (Leclerc et al., 2021, s. 7). Det er ofte i denne proces, at de ligeledes opnår viden omkring Tor-netværket (Bilag 6, l. 305-308).

Opsummering af Preparation & Pre-activity

En fælles forståelse hos eksperterne i indeværende speciale er, at den ulovlige billeddeling i de spontane sager ofte sker på baggrund af, at de unge ikke er klar over det ulovlige element i handlingen. I disse tilfælde er der således ikke tale om en motiveret gerningsperson (Cohen & Felson, 2013, s. 469-470). Dette betyder også, at der i disse spontane forekommer simple eller begrænsede forberedelser samt overvejelser inden, det pågældende materiale deles. Det kræver dog en grundlæggende viden omkring, hvordan internettet og de sociale medier fungerer. Dette vokser børn i høj grad op med qua digitale ændringer. Denne øgede digitalisering fordrer, at de

[6] Term anvendt til at beskrive børneporno, også omtalt *child exploitation material* (Leclerc, Drew, Holt, Cale & Singh, 2021, s. 1).

fra en tidlig alder er vant til teknologier såsom mobiltelefoner, iPads og computere, hvorfor internettet og sociale medier i høj grad er en del af deres dagligdag både i hjemmet og i skolen. Dette er med til at opretholde bestemte rutiner, mønstre og adfærd (Cohen & Felson, 2013, s. 469-470), såsom en tilfældig videresendelse af billeder eller videoer. Denne adfærd bibeholdes ydermere, hvis vedkommende mødes med positive reinforcement såsom anerkendelse og accept omkring billeddelingen fra vennegruppen (Akers, 2011[1994], s. 133-134; Akers & Jennings, 2019, s. 117). Vedkommende vil således imitere handlingen omkring deling af intimt materiale, hvis dette belønnes med status og anerkendelse fra andre. Dette på trods af at vedkommende måske ved, at billeddelingen er ulovligt Denne kløft imødekommes vha. neutraliseringsteknikker (Akers & Jennings, 2019, s. 116; Akers, 2011[1994], s. 132-133). Et eksempel på en neutraliseringsteknik, der i denne sammenhæng kunne benyttes, er *Benægtelse af ansvar*, hvor gerningspersonen ikke tager ansvar for den ulovlige billeddeling, vedkommende har foretaget. Her kunne vedkommende eksempelvis benægte ansvaret med sin unge alder som begrundelse (Sykes & Matza, 2013, s. 225). Som argumenteret for i opsummeringen i afsnit 5.1.1 er det relativt almindeligt at have intimt materiale, qua sexting, liggende i mapper på sin mobiltelefon. Disse forandrede rutineaktiviteter fordrer derfor, at det tilgængelige materiale i højere grad kan tilgås og videresendes når som helst, hvilket ifølge Straffeloven § 264 d er ulovligt. Dette faktum fordrer ligeledes risikoen for, at denne form for kriminalitet øges.

Det er informativt, at de online fora i den planlagte deling af billeder er så centrale for, hvorvidt og hvordan vedkommende begår kriminalitet. Dette peger på, at forbrydelsen til en vis grad er afhængig af sociale relationer. Ifølge den inddragede primære- og sekundære litteratur, er det specifikt her, at de motiverede gerningspersoner lærer om anonymisering og teknologi, heriblandt Tor og VPN. Ligeledes kan statussen i disse fora føre til, at den pågældende gerningsperson blot bliver mere motiveret for at opnå det værdifulde mål (Felson & Clarke, 1998, s. 4-5), hvorfor gerningspersonen ønsker at lære mere om, hvordan dette bedst muligt sker. Forberedelsesfasen hos den planlagte form for ulovlig billeddeling involverer derfor en del læringsprocesser, heriblandt indhentning af information, læring af teknikker samt en forståelse af de socialt gældende normer og værdier på de pågældende online fora. Dette har lighed til den samme modus, som findes hos CSAM. Hertil kan der opnås store mængder af materiale gennem online netværk, hvilket fordres gennem anonymiteten, som Tor og VPN muliggør. Denne kriminalitetsform hører således under Walls typologi Cyber porn and

obscenity. Yderligere i forberedelsen til ulovlig billeddeling gør det sig gældende, jf. specialets Crime Script-tilgang, at jo oftere og mere ferm den motiverede gerningsperson er blevet i denne kriminalitetsform, desto mindre forberedelse og færre spekulationer kræver det fremadrettet, grundet lagringen af manuskripterne i gerningspersonens hukommelse (Haelterman, 2016b, s. 8). Helt konkret gør det sig altså gældende, at hvis den motiverede gerningsperson allerede kender til specifikke fora og teknikker, som kan bidrage til denne ulovlige billeddeling, og vedkommende derudover har succes hermed, vil det være naturligt at benytte samme metode fremover. Det kræver derfor ikke lige så stor forberedelse efter første gang (Akers, 2011[1994], s. 133-134; Akers & Jennings, 2019, s. 117).

5.2.2 Activity

Næste stadie der præsenteres, er Activity. Det er herunder den kriminelle handling, ulovlig billeddeling, udspiller sig online.

I de spontane sager påpeger flere eksperter nemlig, at delingen udføres i form af hævnporno, hvilket ikke er tilfældet hos de planlagte sager (Bilag 5, l. 441-447; Bilag 6, l. 207-217, 546-554). Hævnporno er blevet et udbredt fænomen i relation til ulovlig billeddeling (Holst, 2018, s. 155). Dette involverer ofte en ekskæreste, der deler eller uploader intime billeder af sin forhenværende partner, som vedkommende har fået adgang til gennem eksempelvis tidligere sexting (Bates, 2017 s. 24). Der sker derfor et brud på tilliden mellem de respektive parter, som der oprindeligt forekom i forbindelse med sexting jf. afsnit 5.1.2. Hævnporno kan således være en konsekvens af netop sexting, når der således opstår uvenskab og dermed et ønske om hævn, hvilket Morten Rasmussen beskriver under ekspertinterviewet:

> *"[...] fordi i fredstid der er der jo aldrig nogen, der har problemer. Altså hvis jeg tager nøgenbilleder af min kæreste, mens vi er kærester, jamen så er det fint, fordi så lægger det på min telefon, og så kan det være, at hun er mig utro, og jeg kommer til at hade hende ad helvede til [...]"* (Bilag 6, l. 848-852).

Yderligere opsætter han et helt konkret eksempel på, hvordan de enkelte skridt kan forekomme omkring hævnporno: *"Mand møder kvinde, og det kunne være hyggeligt, at vi tager nogle billeder af det, ik'? Og så bliver de uvenner, og så finder den så vej til alle mulige lyssky sider, hvor man kan hente det"* (Bilag 6, l. 214-217). Det første skridt er således sexting eller fysisk at tage nogle intime billeder sammen, hvor der er en generel enighed og samtykke til stede fra

begge parter. Næst er selve dét at gå fra hinanden, hvor der er nogle negative følelser på spil. Sidst sker så selve delingen af de intime billeder, qua Activity, hvilket i dette tilfælde sker i form af hævnporno.

En generel problematik der knytter sig til fænomenet hævnporno, belyser Lene Wacher Lentz i ekspertinterviewet. Hun påpeger, at den danske Straffelov ikke omfatter, at vedkommende, der har modtaget materialet med samtykke, er nødsaget til at slette det pågældende materiale, hvis ophavsmanden beder om det:

"Jeg bliver opmærksom på den her situation, at hvis man er kærester, og man har udvekslet nøgenbilleder, så har vi faktisk ikke et eller andet, at det skal tilbageleveres, ellers så er det strafbart. Altså det kan man jo beholde for så vidt. Man skal bare ikke videregive det [...] Det er i hvert fald sådan et område, der kommer bag på folk, at man ikke sådan kan straffe folk, hvis de ikke vil skille sig af med billederne" (Bilag 9, l. 153-163).

Som det fremgår i ovenstående citat, er det således ikke ulovligt at beholde materialet, uanset den anden parts vilje hertil, så længe materialet er opnået med berettiget adgang i første omgang. Det er således først, hvis vedkommende deler materialet, eksempelvis for at få hævn, at der er tale om en egentlig kriminel handling.

Som tidligere nævnt i indeværende speciale er udviklingen af digitale medier og teknologi generelt eksploderet. En undersøgelse fra Red Barnet peger ligeledes på, at denne udvikling af anvendelsen af den digitale verden samtidig skaber en konstant fornyelse af digitale medier, heriblandt Apps til smartphones, som der er rig mulighed for at benytte. Stigningen i antal muligheder for at skabe relationer og kommunikere på kryds og tværs øger unægteligt også risikoen for netop at opleve digitale krænkelser (Rambøll, 2021, s. 4). Christoffer Herlufsen påpeger ligeledes denne online udvikling:

Christoffer Herlufsen påpeger ligeledes denne online udvikling:

"Man kan måske sige, at vores generation var nogen af de første, der blev mødt af denne her IT-verden og begyndte at bruge smartphones, hvor at de unge der går i skole og allerede har smartphones fra 3. klasse eller før det, der er det hele jo nyt" (Bilag 7, l. 617-621).

Ovenstående citat beskriver således samme pointe som hos Red Barnet, ift. at denne nye digitaliserede verden fylder mere i børn og unges liv. De digitale sexkrænkelser er derfor også i vækst, da folk hyppigere deler de let tilgængelige billeder spontant. Når hævnporno således

udspiller sig og det intime materiale er blevet delt med den første person i rækken, bliver det herfra ofte videresendt til endnu flere personer. Christoffer Herlufsen giver følgende eksempel:

"[...] der er en ung dreng, der har nogle billeder af sin ekskæreste eller nuværende kæreste, og han deler det med en af hans venner, og den person giver det videre til nogle andre, og så bliver det sendt til nogen på Snapchat eller en Snapchatgruppe et eller andet, og så er der en fjerde person, der tager nogle screenshots af det, og så lige pludselig florerer billedet over det hele, og man kan sige, at alle dem der har sendt billedet videre, er in on it, og en del af det, så det er noget der hurtigt kan sprede sig, og mange der er inde over. Oftest er det ikke fordi, at ham der starter med at dele billedet, har til formål at sprede det ud til 100 mennesker. Ofte vil han eller hende bare sende det til en eller anden, men så fordi det er spændende at se et nøgenbillede af en, man kender, så sender den person det videre, og så kører hele kæden ikk'?" (Bilag 7, l. 182-195).

Morten Rasmussen italesætter ligeledes denne eksplosive spredning:

"[...] men der var der også for eksempel Umbrella-sagen. Det var jo nogen, der havde optaget det her, og så bliver det jo bare eksplosivt delt, fordi[...] Jeg ved ikke, om I har set der findes en video af, hvordan det spreder sig over tid" (Bilag 6, l. 123-127).

Selv hvis det ikke var meningen, at billedet skulle nå ud til så mange, er det dog typisk det, der sker. Som præsenteret i specialets problemfelt jf. kapitel 2, ses der generelt en stigning i digitale sexkrænkelser, hvilket bl.a. kan forklares ud fra disse eksplorative spontane delinger. I ekspertinterviewet med Sidsel Harder beskriver hun dog, hvordan det kun er én ud af hver femte danske unge, som rent faktisk videredeler billedet. Problemet ifølge hende er i stedet, at den femte unge kan formå at dele materialet videre til 20 andre, hvorfor den spontane billeddeling alligevel formår at eksplodere (Bilag 8, l. 134-143). Ikke desto mindre kan denne eksplosive deling ligeledes kan have den konsekvens, at det intime materiale også ender på mørkenettet, hvor motiverede gerningspersoner dermed også opnår uberettiget adgang hertil.

Ift. den planlagte form for ulovlig billeddeling, giver tre af eksperterne, Flemming Kjærside, Morten Rasmussen og Lene Wacher Lentz, udtryk for, at delingen ofte foregår på bestemte servere i udlandet (Bilag 5, l. 278-284; Bilag 6, l. 326-329, 366-371; Bilag 9, l. 248-252). Flemming Kjærside udtaler eksempelvis:

"Der er rigtig mange tjenester, der tilbyder det her, hvor politiet ikke kan få oplysninger, når vi kommer og beder om det, ikke? Mange lægger det på en eller anden server[...] Jeg ved ikke lige, hvad det er for nogle navne. Der ligger nogle i New Zealand, der ligger nogle i Rusland, sådan nogle billedservere, hvor man kan have tingene liggende og kan dele links med hinanden" (Bilag 5, l. 278-284).

Når gerningspersonen agerer via specifikke udenlandske servere, kan vedkommende sløre sin identitet og sit danske tilhørsforhold (Lentz, 2019, s. 15). Dette kan skabe udfordringer i relation til retshåndhævelse (Cole et al., 2021, s. 5). Europol og Eurojust har i en rapport fra 2019 fremlagt, at det ikke er muligt at etablere gerningspersonens fysiske lokation, når vedkommende bl.a. anvender mørkenettet og diverse anonymiseringsteknikker (Tor og VPN). Manglende online lokalitet og data der bliver opbevaret på forskellige servere, gør det derfor uklart, hvilket lands jurisdiktion der gør sig gældende (Eurojust & Europol, 2019, s. 13). De kriminelle udnytter således dette faktum, så de kan undgå at blive opdaget og retsforfulgt på baggrund af den ulovlige billeddeling (Eurojust & Europol, 2019, s. 18).

Derudover findes der Bulletproof hosting services (BPHS). Overordnet set er dette hardware-, software eller applikationsbaseret faciliteter, der kan lagre enhver type af indhold (Goncharov, 2015, s. 3-4). Denne type af *hosting* afviger derfor fra konventionelt internet, da udbyderen ikke lukker brugernes aktiviteterne ned, desuagtet om det er uetisk eller kriminelt (Lusthaus, 2013, s. 57-58). Sådanne Bulletproof hosting services er derfor særligt attraktive for IT-kriminelle (Lusthaus, 2013, s. 58). Måden det kan fungere på i praksis er, at nogen har et forum hostet på en BPHS, hvor kriminelle kan uploade illegalt materiale, såsom intime billeder, med mindre risiko for at blive opdaget (Goncharov, 2015, s. 3). Der sælges derfor en form for beskyttelse, når BPHS-udbydere tilbyder et opbevaringssted for kriminelle, der ikke i ligeså høj grad bliver lukket ned af autoriteter (Lusthaus, 2013, s. 58).

Som nævnt i afsnit 5.2.1 Preparation & Pre-activity stadiet, er nogle gerningspersoner ofte samlere, i form af opbevaring af store mapper med intime billeder af flere forskellige ofre. Dette kan opbevares forskelligt. Nogle bruger de online platforme på mørkenettet eller BPHS, men materialet kan ligeså vel også være på gerningspersonens egen computer. Sidstnævnte er dog mere risikabelt, såfremt autoriteter får adgang til gerningspersonens ejendele.

Morten Rasmussens udtaler, hvordan samlingen af flere billeder kan forekomme:

"Så er der dem, altså de der samlere. Det er jo også i virkeligheden[...] Dem ser man jo. Altså de vil jo helst samle til huse og have så stor en samling som muligt, men de ved også godt: "Jamen det kræver så også, at jeg bytter noget. Altså noget for noget, hvis jeg skal have den største samling i Europa, så bliver jeg også nødt til at give noget ud af min samling"
(Bilag 6, l. 512-517).

I citatet fortæller han desuden, at gerningspersonerne ofte indgår i fællesskaber for at øge sin samling af intimt materiale. Sekundær litteratur beskriver ligeledes en tendens til, at der på disse fora opstår en socialisering mellem gerningspersonerne. De skaber således et fælles mål om at få adgang til og dele disse intime billeder på tværs og mellem hinanden. Der argumenteres således for, at dette fællesskab samt fælles mål for at opnå uberettiget adgang til et bredt spektrum af ofre gør, at gerningspersonerne hver især opnår hurtigere og bedre materiale (Otteren & Gynnild, 2021, s. 7).

Opsummering af Activity

Når der deles billeder spontant sker dette, ifølge specialets primære empiri, oftest i form af hævnporno. Efter endt forhold videredeler en af parterne således de billeder, vedkommende har modtaget med samtykke under sexting. Selve delingen er uberettiget, hvorfor der som bekendt er tale om en kriminel handling jf. Straffelovens § 264 d. En væsentlig pointe i henhold til specialets primære empiri er dog, at selve den eksplosive spredning af materialet ikke nødvendigvis er med forsæt. Internettet har været med til at ændre den måde, vi kommunikerer og lever på, så det nu er blevet muligt at interagere med andre uden overhovedet at forlade hjemmet. Som bekendt er det især nutidens unge, der er vokset op med disse ændrede rutineaktiviteter. De anser det derfor som værende almindeligt at videresende beskeder, billeder, videoer eller links til venner på daglig basis. Når alle således gør dette, kan intime billeder sprede sig hurtigt og til mange uden særlig megen omtanke. Det står således klart, at den motiverede gerningsperson først bliver en realitet i disse spontane sager, når et forhold eksempelvis er blevet afsluttet på dårlige termer. I disse sager bliver der dermed også et specifikt egnet mål; nemlig vedkommende som den motiverede gerningsperson vil hævne sig på.

Gerningspersoner, som har planlagt den ulovlige billeddeling, anvender ofte udenlandske servere eller BPHS for ikke at blive opdaget og fanget under den ulovlige billeddeling. Derudover dannes der ofte en form for samhørighed mellem de kriminelle på disse online fora. Vedkommende kan derfor gennem deling af teknikker og sikkerhedsforanstaltninger lære samt efterligne, hvordan distribueringen af intimt materiale kan foretages og yderligere fremmes (Akers, 2011[1994], s. 134; Akers & Jennings, 2019, s. 118). Når gerningspersonen konstant eksponeres for det intime materiale på mørkenettet og får en generel opfattelse af, at dette er en acceptabel handling, vil vedkommende på baggrund af Differential association få forstærket sine kriminelle tilbøjeligheder. Denne afvigende adfærd vil nogle endda rationalisere eller retfærdiggøre eksempelvis ved at påpege, at offeret selv er skyld i, at det bliver delt online jf. afsnit 2.3 omhandlende ulovlig billeddeling af intimt materiale. Her kan ligeledes trækkes tråde til Sykes og Matzas neutraliseringsteknikker. Ved at neutralisere den ulovlige billeddeling ved at skyde skylden på ofrene, er der således tale om *Benægtelse af offer* (Sykes & Matza, 2013, s. 226).

5.2.3 Post-activity

Følgende stadie omhandler Post-activity, dvs. selve afslutningen på ulovlig billeddeling ved både den spontane og planlagte form.

Ligesom ved uberettiget adgang har gerningspersonen i de spontane billeddelingssager formentlig ikke tænkt over, hvorvidt handlingen kan spores tilbage til vedkommende. Hvis det er delt over Facebook, er det for eksempel relativt nemt og hurtigt at finde frem til, hvem der er en del af billeddelingen, hvilket Morten Rasmussen pointerer:

"Eksempelvis Umbrella-sagen, det var jo nemt altså der[...] Lavede man en editionsbegæring til Facebook, og så fik man at vide, hvem brugerne var der delte det her, ik'? Og tit kunne man jo se det med det samme, fordi det lå jo på alle enhederne, og altså, det var jo den nemme efterforskning i forhold til det her, at man kunne se, hvem det var blevet delt med simpelthen, så det var ikke raketvidenskab og få dem dømt" (Bilag 6, l. 477-483).

Når der deles spontant, forekommer der ikke særlig mange overvejelser omkring digitale spor. Delingen foregår typisk gennem sociale medier, og i de tilfælde hvor vedkommende anvender sin egen profil, vil sandsynligheden for at blive opdaget blot øges.

Ift. den planlagte form for ulovlig billeddeling kan der igen trækkes på de forhold, som gør sig gældende hos CSAM. Gerningspersoner vil på et tidspunkt forlade mørkenettet, hvilket kan være af forskellige årsager. Ifølge Leclerc et al. vil nogle finde det vanskeligt at navigere på mørkenettet eller blot miste interessen i at interagere eller dele billeder med andre kriminelle (Leclerc et al., 2021, s. 8). Den ulovlige billeddeling hos den enkelte gerningsperson stopper i så fald på det gældende tidspunkt. Hvis vedkommende har anvendt en Tor browser, vil de kunne forlade de pågældende kriminelle fora med minimal risiko for at de andre brugere, eller politiet, vil kunne spore dem. Det er således i høj grad gerningspersonens grundige forberedelse jf. afsnit 5.2.1 Preparation & Pre-activity, som sikrer at de kan afslutte handlingen uden at blive fanget.

Når der er tale om gerningspersoner, som planlægger disse kriminalitetsformer inden for IT, og som har stor erfaring herfor, vil der således også være stor sandsynlighed for, at de kender til politiets efterforskningsmuligheder på området, som vi har redegjort for i afsnit 2.1.3. Denne information omkring typiske efterforskningsprocedurer er ligeledes viden, de kriminelle indbyrdes fortæller samt lærer hinanden om. Derudover er det let at finde frem til viden omkring dette på internettet gennem simple søgefunktioner. Herigennem kan de eksempelvis finde frem til, hvordan de udnytter de huller, der forekommer i Retsplejeloven. De kan bl.a. skjule deres online spor ved at benytte sig af udenlandske servere, jf. Activity-stadiet i afsnit 5.2.2, hvilket unægteligt besværliggør det senere efterforskningsarbejde. Flemming Kjærside forklarer i forlængelse heraf:

"Vores lovgivning, den rækker jo kun ned til grænsen, og så må vi se, om de kan finde lovgivning i det land, det handler om, og om vi kan få de oplysninger. Det gør det selvfølgelig endnu sværere, hvis det foregår på Darkweb, fordi der kan man jo skjule sig totalt ud" (Bilag 5, l. 623-628).

Fraværet af klare lovregler ift. efterforskning på internettet kan derfor med fordel benyttes af gerningspersonerne for at nå i mål med billeddelingen uden at blive opdaget. Dog fremgår det af ekspertinterviewet med Morten Rasmussen, at Retsplejeloven i praksis kan strækkes således, at myndighederne omvendt også kan imødekomme ovennævnte smuthuller, men det bestemt kan blive bedre ift. efterforskningen på internettet (Bilag 6, l. 688-722).

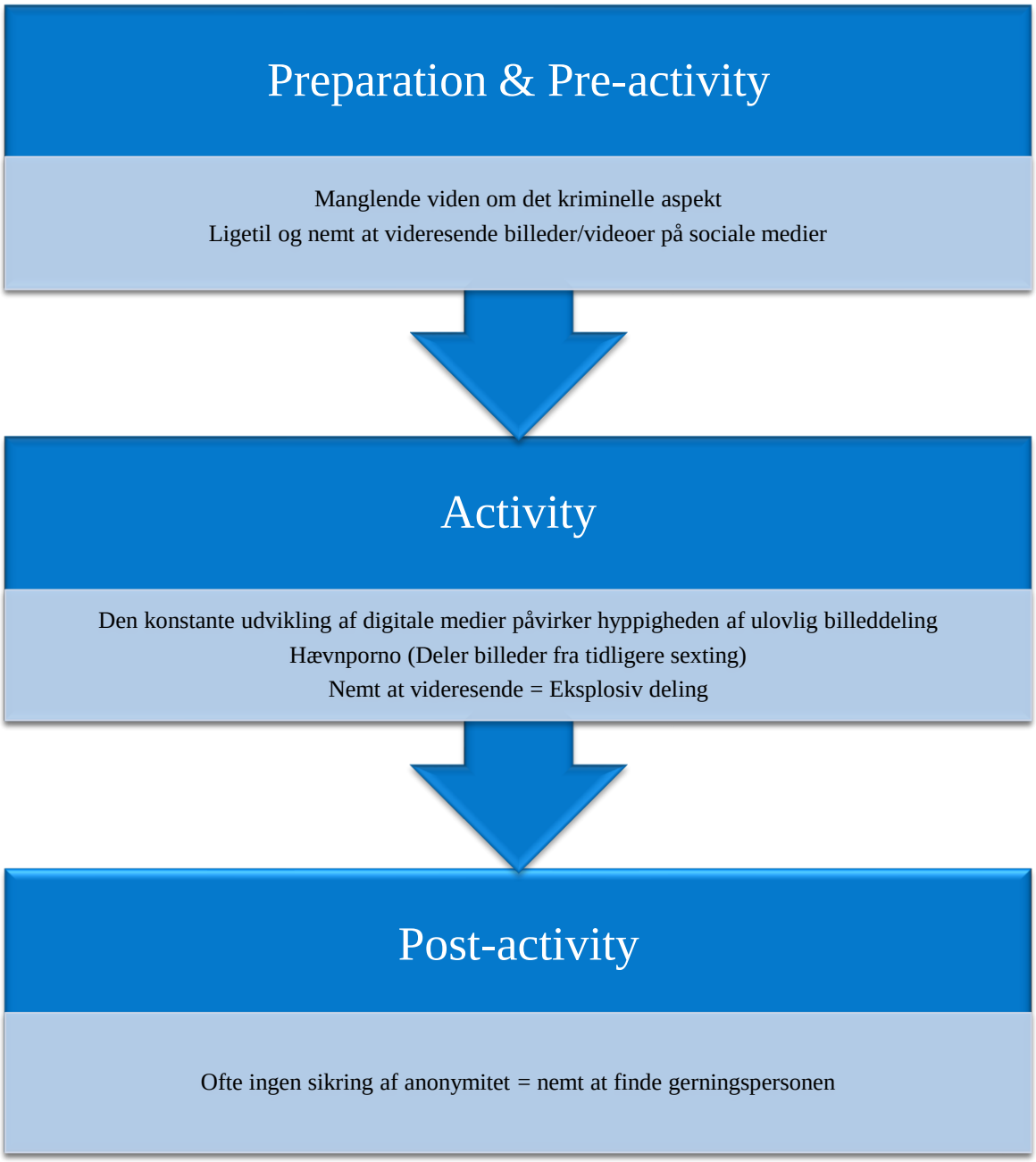
Opsummering af Post-activity

Efter den ulovlige billeddeling er udført, forekommer der forskellige måder hvorpå handlingen afsluttes. Dog gør det sig også i Post-activity fasen gældende, at de spontane former for ulovlig billeddeling ikke indebærer synderlige overvejelser omkring, hvordan vedkommende afslutter delingen. Det er desuden ikke svært at dele et tilfældigt billede med andre, hvorfor delingen sker relativt hurtigt og uden komplikationer. Hvis baggrunden for videredelingen kommer af et hævnmotiv, vil gerningspersonen typisk stoppe automatisk efter, at vedkommende har opnået sin hævn. Selvom den motiverede gerningsperson stopper med at videredele intimt materiale af eksempelvis sin ekskæreste, qua hævnporno, stopper delingen af materialet ikke nødvendigvis. Dette skyldes, som der tidligere er nævnt i indeværende analyse, at billedet ofte spreder sig eksplosivt.

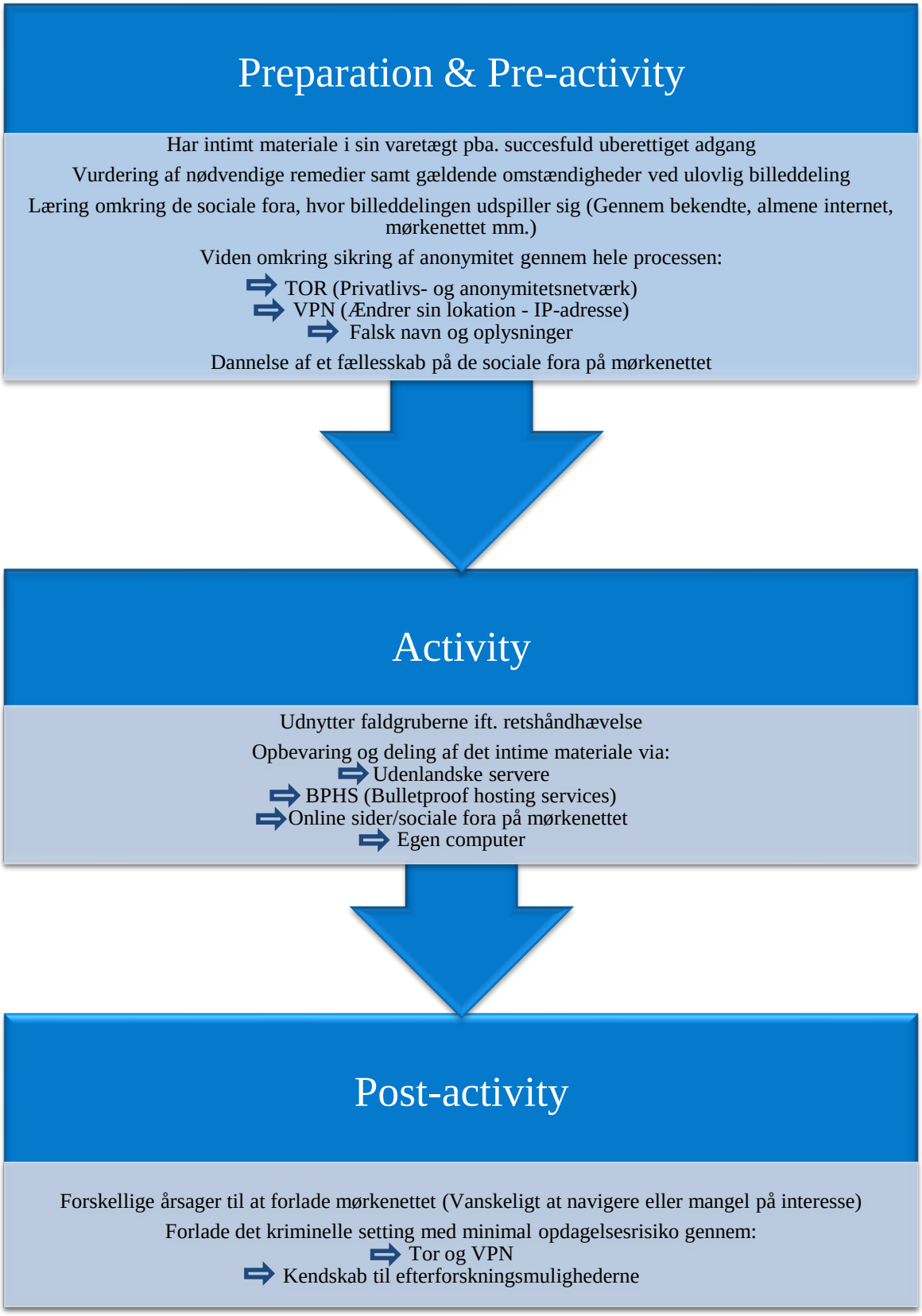
Ligesom i de andre stadier forekommer der i de planlagte tilfælde langt flere overvejelser omkring, hvordan den motiverede gerningsperson videredeler materiale online uden at blive opdaget. Overordnet set vil den motiverede gerningsperson på bedst mulig vis kunne imødekomme muligheden for at dele det ulovlige materiale online og slippe fra det ved at have forberedt sig grundigt. Dette inkluderer bl.a. tilstrækkelig viden omkring mulighederne for at begå den kriminelle handling. Eksemplet på at motiverede gerningspersoner kan undgå politiets efterforskning, kan derfor ses som en del af læringsprocesserne angående kriminel adfærd. Ligesom omkring uberettiget adgang, lærer gerningspersonen på baggrund af læsning af tidligere sager, generelle guides online samt imitation af andres adfærd (Akers, 2011[1994], s. 134; Akers & Jennings, 2019, s. 118), hvordan den ulovlige billeddeling udføres på virtuelle platforme uden at blive opdaget.

Som der ligeledes fremgik under delanalysen uberettiget adgang, forekommer der her en opsummerende visualisering af de skridt, der er blevet gennemgået under de fire stadier ved ulovlig billeddeling. Opsætningen af Figur 6 (Spontan) og Figur 7 (Planlagt) er derfor den samme, dog i relation til ulovlig billeddeling.

Figur 6: Crime Script af *spontan* ulovlig billeddeling



Figur 7: Crime Script af *planlagt* ulovlig billeddeling



Kapitel 6
Diskussion

6. Diskussion

Der er i indeværende speciale undersøgt, hvilke skridt der indgår under uberettiget adgang til intimt materiale og efterfølgende ulovlig billeddeling. Herigennem er det blevet belyst, hvilke overvejelser, handlinger og beslutninger gerningspersonen foretager både før, under og efter den kriminelle aktivitet. Gennem den primære empiri identificerede vi en distinktion mellem en spontan og en planlagt udgave af de to kriminalitetsformer. Blandt disse to udgaver var der betydelig forskel i relation til Crime Script stadierne Preparation & Pre-activity, Activity og Post-activity. Det er mærkværdigt, hvordan især unge mennesker relativt simpelt og uden komplikationer kan få adgang til intimt materiale, opbevare det og yderligere dele det med utallige personer. Der må unægteligt være flere faktorer, som spiller ind i dette ukontrolleret virtuelle rum uden vogtere. Følgende afsnit består derfor af en diskussion af specialets analytiske fund i henhold til den spontane form for uberettiget adgang og ulovlig billeddeling.

I udarbejdelsen af specialets analyse var det fremtrædende, at Crime Scriptet hos den spontane udgave af både uberettiget adgang og ulovlig billeddeling bestod af langt mere simple skridt end i den planlagte udgave af kriminalitetsformerne. Hvis der derimod var fokus på motivationen bag de spontane forbrydelser, ville resultaterne af analysen udfolde sig anderledes. Der kan være forskellige bagvedliggende grunde til, at eksempelvis unge deler et billede relativt nemt og tilfældigt over sociale medier. Spørgsmålet omkring *hvorfor* der handles spontant er dog som bekendt ikke fokusset hos Crime Script-tilgangen jf. afsnit 4.1. Hvis specialets forskningsdesign ikke bundede i en Crime Script tilgang, havde det været fordelagtigt at supplere med et mere motivbaseret perspektiv på de kriminelle handlinger. Flere af specialets eksperter påpeger bl.a., at ulovlig billeddeling ofte sker ud fra et ønske om status og anerkendelse i den sociale sammenhæng, vedkommende befinder sig i (Bilag 5, l. 404-405; Bilag 6, l. 502-504, 546-547; Bilag 7, l. 430-431). Ligeså vel kan der herske en forestilling hos de unge om, at alle andre også deler intime billeder (Wandel, Pihl & Sørensen, 2016, s. 9). Ud fra denne Flamingoeffekt jf. afsnit 2.3, ulovlig billeddeling af intimt materiale, opstår der en såkaldt flertalsmisforståelse, hvorfor den enkelte unge anerkender denne kriminelle handling, da det synes at være fordelagtigt. Vedkommende agerer ud fra en fejlagtig opfattelse af, at de andre anser ulovlig billeddeling som acceptabel adfærd. De følger derfor en norm, som de fleste egentligt finder uacceptabel. Disse normer og værdier, der eksisterer i den pågældende gruppe, kan derfor have indflydelse på den enkeltes tilbøjelighed til at deltage i kriminelle aktiviteter. Sidsel Harder beskrev bl.a. i ekspertinterviewet, hvordan studier peger på, at det kun er hver

femte unge, der reelt videresender ulovligt materiale (Bilag 8, l. 140-141). Dette stemmer således overens med tidligere fund, da vi i afsnit 2.3 omhandlende ulovlig billeddeling af intimt materiale ligeledes beskriver, hvordan fire ud af fem unge ikke videredeler intimt materiale, men diskursen i medierne kan være med til at skabe disse flertalsmisforståelser (Mølgaard, 2019, s. 125-127).

Det er derfor muligt, at spontaniteten i disse handlinger ikke er så tilfældige, som de umiddelbart fremstår, når der udelukkende er fokus på, *hvordan* forbrydelserne begås. Handlingerne kan derimod være præget af overvejelser omkring de normer, der gør sig gældende i den social sammenhæng, og hvorledes disse bedst kan opfyldes. Selvom at der således reageres spontant i situationen, kan det alligevel skyldes bagvedliggende faktorer, eksempelvis følelsesmæssige reaktioner såsom spænding, ophidselse og glæde. Derudover kan følelser såsom sorg og vrede ligeledes gøre sig gældende, når det intime materiale deles i form af hævnporno. Selvom at handlingerne således fremstår impulsive, kan der dog stadig være en kalkulering af fordele og ulemper i den spontane udgave, ligesom det ofte er tilfældet hos den planlagte form. Den spontane udgave må derfor også i nogle tilfælde bestå af en vurdering af, hvilke konsekvenser den kriminelle handling kan medføre.

Som bekendt jf. afsnit 5.2.1, omhandlende Preparation og Pre-activity ift. ulovlig billeddeling, bunder spontan videredeling af intimt materiale ofte i mangelfuld viden omkring konsekvenserne af dette, heriblandt Straffeloven. I afsnit 2.3.2 beskrives det ligeledes, at Folketinget i 2017 fremsatte et forslag omkring udarbejdelsen af en ny paragraf i Straffeloven i henhold til digitale krænkelser. Dette forslag kommer i kølvandet på, at netop deling og efterspørgsel på intimt materiale befinder sig i en gråzone rent juridisk. Denne gråzone fordrer ligeledes forvirring og uklarhed omkring retstilstanden både ift. offer og gerningsmand. Dette kan derfor ligeledes understøtte forklaringen omkring, *hvorfor* ulovlig billeddeling forekommer. Børn og unge har endnu ikke udviklet den fulde modenhed og erfaring til at kunne vurdere de mulige konsekvenser ved handlinger. Dette kan derfor forklare, hvorfor de ikke overvejer og planlægger de kriminelle aktiviteter men derimod blot handler ud fra den situation, de befinder sig i (Wandel et al., 2016, s. 6). Dette kan hos nogen skyldes manglende *moralske barrierer*, heriblandt hvad der anses som værende rigtig og forkert adfærd. Hvis de ikke har opbygget et *moralsk kompas*, vil der i højere grad være risiko for, at de ender med at begå kriminalitet, såsom ulovlig billeddeling (Bjørgo, 2016, s. 15-16). Disse moralske barrierer dannes på baggrund af uformel kontrol herunder social interaktion (Bjørgo, 2016, s. 16). Det

kan derfor diskuteres, hvorvidt børn og unge har haft mulighed for at opbygge moralske barrierer, der forhindrer dem i at begå kriminalitet. Såfremt individet ikke har fået den nødvendige information omkring ulovlig billeddeling, vil de uden megen overvejelse videresende intimt materiale. Af samme årsag argumenterer Red Barnet for, at børn og unge skal oplyses om den online verden, de til dagligt interagerer i, herunder hvilke rettigheder individet har ift. billeder og videoer (Wandel et al., 2016, s. 10). Dette kunne eksempelvis formidles gennem gode rollemodeller, såsom forældre, skolen eller medierne (Bjørgo, 2016, s. 17). Det kan dog virke besynderligt, at denne viden og disse moralske barrierer ikke i højere grad er udbredt hos børn og unge. Jf. afsnit 2.3.1, omhandlende forebyggende indsatser og rådgivning, fremstår det netop tydeligt, at der er fokus på denne oplysning og forebyggelse i både politiregi, kommuner samt regeringen. Dette taler derfor i retning af, at de unge ofte kalkulerer mellem den status, de kan opnå på baggrund af billeddelingen, og den straf de potentielt kan udsættes for, hvis de opdages i handlingen.

Kapitel 7
Kriminalpræventive perspektiver

7. Kriminalpræventive perspektiver

Imidlertid har de empiriske fund i specialets analyse demonstreret, at der er et behov for forebyggelse af både uberettiget adgang og ulovlig billeddeling. Ved at kortlægge de enkelte sekvenser i de opstillede Crime Script stadier, kan lignende situationer identificeres og imødekommes på forhånd. Dette styrker muligheden for situationsbestemte indsatser i forhold til kriminalitetsforebyggelse (Keatley, 2018, s. 133; Healterman, 2016b, s. 13). I afsnit 2.3.1 har vi redegjort for et udsnit af de forebyggende indsatser, der de seneste år er blevet implementeret i Danmark. Dette omhandler som bekendt bl.a. samarbejdsplaner i politiregi, nyt undervisningsmateriale til brug i skoleregi samt en udførlig rapport fra Regeringen, hvori der er fokus på eksempelvis bevissikring samt argumenter for højere straffe ift. IT-kriminalitet. Derudover stod det hurtigt klart, at disse kriminalitetsformer ikke kan fjernes, medmindre internettet bliver lukket, hvilket eksperterne ifølge heraf understreger anses som værende umuligt og langt fra hensigtsmæssigt (Bilag 5, l. 511-512; Bilag 6, l. 836-840). Disse udtalelser fra henholdsvis Flemming Kjærside og Morten Rasmussen påpeger således, at IT-kriminalitet er kommet for at blive, og der i stedet skal være fokus på, hvordan disse kriminalitetsformer imødekommes. Vi vil i indeværende afsnit forsøge at kortlægge yderligere kriminalpræventive perspektiver, med det formål at specialet kan bidrage til bekæmpelse og forebyggelse af uberettiget adgang og ulovlig billeddeling.

I ovenstående diskussion i kapitel 6 fremgår det, at der stadig er brug for yderligere formidling trods et øget fokus på oplysning omkring deling af intimt materiale. Dette skyldes, at denne formidling således kan bidrage præventivt til, at nogle individer ikke blot reagerer spontant men i højere grad overvejer handlingens konsekvenser, da de bliver klar over, at handlingen er kriminel (Bjørgo, 2016, s. 15-16). Derudover kan formidlingen af konsekvenser ligeledes fungere som *Afskrækkelse ved trussel om straf* (Bjørgo, 2016, s. 21-22). Afskrækkelsen heraf vil derfor afholde nogle af de unge i at videredele ulovligt materiale, da de netop bliver bevidste om risikoen af straf. Som yderligere diskuteret i ovenstående kapitel 6, kan den spontane udgave ligeledes være præget af rationelt tænkende aktører, heriblandt en kalkulering af potentielle konsekvenser. Ved at gøre konsekvenserne tydelige for den generelle befolkning, er det muligt at afskrække individer i at begå lovbrud. Påvirkning af de sociale værdier kan give individet en forståelse af, hvor skadeligt kriminalitet kan være. Vi vurderer, at effekten af

straf, *General Deterrence*[7], derfor også vil styrke de tidligere nævnte moralske barrierer, da individet overvejer de mulige konsekvenser ved kriminalitet (Andenaes, 1971, s. 17-22).

Ydermere vil vi argumentere for, at implementeringen af en *Pop-up funktion* på diverse sociale medier ligeledes vil kunne virke forebyggende. Et konkret eksempel herpå kunne være, at når det enkelte individ vil sende eller videredele materiale på Messenger, der omfatter eksempelvis nøgenhed, vil denne funktion automatisk træde i kraft. Pop-up beskeden kunne derfor omhandle, om vedkommende er sikker på at sende billedet, da det strider mod Facebooks generelle regler. Denne tanke lægger sig op ad General Deterrence, hvor det pågældende individ bliver bevidst omkring, at den kriminelle aktivitet netop er strafbar. Denne situationelle kriminalpræventive metode kan drage paralleller til den strategi, der ofte gør sig gældende hos CSAM. Strategiens formål er at forhindre især førstegangsgerningspersoner i at opnå adgang til CSAM. Her vil søgningen på særlige ord relateret til CSAM resultere i en advarsel på skærmen omkring det kriminelle aspekt i handlingen (Edwards, Christensen, Rayment-McHugh & Jones, 2021, s. 9). Vi vurderer således ud fra et præventivt perspektiv, at yderligere oplysning, samt eventuelle notifikationssystemer, anses som fortrinlige foranstaltninger ift. de spontane sager (Bilag 6, l. 840-848, 854-859, 876-878; Bilag 9, l. 123-136, 410-411). Et yderligere eksempel på en situationel kriminalpræventiv løsning, der ligeledes gør sig gældende hos CSAM, er *Image hashing.* Dette er den primære teknologi, som anvendes til at opdage netop CSAM (Lee, Ermakova, Ververis & Fabian, 2020, s. 6). Måden hvorpå dette kan lade sig gøre er, at tidligere identificeret CSAM bliver afstemt med en unik *hashværdi*, dvs. digitalt fingeraftryk eller signatur hos det pågældende billede. Hvert billede og dens tilhørende hashværdi bliver således gemt i en database (Lee et al., 2020, s. 6). Ved at implementere denne teknologi i henhold til intimt materiale generelt, er det derfor muligt at opspore materialet hurtigere på internettet gennem hashværdien og hertil blokere det specifikke billede. Det er dog vigtigt, at databasen regelmæssigt opdateres, især ud fra det faktum, at delingen af intimt materiale som bekendt hyppigt eskalerer. Ved kontinuerligt at opdatere databasen, øges muligheden således for at finde kopier af det samme materiale (Lee et al., 2020, s. 6-7). Implementeringen af denne teknologi på forhånd kan således *reducere skadevirkningen* ved ulovlig billeddeling (Bjørgo, 2016, s. 28). Vi vurderer hertil, at implementeringen af Image

[7] Refererer til effekten af straf på den generelle befolkning. Straffens formål er således at afskrække folk i at begå kriminalitet (Andenaes, 1971, s. 17-18).

hashing potentielt kan minimere risikoen for en spiral af viktimisering[8] hos offeret, eftersom det intime materiale kan blokeres inden andre kriminelle videredeler det yderligere. På denne måde kan den eksplosive deling på internettet minimeres, og normaliteten i offerets liv kan hurtigere genoprettes (Bjørgo, 2016, s. 28). En væsentlig problematik er dog, at gerningspersonen i princippet kan ændre hashværdien gennem ændringer i selve billedet eller filnavnet (Bilag 7, l. 452-456; Lee et al., 2020, s. 6). Sådanne mindre modifikationer kan gøre, at filen ikke bliver opfanget gennem Image hashing. En måde at omgå denne problematik på er at implementere AI billedgenkendelse (Artificial Intelligence). Dette kunne eksempelvis være Google AI implementering, som i forvejen hjælper organisationer med at opdage og rapportere CSAM online. Selvom at Google bruger et neuralt netværk til at opfange CSAM, kan funktionen dog også opspore materiale, som ikke identificeres som CSAM (Lee et al., 2020, s. 8). På baggrund af billedgenkendelse er det derfor muligt at spore og identificere materiale, såsom nøgenbilleder, som bliver delt gentagne gange. Jf. mekanismen *Beskytte sårbare mål* (Bjørgo, 2016, s. 26), kan dette beskytte ofrene i at få delt deres billeder eksplosivt. Funktionen opsættes derfor til at genkende et specifikt billede, der er blevet stjålet gennem uberettiget adgang og derimod ikke alt intimt materiale på internettet. Image hashing og AI billedgenkendelse kan desuden som situationelle præventive strategier øge opdagelsesrisikoen af gerningspersonerne. Materialet kan ikke distribueres lige så let, når det er muligt at identificere de stjålne intime billeder og videoer online. Billeddelingen afværges således i det øjeblik, aktiviteten påbegyndes i form af opsporing af hashværdien og AI genkendelse af billedet. Derudover kan en Pop-up funktion, som blev præsenteret i indledningen af dette afsnit, kobles til en AI applikation. Dette muliggør, at de mere simple delinger af eksempelvis nøgenbilleder på de sociale medier ligeledes bliver opfanget og blokeret.

Foruden at have klarlagt væsentlige pointer ift. forebyggelse af den spontane del af ulovlig billeddeling ovenfor, har vi udarbejdet scripts af den planlagte udgave af både uberettiget adgang samt ulovlig billeddeling, som kan benyttes ud fra et forebyggende perspektiv. Hos den planlagte form knytter sig nogle andre strategier, både ift. hvordan den motiverede gerningsperson skal tilgå den kriminelle handling men samtidig også, hvordan vedkommende bedst muligt undgår at blive opdaget. Videreformidling af oplysning gør sig dog stadig gældende i den planlagte form, men fokusset er i stedet på, at offeret skal have bedre oplysning,

[8] Den proces der forekommer, når et offer igen og igen oplever at få delt sit intime materiale og dermed bliver viktimiseret på ny hver gang.

herunder hvordan de begår sig sikkert online. I den spontane form var fokus i højere grad på oplysning ift. konsekvenser af den kriminelle handling, og hvorledes den danske lovgivning lyder ift. ulovlig billeddeling. For bedst muligt at kunne *beskytte sårbare mål* (Bjørgo, 2016, s. 26) i de planlagte sager, kræver det generelt en større opmærksomhed på relevante forholdsregler for at undgå at blive offer for et Social Engineering-angreb. En mulig måde at forebygge dette på er derfor at øge den sociale bevidsthed omkring Social Engineering-angreb, hvor individet lærer, hvordan privat information holdes sikkert. Det skal således inkorporeres som en del af den menneskelige adfærd og forståelse (Salahdine & Kaabouch, 2019, s. 9; Hadgany, 2010b, s. 2). Det kan dog være svært at oplyse om, hvad individet præcis skal være opmærksom på, når gerningspersonen blot kan opfinde nye måder at opnå denne uberettiget adgang på (Bilag 9, l. 603-631). To væsentlige mekanismer, som brugere af de sociale medier med fordel kan gøre brug af, er to-trins-godkendelse, samt at den pågældende platform gør opmærksom på, hvis der opstår et loginforsøg til ens profil fra en fremmed lokation. Disse forebyggelsesmuligheder kan netop være med til at stoppe gerningspersonen i at opnå både et single-stage-attack samt et multi-stage-attack, jf. afsnit 5.1.2 omhandlende stadiet Activity i uberettiget adgang.

Kontinuerlig oplysning til de potentielle ofre anses derfor som et betydeligt redskab for at forebygge et sådant angreb. Vi vil således argumentere for at netop generel og kontinuerlig oplysning omkring digital adfærd og sikkerhed i nogen grad vil kunne beskytte sårbare mål for at blive ofre for eksempelvis Social Engineering-angreb.

En anden vigtig forholdsregel, som individet kan tage for ikke at eksponere sig selv for et fremtidigt Social Engineering angreb, er at danne en stærk adgangskode og aldrig dele denne med andre (Bilag 5, l. 153-155, 517-534; Bilag 6, l. 871-878; Bilag 7, l. 88-92, 144-149, 486-491; Koyun & Janabi, 2017, s. 7537; Ozkaya, 2018b, s. 129). Da det typisk er igennem adgangskoder, at der anskaffes uberettiget adgang i Social Engineering-angreb, vil denne indførte sikkerhedsforanstaltning formentlig mindske risikoen for, at der opnås adgang til det pågældende individs konti. Det er dog ikke nok at holde adgangskoder privat. Der eksisterer en generel konsensus om, at lige meget hvor teknisk sikkert et netværk er, vil det menneskelige element altid være en sårbarhed i et Social Engineering-angreb (Conteh & Schmick, 2016, s. 34; Ozkaya, 2018a, s. 8; Lohani, 2019, s. 385).

Ift. de planlagte sager omhandlende ulovlig billeddeling er Tor og VPN som bekendt to netværk, som flere gerningspersoner kan benytte, når de ulovligt deler billedmateriale på mørkenettet. Enhver kan i princippet installere dem, da Tor er gratis og VPN er billigt at tilgå. Derudover findes der en masse information online omkring, hvordan de benyttes. Dette kan således forekomme problematisk, da de to netværk kan fremme kriminalitetsformer såsom ulovlig billeddeling. Med Bjørgos situationelle mekanisme *Afværge ved at opdage og standse kriminelle handlinger, før de sker*, vælger vi at argumentere for, at der således forefindes måder, hvor ulovlig billeddeling kan besværliggøres på. Når først gerningspersonen har foretaget sine sikkerhedsforanstaltninger, og befinder sig på mørkenettet, er det væsentligt sværere at opspore den kriminelle adfærd. Det er derfor i højere grad hensigtsmæssigt at påvirke de betydelige skridt forinden dette. Konkrete eksempler herpå er at gøre Tor til en betalingstjeneste samt øge prisen på VPN-netværk. På denne måde kan antallet af motiverede gerningspersoner mindskes, såfremt de ikke har råd til eller ikke er villige til at betale for det. Denne besværliggørelse med betaling vil dog ikke forhindre alle i at udføre ulovlig billeddeling på mørkenettet, da der stadig vil forekomme motiverede gerningspersoner. Dette kunne eksempelvis være en kalkulering af flere potentielle fordele end ulemper.

D. 1. april 2022 trådte politiets Online Patrulje i kraft. Denne enhed er blevet etableret på baggrund af politiets flerårsaftale, da der herskede en bred enighed om, at der manglede en digital patruljeenhed. Denne online patrulje har til formål at patruljere på diverse sociale medier for at indgå i dialog med borgerne, især børn og unge som målgruppe, for at forebygge uhensigtsmæssig adfærd. På denne måde kan de gennem eksempelvis Facebook kommunikere med brugere, som beretter om kriminel adfærd (Politi, s.d.-b). Med fokus på forebyggelse, disruption og efterforskning på diverse sociale medier vil denne online patrulje have indflydelse på de mere spontane udgaver af billeddeling. De kan således oplyses om, via deres Facebook-side, når brugere eksempelvis opfanger en ulovlig billeddeling. Derudover kan de være synlige og eksplicitte omkring ordentlig digital adfærd. Patruljen er dog fortsat under opbygning, hvorfor de først forventer at have opgaver og udstyr helt på plads ved udgangen af året (Bjørnholdt, 2022). Når patruljen således er ordentlig etableret, ville det være særligt fordelagtigt, at de ligeledes indfører mørkenettet som et online område, hvorpå der skal patruljeres. Det vil således være fordelagtigt, at patruljeringen på mørkenettet således både forekommer synlig og usynlig, da dette således ville kunne forebygge og afskrække bedst muligt. Denne patruljering på mørkenettet vurderes nødvendigt, da det netop er her planlagt

IT-kriminalitet forekommer, og det ligeledes er her, jf. kapitel 5, at der statistisk set forefindes det største antal af ofre. Deres tilstedeværelse vil have en afskrækkende effekt på de kriminelle brugere af mørkenettet, såfremt disse individer er bevidste omkring patruljeringen. Afskrækkelsen ligger i, at der foreligger en potentiel risiko for, at de kan blive opdaget af det online politi og hermed straffes, på trods af de sikkerhedsforanstaltninger hver enkelt må have forberedt forinden. Dette vil således både have en præventiv effekt på dem, der påtænker at opnå adgang til disse kriminelle fora, men ligeledes også de gerningspersoner, der allerede befinder sig på disse sider (Bjørgo, 2016, s. 21-22).

Yderligere er det muligt for patruljen at disrupte og nedlukke de kriminelle fora, hvor der bliver distribueret intimt materiale. Dette er dog ikke så ligetil. Ligesom hos CSAM kræver det både den korrekte erfaring mht. mørkenettet og IT-kriminalitet, men desuden også et grundigt forarbejde og viden omkring de juridiske og tekniske omstændigheder, der knytter sig hertil (Demeyer, Lievens & Dumortier, 2013, s. 9). Vi vil dog ikke gå i dybden med de potentielle problematikker men derimod blot fremvise de muligheder, der foreligger hos den nye online patrulje. Nedlukningen af sociale fora på mørkenettet fordrer bl.a., at gerningspersonen mister den samhørighed, der anses som fordelagtig for at kunne videredele og anskaffe intimt materiale bedst mulig. Samtidig skabes der potentiale for, at ofrene kan blive identificeret og lokaliseret, da politiet retrospektivt kan finde de forurettede af det intime materiale (Bilag 5, l. 424-428). Dog kan det omvendt også udledes, at denne nedtagning blot medfører, at de pågældende motiverede gerningspersoner søger hen imod andre eller nyoprettede sider på mørkenettet. Der vil derfor blot forekomme en *forskydning* af den ulovlige billeddeling. Yderligere vil nedlukningen ikke imødekomme problemet omkring, at gerningspersonerne stadig har muligheden for at have det intime materiale på deres egen computer eller BPHS. Lukningen skal således ikke ses som en endegyldig måde, hvorpå ulovlig billeddeling kan komme til livs. Det vil dog uden tvivl gøre det mere besværligt for hver enkelt gerningsperson at finde nye fora og sider, hvorfra de kan dele og anskaffe intimt materiale.

I afsnit 2.1.3 har vi redegjort for væsentlige problematikker ift. det danske politis muligheder for efterforskning på internettet. Bl.a. er gråzonen for, hvad politiet må og ikke må foretage sig online særlig vigtig at have fokus på i henhold til forebyggelsesmuligheder. I selvsamme afsnit redegjorde vi for, at der eksempelvis ikke er regler for, hvordan politiet infiltrerer eller overvåger for bl.a. falske profiler online (Lentz, 2018, s. 138). I ekspertinterviewet med Morten Rasmussen italesatte han således, at det til tider kunne være ønskværdigt at eksempelvis kunne

få indbygget en regel for, at metoder såsom *honeypot*[9] kan benyttes i kampen mod online kriminalitet, hvilket der bl.a. er lovligt i det amerikanske system (Bilag 6, l. 732-746). I forlængelse af indeværende speciales omdrejningspunkt ville et klassisk eksempel på metoden i praksis være, at det online politi får adgang til en social platform, hvor de kan aflæse den sociale interaktion og kommunikation. Ved at pågribe administratoren og derefter udgive sig for at være vedkommende, kan de bruge innovative midler for at lokke brugerne til at videregive oplysninger og intimt materiale, som politiet potentielt kan bruge til den videre efterforskning af disse online fora. Denne metode er allerede benyttet i henhold til online kryptomarkeder (Martin et al., 2019, s. 28-29). Her agerer de eksempelvis som administrator, hvortil de oplyser sælgere om, at de skal uploade produktbilleder på ny, grundet en teknisk fejl. Vi antager, at denne fremgangsmåde ligeledes vil være fordelagtigt at implementere ift. ulovlig billeddeling i dansk regi, da det potentielt ville give mulighed for at opspore og fange nogle af gerningspersonerne. Ved at posere som administrator kan de således udnytte den tillid, der allerede er opbygget mellem brugerne og den tidligere kriminelle administrator. På trods af at brugerne ofte anvender falske navne og profiler, jf. afsnit 5.2.1 vedrørende Preparation og Pre-activity i ulovlig billeddeling, kan politiet muligvis gennem den dannede samhørighed få fat i personfølsom information om de kriminelle eller lykkes at spore deres korrekte oplysninger.

[9] "*Hvis man sætter noget kriminelt op, som egentlig ikke er noget kriminelt, og så lokker folk*" (Bilag 6, l. 734-735).
"*As its name suggests, a honeypot is designed to attract and stick. A honeypot or deception host is a designated area within a computer system or network that has been designed specifically with the expectation that it will be attacked by unauthorized users, whether internal or external to the organization operating the honeypot"* (Gregory, 2018, s. 278-279).

Kapitel 8
Konklusion

8. Konklusion

Indeværende speciale er udarbejdet med ønsket om at besvare problemformuleringen:

Hvilke skridt indgår i anskaffelsen af uberettiget adgang til intimt materiale samt den ulovlige videredeling heraf?

De følgende skridt der er blevet identificeret i indeværende speciale, er opnået på baggrund af fem ekspertinterviews samt supplerende eksisterende litteratur. På baggrund af specialets abduktive tilgang muliggøres det derfor, at disse skridt ikke er endegyldige men åbne for videreformidling og arbejde. Et væsentligt analytisk fund vi dog har gjort os i udarbejdelsen af analysen er, at der forekommer forskellige udgaver af uberettiget adgang samt ulovlig billeddeling. Dette kan gøres enten gennem relative simple skridt, dvs. en spontan form for kriminalitet, eller mere udførligt med mere planlægning samt flere overvejelser, nemlig en planlagt udgave. For at gøre det så konkret og overskueligt som muligt, vil disse to udgaver konkluderes særskilt.

8.1 Spontant

Det er fremtrædende hos den spontane udgave af opnåelsen af adgang til intimt materiale, at digitale enheder såsom mobiltelefoner, computere og iPads er blevet en normal del af hverdagen qua ændrede rutineaktiviteter. Social- og digital adfærd påvirkes derfor af, hvordan disse indgår i dagligdagen og sociale interaktioner. Sexting er eksempelvis blevet en almindelig måde at udtrykke sig på seksuelt. For at kunne udføre denne handling, kræver det således mindst én digital enhed, som har adgang til internettet. Ligeledes identificerede vi vigtigheden af tillid mellem de respektive parter, da dette muliggør, at der bliver videresendt intime billeder uden frygt for, at det vil blive delt med andre. Der er således ikke tale om uberettiget adgang i disse tilfælde, da sexting er en legal handling. Når forholdet dog ophører, stopper sexting typisk også. Yderligere kan der opstå tilfælde af ufrivillig sexting, hvor modtageren opnår berettiget adgang til intimt materiale uden et ønske herom. Der er således tale om blufærdighedskrænkelse, hvorfor at denne handling er strafbar i modsætning til almindelig sexting. Begge former for sexting er ikke desto mindre lette at udføre, da det blot kræver en digital enhed med internet, et kamera samt et medie, som der kan videresendes intimt materiale igennem.

Vi identificerede i den spontane ulovlige billeddeling, at det kriminelle aspekt ikke altid står klart for især unge, som deler intimt materiale. Denne manglende viden fordrer derfor, at forberedelserne er relativt simple. I den primære- og sekundære empiri peges der på, hvor let det er at videresende materiale på de sociale medier, da det blot kræver et enkelt klik. Det er dog stadig nødvendigt med en vis mængde af viden om og forståelse af, hvordan disse platforme benyttes, hvilket især unge er vokset op med qua de føromtalte rutineaktiviteter. Når der spontant bliver delt intimt materiale, sker det oftest i form af hævnporno. Letheden ved at navigere på digitale enheder, tilgængeligt berettiget intimt materiale samt et forhold, der muligvis endte på dårlige termer, er med til at muliggøre denne form for ulovlig billeddeling. Når videredelingen forekommer i disse spontane tilfælde, sker der typisk en eksplosiv deling. Her er det sjældent, at individerne sikrer anonymitet, hvorfor det er lettere for politiet at finde frem til de(n) pågældende gerningsperson(er).

8.2 Planlagt

Som der blev identificeret i de mere spontane tilfælde af uberettiget adgang til intimt materiale, gør kravet om digitale enheder med internetadgang sig ligeledes gældende hos den planlagte udgave. Af analysen kan det konkluderes, at Social Engineering er en af de mest anvendte metoder i anskaffelsen af uberettiget adgang. For at forberede dette angreb tilegner gerningspersonen sig viden omkring offeret, og hvilke psykologiske taktikker der er nødvendige ift. manipulation og tillid. Denne viden kan let tilgås i form af offentligt tilgængeligt materiale på internettet samt beretninger om andre kriminelles erfaringer. Når gerningspersonen således har forberedt disse væsentlige skridt, kan selve Social Engineering-angrebet foregå. Det er af empirien fundet, at hvis gerningspersonen udgiver sig for at være en ven/veninde, vil vedkommende hurtigere imødekomme opnåelsen af tillid. Dette er derfor et væsentligt skridt i opnåelsen af uberettiget adgang. Qua digital adfærd kan gerningspersonen ligeledes være bekendt med faktummet, at adgangskoder ofte genbruges. Dette fordrer derfor, at hvis gerningspersonen først har fået adgang til en adgangskode til én platform, vil der derfor være risiko for, at vedkommende således kan få adgang til andre platforme pba. samme adgangskode. Når gerningspersonen slutteligt har fået uberettiget adgang til det ønskede intime materiale, vil et clear exit være at foretrække. Dette betyder altså, at gerningspersonen formår at afslutte handlingen uden at blive opdaget. Efter et clear exit kan gerningspersonen fortsætte med at udføre de samme skridt i henhold til andre ofre og på denne måde udføre et multi-stage-attack. De genbruger derfor det samme manuskript på et utal af ofre.

Efter gerningspersonen således har lykkes med at forlade offerets platforme uden at blive opdaget, kan vedkommende herefter påbegynde den ulovlige billeddeling af materialet. En del af forberedelsen hertil er således at opnå viden omkring, hvor det synes fordelagtigt at dele materialet uden at blive opdaget. Denne viden kan eksempelvis tilgås gennem bekendte, det almene internet eller mørkenettet. Hertil identificerede vi, at det er nødvendigt for gerningspersonen at sikre anonymitet. Dette sker typisk gennem en Tor browser, VPN-netværk eller falske navne samt oplysninger. Når al forberedelse er udført, kan gerningspersonen gå i gang med selve den ulovlige billeddeling. Gerningspersonen udnytter ofte faldgruberne ift. den danske retshåndhævelse i form af billeddeling på udenlandske servere. Derudover anvender flere gerningspersoner BPHS til opbevaring af deres stjålne materiale samt sociale fora på mørkenettet. Sidstnævnte består især af læring omkring sikkerhed, og hvordan de kan opnå en stor samling af billeder.

Således kan der med indeværende speciale konkluderes væsentlige trin i kriminalitetsformerne uberettiget adgang til intimt materiale samt ulovlig billeddeling heraf. Der er dog forskel på, om skridtene er simple eller mere kompliceret. Ikke desto mindre konkluderer vi, at de to kriminalitetsformer unægtelig hænger sammen, da uberettiget adgang opstår på ny, hver gang ulovlig billeddeling udføres.

Litteraturliste

Abdullah A., Xu, Y. & Chan, T. (2017) *"An empirical study on the susceptibility to Social Engineering in social networking sites: the case of Facebook".* European journal of information systems. Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.1057/s41303-017-0057-y

Abraham, S. & Chengalur-Smith, I. (2010). *An overview of Social Engineering malware: Trends, tactics, and implications.* Technology in Society. Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.1016/j.techsoc.2010.07.001

Airehrour, D., Nair, N., V. & Madanian, S. (2018). *Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model*. Informationen. Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.3390/info9050110

Akers, R. L. (2011 [1994]). A Social Learning Theory of Crime. I Cullen, F. T. & Agnew, R. *Criminological Theory: Past to Present* (s. 130-137). Oxford University Press.

Akers, R. L. & Jennings, W. G. (2019). The Social Learning Theory of Crime and Deviance. I Krohn, M. D., Hendrix, N. Hall, G. P. & Lizotte, A. J. *Handbook on Crime and Deviance* (s. 113-129). Springer.

Andenaes, J. (1971). *The Moral of Educative Influence of Criminal Law*. Journal of social issues. Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.1111/j.1540-4560.1971.tb00651.x

Andersen, L. B., Binderkrantz, A. S., & Hansen, K. M. (2020). Forskningsdesign. I Hansen, K. M., Andersen, L. B., & Hansen, S. W. *Metoder i Statskundskab* (s. 69-95). Hans Reitzels Forlag.

Bates, S. (2017). *Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors*. Femenist Criminology. Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.1177/1557085116654565

Bejder, P., Sørensen, K., Pihl, M., Spanier, G. & Jørgensen, G. (2014). *Sårbar og søgende - Viden og værktøjer til at skabe dialog med udsatte unge om grænser og seksualitet på nettet.*

Red Barnet. Sidst lokaliseret d. 6. juni 2022 på: https://redbarnet.dk/media/1158/saarbar-og-soegende.pdf

Birkler, J. (2021). Begrundelsesformer. I Birkler, J. *Videnskabsteori - En grundbog* (s. 77-96). Munksgaard.

Bjørgo, T. (2016). Introduction: A comprehensive model for preventing crime. I Bjørgo, T. *Preventing Crime: A Holistic Approach.* (s. 1-35). Palgrave-Macmillan.

Bjørnholdt, K. (2022). *Vi skal være nærbetjenten på nettet.* Dansk Politi. Sidst lokaliseret d. 6. juni 2022 på: https://dansk-politi.dk/nyheder/vi-skal-vaere-naerbetjenten-paa-nettet

Boolsen, M. W. (2020). Ground Theory. I Brinkmann, S. & Tanggaard, L. *Kvalitative metoder – En grundbog.* (309-346). Hans Reitzels Forlag.

Brinkmann, S. (2020). Etik i en kvalitativ verden. I Brinkmann, S. & Tanggaard, L. *Kvalitative metoder – En grundbog* (s. 581-600). Hans Reitzel Forlag.

Brinkmann, S. & Tanggaard, L. (2020). Kvalitative metoder, tilgange og perspektiver: En introduktion. I Brinkmann, S. & Tanggaard, L. *Kvalitative metoder – En grundbog* (s. 15-29). Hans Reitzel Forlag.

Bryman, A. (2016). Qualitative Research. I Bryman, A. *Social Research Methods* (s. 373-405). Oxford University Press.

Call, C. (2021). *Perceptions of Image-Based Sexual Abuse Among the American Public.* Longwood University. Criminology, Criminal Justice, Law & Society. Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.54555/ccjls.3769.30145

Center For Cybersikkerhed (2021). *Trusselsvurdering - Cybertruslen mod Danmark 2021*. 1. udgave. Center for cybersikkerhed. Sidst lokaliseret d. 6. juni 2022 på: https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/cybertruslen-mod-danmark-2021.pdf

Chainey, S. P. & Berbotto, A. A. (2021). *A structured methodical process for populating a Crime Script of organized crime activity using OSINT. Trends in organized crime*. Springer. Sidst lokaliseret d. 6. juni 2022 på doi: 10.1007/s12117-021-09428-9

Chainey, S. P. & Tompson, L. (2011). *Profiling illegal waste activity: Using Crime Scripts as a data collection and analytical strategy.* European journal on criminal policy and research.

Chantler, A. N. & Broadhurst R. G. (2008). *Social Engineering and Crime Prevention in Cyberspace*. Korean Society of Criminal Policy. Sidst lokaliseret d. 6. juni 2022 på doi: 10.2139/ssrn.2138714

Chatzinikolaou, A. & Lievens, E. (2020). *A legal perspective on trust, control and privacy in the context of sexting among children in Europe.* Journal of Children and Media. Sidst lokaliseret d. 6. juni 2022 på doi: 10.1080/17482798.2019.1697320

Chavez, N. & Bichler, G. (2019). *Guarding against Cyber-Trespass and Theft: Routine Precautions from the Hacking Community.* International Journal of Cyber Criminology. Sidst lokaliseret d. 6. juni 2022 på doi: 10.5281/zenodo.3551489

Chinta, M., Alaparthi, J. & Kodali, E. (2016). *A Study on Social Engineering Attacks and Defence Mechanisms.* Academia.

Christensen, E. (02. september 2021). *Kære regering: Digitale krænkelser blandt unge kræver større indsats*. Sidst lokaliseret d. 6. juni 2022 på: https://jyllands-posten.dk/debat/breve/ECE13241261/kaere-regering-digitale-kraenkelser-blandt-unge-kraever-stoerre-indsats/

Cohen, L. E. & Felson, M. (2013). Routine Activity Theory. I Cullen, F. T., Agnew, R., & Wilcow, P. *Criminological Theory: Past to Present* (s. 469-479). Oxford: Oxford University Press.

Cole, R., Latif, S. & Chowdhury, M. M. (2021). *Dark Web: A Facilitator of Crime.* ResearchGate. Sidst lokaliseret d. 6. juni 2022 på doi: 10.1109/ICECCME52200.2021.9591011

Conteh, N. Y. & Schmick, P. J. (2016). *Cybersecurity: Risks, vulnerabilities and countermeasures to prevent Social Engineering attacks.* International Journal of Advanced Computer Research. Sidst lokaliseret d. 6. juni 2022 på doi: 10.19101/IJACR.2016.623006

Cornish, D. B. (1993). Crimes as Scripts. I Zahm, D. & Cromwell, P. *Proceedings of the International Seminar on Environmental Criminology and Crime Analysis* (s. 30-45). University of Miami Coral Gables, Florida.

Cornish, D. B. & Clarke, R. V. (2013). Crime as a Rational Choice. I Cullen, F. T., Agnew, R., & Wilcow, P. *Criminological Theory: Past to Present* (437-442). Oxford University Press.

Dahl, K. M., Pedersen-Hentz, S., Østergaard, S. V. & Østergaard, J. (2018). *Unges opfattelser af køn, krop og seksualitet.* Det Nationale Forsknings- og Analysecenter for Velfærd. Sidst lokaliseret d. 6. juni 2022 på: https://pure.vive.dk/ws/files/1765711/100739_Unges_opfattelser_af_k_n.pdf

Danmarks Statistik (2020). *IT-anvendelse i befolkningen.* Sidst lokaliseret d. 6. juni 2022 på: https://www.dst.dk/Site/Dst/Udgivelser/GetPubFile.aspx?id=29450&sid=itbef2020

Deakin, H. & Wakefield, K. (2013). *Skype interviewing: Reflections of two PhD researchers*. SAGE Journals. Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.1177/1468794113488126

Demant, J., Jørgensen, K. M., Harder, S. K. (2018). *Unges kriminelle adfærd på nettet.* Det Kriminalpræventive Råd. Sidst lokaliseret d. 6. juni 2022 på: https://dkr.dk/media/7121/unges-kriminelle-adfaerd-pa-nettet_ny.pdf

Demeyer, K., Lievens, E. & Dumortier, J. (2013). *Blocking and Removing Illegal Child Sexual Content: Analysis from a Technical and Legal Perspective.* Policy & Internet. Sidst lokaliseret d. 6. juni 2022 på doi: 10.1002/poi3.8

Digitaliseringsstyrelsen (2020). *Ny FN-måling: Danmark er fortsat verdensmestre i offentlig digitalisering.* Sidst lokaliseret d. 6. juni 2022 på: https://digst.dk/nyheder/nyhedsarkiv/2020/juli/ny-fn-maaling-danmark-er-fortsat-verdensmestre-i-offentlig-digitalisering/

Digitalt ansvar s.d. *Hacking.* Sidst lokaliseret d. 6. juni 2022 på: https://digitaltansvar.dk/viden/ordbog/hacking/

DKR (2021). *Digital risikoadfærd - En undersøgelse af borgeres digitale risikoadfærd, it-kriminelles adfærd og myndigheders og virksomheders arbejde med at forebygge borgerrettet*

it-kriminalitet. Det Kriminalpræventive råd, Forbrugerrådet Tænk. Sidst lokaliseret d. 6. juni 2022 på: https://dkr.dk/media/9542/digital-risikoadfaerd.pdf

DKR (2016). *Når forbrydelser bliver digitale - En anatologi om IT-kriminalitet og adfærd på internettet.* Det Kriminalpræventive Råd. Sidst lokaliseret d. 6. juni 2022 på: https://dkr.dk/media/7027/naar-forbrydelser-bliver-digitale.pdf

DKR (2017). *Pris til Dit Liv På Nettet.* Sidst lokaliseret d. 6. juni 2022 på: https://dkr.dk/nyheder/2017/apr/pris-til-dit-liv-paa-nettet

Duedahl, P., & Jacobsen, M. H. (2010). Grundbegreber. I P. Duedahl, & M. H. Jacobsen, *Introduktion til dokumentanalyse* (s. 31-52). Syddansk Universitetsforlag.

Edwards, G., Christensen, L. S., Rayment-McHugh, S. & Jones, C. (2021). *Cyber strategies used to combat child sexual abuse material.* Trends & Issues in crime and criminal justice. Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.52922/ti78313

Enevoldsen, M. s.d. *Hvad siger loven om billeddeling?* Center for Digital Dannelse. Sidst lokaliseret d. 6. juni 2022 på: https://digitaldannelse.org/vidensbase/billeddeling-3-paragraffer-du-skal-kende/

Eurojust & Europol (2019). *Common challenges in combating cybercrime - As identified by Eurojust and Europol*. Europol and Eurojust Public Information. Sidst lokaliseret d. 6. juni 2022 på: https://www.europol.europa.eu/cms/sites/default/files/documents/common_challenges_in_combating_cybercrime_2018.pdf

Europol (2021). *Serious and Organised Crime in the EU: A corrupting influence*. EU SOCTA 2021. Sidst lokaliseret d. 6. juni 2022 på: https://www.europol.europa.eu/media-press/newsroom/news/serious-and-organised-crime-in-eu-corrupting-influence

Felson, M. & Clarke, R. V. (1998). *Opportunity Makes the Thief. Practical Theory for Crime Prevention*. Police Research Series; Research, Development and Statistics Directorate. Sidst lokaliseret d. 6. juni 2022 på: https://popcenter.asu.edu/sites/default/files/opportunity_makes_the_thief.pdf

Folketinget (2017). *Forslag til folketingsbeslutning om udarbejdelse af en ny paragraf i straffeloven vedrørende digitale sexkrænkelser.* Folketingstidende A. Sidst lokaliseret d. 6. juni 2022 på: https://www.retsinformation.dk/api/pdf/188468

Fusch, P., Fusch, G. E. & Ness, L. R. (2018). *Denzin's Paradigm Shift: Revisiting Triangulation in Qualitative Research.* Journal of Social Change, Walden University. Sidst lokaliseret d. 6. juni 2022 på doi: 10.5590/JOSC.2018.10.1.02.

Goncharov, M. (2015). *Criminal Hideouts for Lease: Bulletproof Hosting Services*. TrendLabs. Sidst lokaliseret d. 6. juni 2022 på: https://eriskhub.com/files/articles/wp-criminal-hideouts-for-lease.pdf

Gregory, W. J. (2018). *Honeypots: Not for Winnie The Pooh but for Winnie The Pedo. Law enforcement's lawful use of technology to catch perpetrators and help victims of child exploitation on the dark web.* George Mason law review.

Hadnagy, C. (2010a). Mind tricks: Psychological Principles Used In Social Engineering. I Hadnagy, C. *Social Engineering The Art of Human Hacking* (s. 101-180). Wiley Publishing. Sidst lokaliseret d. 6. juni 2022 på: https://ebookcentral.proquest.com/lib/aalborguniv-ebooks/reader.action?docID=706746

Hadnagy, C. (2010b). A look into the World of Social Engineering. I Hadnagy, C. *Social Engineering The Art of Human Hacking* (s. 1-22). Wiley Publishing. Sidst lokaliseret d. 6. juni 2022 på: https://ebookcentral.proquest.com/lib/aalborguniv-ebooks/reader.action?docID=706746

Haelterman, H. (2016a). Series Editor's Preface. I Haelterman, H., *Crime Script Analysis - Preventing Crime Against Business* (s. vii-viii). Crime Prevention and security management. Sidst lokaliseret d. 6. juni 2022 på: https://link-springer-com.zorac.aub.aau.dk/content/pdf/10.1057/978-1-137-54613-5.pdf

Haelterman, H. (2016b). Crimes as Scripts. I Haelterman, H., *Crime Script Analysis - Preventing Crime Against Business* (s. 7-26). Crime Prevention and security management. Sidst lokaliseret d. 6. juni 2022 på: https://link-springer-com.zorac.aub.aau.dk/content/pdf/10.1057/978-1-137-54613-5.pdf

Harder, S. K. (2022). *Images with Nudity and Consequences. Social Situations, Pleasures and Harms in Sexting, Image-Based Abuse and Pornography.* Department of Sociology. Faculty of Social Sciences. University of Copenhagen. Ph.D. Dissertation 2022. Sidst lokaliseret d. 6. juni 2022 på: https://doi-org.zorac.aub.aau.dk/10.1080/13676261.2020.1757631

Harrits, G. S., Pedersen, C. S., Halkier, B., & Møller, A. M. (2020). Indsamling af interviewdata. I Hansen, K. M., Andersen, L. B., & Hansen, S. W. *Metoder i statskundskab* (s. 180-211). Hans Reitzels Forlag.

Hasan, M., Prajapati, N. & Vohara, S. (2010). *Case study on Social Engineering techniques for persuasion.* International journal on applications of graph theory in wireless ad hoc networks and sensor networks. Sidst lokaliseret d. 6. juni 2022 på doi: 10.5121/jgraphoc.2010.2202

Hatuka, T. & Toch, E. (2014). *The emergence of portable private-personal territory: Smartphones, social conduct and public spaces*. SAGE Journals. Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.1177/0042098014524608

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in Progress - Theory and prevention of technology-enabled offenses.* Routledge. Sidst lokaliseret d. 6. juni 2022 på: https://doi-org.zorac.aub.aau.dk/10.4324/9781315775944

Holst, N. S. (2018). *Børn og unges deling af digitale billeder og film.* Nordisk Tidsskrift for Kriminalvidenskab. Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.7146/ntfk.v105i2.120554

Hutchings, A. & Holt, T. J. (2015). *A Crime Script analysis of the online stolen data market.* The British Journal of Criminology. Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.1093/bjc/azu106

Jaishankar, K. (2009). *Sexting: A new form of Victimless Crime?* International Journal of Cyber Criminology. Sidst lokaliseret d. 6. juni 2022 på: https://www.researchgate.net/profile/Jaishankar-Karuppannan/publication/255564695_Sexting_A_new_form_of_Victimless_Crime/links/55859acc08aef58c039ee03a/Sexting-A-new-form-of-Victimless-Crime.pdf

Johansen, K. B. H., Pedersen, M. P. & Tjørnhøj-Thomsen, T. (2019). *Visual gossiping: non-consensual 'nude' sharing among young people in Denmark.* Culture, health & sexuality. Taylor & Francis Group. Sidst lokaliseret d. 6. juni 2022 på: https://doi-org.zorac.aub.aau.dk/10.1080/13691058.2018.1534140

Justitsministeriets Forskningskontor (2021). Udsathed for vold og andre former for kriminalitet. I: *Offerundersøgelserne 2005-2020.* Justitsministeriets Forskningskontor. Sidst lokaliseret d. 6. juni 2022 på: https://www.justitsministeriet.dk/wp-content/uploads/2021/12/Udsathed-for-vold-og-andre-former-for-kriminalitet.-Offerundersoegelserne-2005-2020-WT.pdf

Karpatschof, B. (2020). Den kvalitative undersøgelsesforms særlige kvaliteter. I Brinkmann, S. & Tanggaard, L. *Kvalitative metoder – En grundbog* (s. 557-580). Hans Reitzel Forlag.

Keatley, D. (2018). Crime Script Analysis. I Keatley, D. *Pathways in crime - An Introduction to Behaviour Sequence Analysis* (s. 125-136). Palgrave Macmillan. Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.1007/978-3-319-75226-6

Koyun, A. & Janabi, E. A. (2017). *Social Engineering Attacks.* Journal of Multidisciplinary Engineering Science and Technology. Sidst lokaliseret d. 6. juni 2022 på: https://www.jmest.org/wp-content/uploads/JMESTN42352270.pdf

Kruize, P. (2018). *Internetkriminalitet 2017 - Offerundersøgelse om identitetstyveri, bedrageri, afpresning og chikane i cyberspace.* Det Kriminalpræventive Råd. Sidst lokaliseret d. 6. juni 2022 på: https://emu.dk/sites/default/files/2019-05/Internetkriminalitet%202017.pdf

Kruize, P. (2013). *Kriminalitet i en digitaliseret verden – samlet rapport.* Forskningsrapport, Det Juridiske Fakultet, Københavns Universitet. Sidst lokaliseret d. 6. juni 2022 på: https://dkr.dk/media/7008/kriminalitet-i-en-digitaliseret-verden-samlet-rapport.pdf

Kvale, S. & Brinkmann, S. (2015a). Interviewvariationer. I Kvale, S. & Brinkmann, S. *Interview - Det kvalitative forskningsinterview som håndværk* (s. 197-218). Hans Reitzels Forlag.

Kvale, S. & Brinkmann, S. (2015b). Tematisering og design af interviewundersøgelse. I Kvale, S. & Brinkmann, S. *Interview - Det kvalitative forskningsinterview som håndværk* (s. 151-176). Hans Reitzels Forlag.

Kvale, S. & Brinkmann, S. (2015c). Udførelse af et interview. I Kvale, S. & Brinkmann, S. *Interview - Det kvalitative forskningsinterview som håndværk* (s. 177-196). Hans Reitzels Forlag.

Kvale, S. & Brinkmann, S. (2015d). Transskription af interview. I Kvale, S. & Brinkmann, S. *Interview - Det kvalitative forskningsinterview som håndværk* (s. 235-248). Hans Reitzels Forlag.

Kvale, S. & Brinkmann, S. (2015e). Forberedelse til interviewanalyse. I Kvale, S. & Brinkmann, S. *Interview - Det kvalitative forskningsinterview som håndværk* (s. 249-266). Hans Reitzels Forlag.

Kvale, S. & Brinkmann, S. (2015f). Samtaler om interview. I Kvale, S. & Brinkmann, S. *Interview - Det kvalitative forskningsinterview som håndværk* (s. 369-398). Hans Reitzels Forlag.

Kvale, S. & Brinkmann, S. (2015g). Den sociale konstruktion af validitet. I Kvale, S. & Brinkmann, S. *Interview - Det kvalitative forskningsinterview som håndværk* (s. 313-338). Hans Reitzels Forlag.

Lavorgna, A. (2014). *Script Analysis of Complex Criminal Activities: Investigating the Use of the Internet as a Facilitator for Offline Transit Crimes*. SAGE Publications, Ltd. Sidst lokaliseret d. 6. juni 2022 på: https://dx.doi.org/10.4135/9781446273050135182 85

Leclerc, B., Drew, J., Holt, T. J., Cale, J. & Singh, S. (2021). *Child sexual abuse material on the darknet: A script analysis of how offenders operate. Trends & issues in crime and criminal justice*. Australian Institute of Criminology. Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.52922/ti78160

Lee, H., Ermakova, T., Ververis, V. & Fabian, B. (2020). *Detecting child sexual abuse material: A comprehensive survey*. Forensic Science International: Digital Investigation. Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.1016/j.fsidi.2020.301022

Lentz, L. W. (2018). Efterforskningens grænser på internettet. I R. F. Jørgensen, & B. K. Olsen, *Eksponeret - Grænser for privatliv i en digital tid*. GadJur.

Lentz, L. W. (2019). *Politiets hemmelige efterforskning på internettet*. Ph.d. Afhandling. Aalborg Universitetsforlag.

Leukfeldt, E. R. & Yar, M. (2016). *Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis.* Deviant Behavior, Routledge Taylor & Francis Group. Sidst lokaliseret d. 6. juni 2022 på doi: 10.1080/01639625.2015.1012409.

Lohani, S. (2019): *Social Engineering: Hacking into Humans. International Journal of Advanced Studies of Scientific Research*. Birla Institute of Applied Sciences, Bhimtal.

Lusthaus, J. (2013). *How organised is organised cybercrime?* Global Crime. Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.1080/17440572.2012.759508

Mandau, M. B. H. (2019). *'Directly in Your Face': A Qualitative Study on the Sending and Receiving of Unsolicited 'Dick Pics' Among Young Adults.* Sexuality & Culture. Sidst lokaliseret d. 6. juni 2022 på doi: 10.1007/s12119-019-09626-2

Martin, J., Cunliffe, J. & Munksgaard, R. (2019). A Modern-day History of Cryptomarkets. I Martin, J., Cunliffe, J. & Munksgaard, R. *Cryptomarkets: A Research Companion, Cryptomarkets: A Research Companion.* (s. 5-34). Emerald Publishing Limited.

Midt- og Vestjyllands Politi. (2021). *27-årig mand tiltalt i stor hackersag.* Sidst lokaliseret d. 6. juni 2022 på: https://politi.dk/midt-og-vestjyllands-politi/nyhedsliste/27aarig-mand-tiltalt-i-stor-hackersag/2021/11/16

Mølgaard, M. (2019). *Delt - En bog til unge om digitale sexkrænkelser*. Straarup & Co.

Møller, K. (2013). Rational choice. I Sørensen, A-S. & Jacobsen, M., H. *Kriminologi - en introduktion* (s. 193-121). Hans Reitzels Forlag.

Natow, R. S. (2019). *The use of triangulation in qualitative studies employing elite interviews*. Qualitative Research Journal, SAGE Journals. Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.1177/1468794119830077

Otteren, H. & Gynnild, A. (2021). *Remote Female Fixation—A Grounded Theory on Semi-Illegal Sharing of Nude Imagery Online. Forum Qualitative Sozialforschung / Forum: Qualitative Social Research.* Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.17169/fqs-22.2.3556

Ozkaya, E. (2018a). Introduction to Social Engineering. I Ozkaya, E. *Learn Social Engineering. Learn the art of human hacking with an internationally renowned expert* (s. 5-37). Packt Publishing.

Ozkaya, E. (2018b). Targeting and Recon. I Ozkaya, E. *Learn Social Engineering. Learn the art of human hacking with an internationally renowned expert* (s. 115-129). Packt Publishing.

Politi s.d.-a. *Anmeld uberettiget adgang*. Sidst lokaliseret d. 6. juni 2022 på: https://politi.dk/hacking/anmeld-uberettiget-adgang

Politi s.d.-b. *Politiets Online Patrulje.* Sidst lokaliseret d. 6. juni 2022 på: https://politi.dk/virksomheden/national-enhed-for-saerlig-kriminalitet/politiets-online-patrulje

Politi (2018). *Dansk politi vil sikre hurtigere og bedre hjælp til ofre for digitale sexkrænkelser.* Sidst lokaliseret d. 6. juni 2022 på: https://politi.dk/rigspolitiet/nyhedsliste/dansk-politi-vil-sikre-hurtigere-og-bedre-hjaelp-til-ofre-for-digitale-sexkraenkelser/2018/11/01

Politi, F. (2022). *Kredsrådets samarbejdsplan 2022.* Fyns Politi. Sidst lokaliseret d. 6. juni 2022 på: https://politi.dk/-/media/mediefiler/soejyl/dokumenter/kredsraadet/samarbejdsplaner/samarbejdsplan-kredsr%C3%A5det-2022.pdf?la=da&hash=BFC0A24DD6183F4C69F2E862D1B19483B13CA9F5

Rahman, K. F. (2012). *'Triangulation' Research Method as the Tool of Social Science Research.* BUP Journal. Sidst lokaliseret d. 6. juni 2022 på: https://www.researchgate.net/publication/331645590_%27Triangulation%27_Research_Method_as_the_Tool_of_Social_Science_Research

Rambøll (2021). *Børn og unges oplevelser med digitale krænkelser - Afrapportering af undersøgelse 2021.* Red Barnet. lokaliseret d. 6. juni 2022 på:

https://redbarnet.dk/media/7983/sletdet-boern-og-unges-oplevelser-med-digitale-kraenkelser-rapport.pdf

Regeringen (2017). *Skærpet indsats mod digitale sexkrænkelser*. Regeringen. Sidst lokaliseret d. 6. juni 2022 på: https://www.uvm.dk/publikationer/folkeskolen/2017-skaerpet-indsats-mod-digitale-sexkraenkelser

Rigspolitiet (01. november 2018). *Dansk politi vil sikre hurtigere og bedre hjælp til ofre for digitale sexkrænkelser*. Sidst lokaliseret d. 6. juni 2022 på: https://politi.dk/rigspolitiet/nyhedsliste/dansk-politi-vil-sikre-hurtigere-og-bedre-hjaelp-til-ofre-for-digitale-sexkraenkelser/2018/11/01

Ritzau (06. januar 2020a). *Anmeldelser af billeddelinger er fordoblet på få år*. Sidst lokaliseret d. 6. juni 2022 på: https://www.berlingske.dk/samfund/anmeldelser-af-billeddelinger-er-fordoblet-paa-faa-aar

Ritzau (06. januar 2020b). *Umbrella-sagen satte fokus på digitale sexkrænkelser, og det kan have fået flere til at anmelde, mener politi.* Sidst lokaliseret d. 6. juni 2022 på: https://www.avisen.dk/anmeldelser-af-billeddelinger-er-fordoblet-paa-faa-a_580995.aspx

Ritzau (21. februar 2022a). *27-årig anklages for at krænke 516 ofre i kæmpe hackersag.* Sidst lokaliseret d. 6. juni 2022 på:https://www.berlingske.dk/samfund/27-aarig-anklages-for-at-kraenke-516-ofre-i-kaempe-hackersag

Ritzau (16. marts 2022b). *Delte mappe med tusindvis af nøgenfotos: Jeg ville være flink.* Sidst lokaliseret d. 6. juni 2022 på: https://www.sn.dk/danmark/delte-mappe-med-tusindvis-af-noegenfotos-jeg-ville-vaere-flink/

Ritzau Krimi (28. marts 2022). *Hundredvis af kvinder må vente på erstatning i billedmappe-sag.* Sidst lokaliseret d. 6. juni 2022 på: https://www.nordjyske.dk/nyheder/krimi/hundredvis-af-kvinder-maa-vente-paa-erstatning-i-billedmappe-sag/2722754

Salahdine, F. & Kaabouch, N. (2019). *Social Engineering Attacks: A survey. MDPI.* Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.3390/fi11040089

Sardá, T., Natale, S., Sotirakopoulos, N. & Monaghan, M. (2019). *Understanding online anonymity.* SAGE Journals. Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.1177/0163443719842074

Strasburger, V. C., Zimmerman, H., Temple, J. R. & Madigan, S. (2019). *Teenagers, Sexting, and the Law.* American Academy of Pediatrics. Sidst lokaliseret d. 6. juni 2022 på doi: 10.1542/peds.2018-3183

Staunæs, S. & Søndergaard, D. M. (2005). Interview i en tangotid. I Järvinen, M. & Mik-Meyer, N., *Kvalitative metoder i et interaktionistisk perspektiv* (s. 49-72). Hans Reitzels Forlag.

Sykes, G., M. & Matza D. (2013). Techniques of Neutralization. I Cullen, F. T., Agnew, R., & Wilcox, P. *Criminological Theory: Past to Present* (s. 221-228). Oxford University Press.

Sørensen, A-S. (2013). Kriminalitet i tal. I Sørensen, A-S. & Jacobsen, M., H. *Kriminologi - en introduktion* (s. 23-40). Hans Reitzels Forlag.

Tanggaard, L. & Brinkmann, S. (2020a). Interviewet: Samtalen som forskningsmetode. I Brinkmann, S. & Tanggaard, L. *Kvalitative metoder – En grundbog* (s. 33-64). Hans Reitzel Forlag.

Tanggaard, L. & Brinkmann, S. (2020b). Kvalitet i kvalitative studier. I Brinkmann, S. & Tanggaard, L. *Kvalitative metoder - En grundbog* (s. 657-670). Hans Reitzels Forlag.

Thagaard, T. (2004). Dataindsamling: Observation. I Thagaard, T. *Systematik og indlevelse. En indføring i kvalitativ metode* (s. 65-85). Akademisk Forlag.

Van der Bruggen, M. & Blokland, A. (2021). *A Crime Script Analysis of Child Sexual Exploitation Material Fora on the Darkweb*. Sage Publications. Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.1177/1079063220981063

Viano, E. C. (2017). Cybercrime: Definition, Typology, and Criminalization. I Viano, E. C. *Cybercrime, Organized Crime, and Societal Responses.* (s. 3-22). Springer International Publishing.

Wandel, R., Pihl, M. & Sørensen K. (2016). *"Når børn og unge deler intime billeder på nettet. Nøgen på nettet"*. Red Barnet. Sidst lokaliseret 6. juni 2022 på: https://redbarnet.dk/media/1591/naar_boern_og_unge_deler_intime_billeder_paa_nettet.pdf

Waschke, M. (2017). Why Doesn't Somebody Stop It? I Waschke, M. *Personal Cybersecurity - How to avoid and recover from cybercrime.* (s. 153-174). Apress. Sidst lokaliseret d. 6. juni 2022 på doi: 10.1007/978-1-4842-2430-4

Webroot, s.d. *What is Social Engineering? Examples & Prevention Tips.* Sidst lokaliseret d. 6. juni 2022 på: https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering

Wohlin, C. (2014). *Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering*. Blekinge Institute of Technology. Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.1145/2601248.2601268

Ybarra, M. L. & Mitchell, K. J. (2014). *"Sexting" and Its Relation to Sexual Activity and Sexual Risk Behavior in a National Survey of Adolescents.* Journal of Adolescent Health. Sidst lokaliseret d. 6. juni 2022 på doi: 10.1016/j.jadohealth.2014.07.012

Żadkowska, M., Dowgiałło, B., Gajewska, M., Herzberg-Kurasz, M. & Kostecka, M. (2022). *The Sociological Confessional: A Reflexive Process in the Transformation From Face-To-Face to Online Interview.* Sage Journals. Sidst lokaliseret d. 6. juni 2022 på: https://doi.org/10.1177/16094069221084785

Åkerstrøm, M. & Wästerfors, D. (2018). *"Kvalitative interviews - praktiske råd og analytiske muligheder".* I Jacobsen, M. H. *Metoder i kriminologi* (s. 141-171). Hans Reitzels Forlag.

Aalborg Universitet, (s.d.). *GDPR for studerende.* Sidst lokaliseret d. 6. juni 2022 på: https://www.studerende.aau.dk/gdpr