POLITIHØGSKOLEN

KILDE TIL BEKYMRING ELLER OPPLYSNING?

POLITIETS OPPFATNINGER AV ÅPNE INTERNETTKILDER TIL ETTERFORSKNINGSFORMÅL

Bjørn Rasmussen

MASTER I ETTERFORSKNING 2018

Sammendrag

Avhandlingen søker innblikk i politiansattes oppfatninger av åpent tilgjengelig informasjon på internett til etterforskningsformål. 4 fokusgrupper, bestående av 22 politiansatte ble intervjuet om deres holdninger til åpne internettkilder. Den analytiske rammen for undersøkelsen er hentet fra adferdsforskning innen feltet teknologiakseptanse. En studie fra 2014 gjennomført i USA viste at 81% av polititjenestepersoner i USA aktivt benyttet sosiale medier som et verktøy i sitt arbeide, til tross for at man hadde få etablerte standarder og metoder for bruk av sosiale medier til etterforskning.

Norsk politi fikk i 2018 etablert en nasjonal standard som beskriver metoder for innhenting av åpent tilgjengelig informasjon på internett til politimessige formål. Denne utgjør oppgavens teoretiske grunnlag for videre praktiske, juridiske og etiske drøftinger opp mot fokusgruppenes synspunkter.

Undersøkelsen viste at politiet er bekymret for å gjøre feil når skal benytte åpne kilder på internett. Feil som å legge igjen digitale spor som kan eksponere deres privatliv, skade etterforskningen eller utsette politiets egne nettverk for dataangrep. Også feil fra upålitelige kilder som er vanskelige å vurdere var en bekymring.

Åpne kilder verdsettes samtidig høyt for rask og enkel tilgang til informasjon, som kanskje ikke finnes andre steder. Åpne kilder ble beskrevet som avgjørende i oppdagelsen og oppklaringen av flere kriminalitetstyper. Disse fordelene skaper også forventinger, både fra publikum og de politiansatte selv om å kunne håndheve loven og beskytte innbyggerne, også på internett.

Til tross for den nye standarden, var det mye usikkerhet knyttet til hvilke lover og regler som gjelder for å nytte informasjon fra det åpne nettet og sosiale medier til etterforskning. Det var også vanskelig for gruppene å identifisere etiske problemstillinger rundt deres bruk av åpen kildeinformasjon.

Dersom søk på åpne internettkilder blir mer utbredt brukt av politiansatte, kan det bedre etterforskningen av internettrelatert hverdagskriminalitet og føre til at en større andel av denne typen kriminalitet både anmeldes og oppklares. Mindre mørketall kan gi et mer nøyaktig grunnlag for bekjempelse og videre forsking.

Summary

This dissertation seeks insight into police officers' perceptions of openly available information on the internet for investigative purposes. Data was gathered from 4 focus groups, comprising 22 police officers interviewed about their attitudes to open internet sources. The analytical framework for the survey is taken from behavioral research in the field of technology acceptance. A 2014 study conducted in the United States showed that 81% of police officers in the United States actively used social media as a tool in their work, despite having few established standards or methods for social media investigations.

In 2018, the Norwegian police established a national standard that describes methods for collection of openly available information on the Internet for police purposes. This standard forms theoretical basis of the thesis and to identify practical, legal and ethical considerations for comparison with the focus group data.

The study showed that the police are concerned about making mistakes when using open Internet sources. Mistakes like leaving digital tracks that can expose their privacy, damage the investigation or expose the police's own network to computer attacks. Also mistakes resulting from a perception of unreliability in open sources were a concern.

At the same time, open sources are highly valued for quick, easy to access information, which may not be found in the police's own registries. Open sources were described as crucial in the discovery and successful procecution of several types of crime. These benefits also create expectations, both from the public and the police officers themselves to be able to enforce the law and protect their citizens - online and off.

Despite the new standard, there was a great deal of uncertainty about which laws and regulations apply applies to utilizing information from the open web and social media for investigation. It was also difficult for the focusgroups to identify ethical issues arising from their use of open source information.

If open source internet investigations can become more widespread among Norwegian police, it may increase the capability of tackling internet-related everyday crime. Which in turn could ensure that a greater percentage of these types of crimes are both reported and resolved, creating a more accurate basis for further research.

Forord

Denne avhandlingen avslutter et treårig deltidsstudium i etterforskning ved Politihøgskolen. Stor takk til min veileder Sverre Flaatten tålmodighet, faglig veiledning, oppmuntring og tilbakemelding underveis. Takk også fakultetsmedlemmer ved Politihøgskolen Olav Dahl og Pål Winnæss. Takk også til Kira Vrist Rønn for hennes interesse og bidrag. Takk til lederne mine ved Kripos for tilrettelegging som har vært avgjørende for å endelig komme i mål med prosjektet. I tillegg vil jeg takke deltakerne i intervjugruppene for deres unike innsikt og flotte engasjement. Til slutt en stor takk til min kjære samboer for hennes støtte og tålmodighet.

Innhold

1. Innledning

1.1. Introduksjon

Informasjon sies å være livsblodet i enhver etterforskning (Chilton, 2013, s. 204). Internett representerer en enorm kilde til informasjon om nesten alle former for aktivitet i samfunnet. SINTEF konstaterte for noen år siden at 90 prosent av all data i verdenshistorien er generert de siste to årene, og at stadig mer blir tilgjengelig på nettet (Brandtzæg, 2013). Dette prosjektet tar utgangspunkt idéen om at politietterforskninger rutinemessig og på forsvarlig vis kan gjøre nytte av informasjon som er allment tilgjengelig på nettet. Dagens etterforskere bør kunne vurdere åpne internettkilder som arbeidsmetode på lik linje med for eksempel avhør.

Studien søker innsyn i perspektivet til politiansatte som jobber med etterforskning. Hvordan ser de internettets potensiale for deres arbeid? Oppfattes det som en kilde til bekymring, eller en ressurs til støtte for etterforskningen? Hva baserer etterforskerne sine synspunkter på? Overordnet ønsker avhandlingen å besvare spørsmålet:

Hva er politiets oppfatninger av åpne internettkilder til etterforskningsformål?

Svaret er søkt ved å analysere intervjuer av 4 grupper rekruttert fra etterforskningsavdelinger i ulike deler av landet. Gruppene bestod av totalt 22 politiansatte med etterforskning som sin primæroppgave. Fokuset for intervjuene er formet av teori innen forskningsfeltet teknologiakseptanse – forståelsen av hva som får folk til å ta i bruk eller avvise ny informasjonsteknologi. En teoretisk modell fra feltet, UTAUT-modellen, er brukt til forberedelse, gjennomføring og tolkning av den empiriske undersøkelsen. I avhandlingens analysekapittel brukes elementer av UTAUT-modellen som byggesteiner for å konseptualisere funnene fra undersøkelsen i en ny modell, kalt teknologiakseptanse perspektiv (TAP). UTAUT presenteres mer detaljert i kapittel 3 om metode.

1.2. Bakgrunn og begrunnelse for oppgaven

Samfunnsdebatten virker å preges av oppfatninger om at politiet ikke holder følge med informasjon- og kommunikasjonsrevolusjonen som har preget samfunnet siden starten av 90-tallet; da nettverk av datamaskiner begynte å bli allment tilgjengelig gjennom «World Wide

Web», eller internett (McPherson, 2009). Mediene[1], forskere (NorSIS, 2018) og politiet selv (Politidirektoratet, 2017) påpeker i nylige publikasjoner et betydelig kompetansegap mellom politi- og påtalemakten og internettets potensiale. Potensialet gis begge fortegn i debatten. Positivt som et allment verktøy for bedring av kommunikasjon, samhandling og forståelse. Negativt i form av eksempelvis datatyveri, svindel, omsetning av ulovlige varer og seksuelle overgrep mot både barn og voksne.

For mange politietterforskere vil det ikke kreve mye praktisk opplæring for å ta i bruk åpne internettkilder som metode. Nettsider og mobilapplikasjoner tilstreber typisk å være så brukervennlige og intuitive som mulig. De aller fleste har også brukerkonti og omfattende erfaring med mange av de største åpne internettkildene – sosiale medier – fordi de allerede bruker dem i sitt privatliv[2]. Denne «hastighetsforskjellen» mellom rask og enkel tilgang til informasjon med potensielt stor verdi for etterforskningen, og de ofte mer tidkrevende etiske og juridiske retningslinjene som må ligge til grunn for å sikre tillit til politiets metoder, kan være problematisk. Robert David Steele, tidligere CIA-offiser og siden aktivist for åpen kildeetterretning, påpeker nødvendigheten av kildekritikk (2007, s. 130):

> *To exclude the information flow carried by the Internet is to exclude the greatest emerging data source available. While the Internet is a source of much knowledge, all information gleaned from it must be assessed for its source, bias and reliability.*

Det er altså ikke tilstrekkelig å vite hvordan man sikrer informasjon fra åpne internettkilder – etterforskerne må også være i stand til å gjøre vurderinger rundt pålitelighet, legalitet og etikk. UTAUT-modellen slik den anvendes her, adresserer ikke de etiske og juridiske vurderingene som inngår i politietterforskning. Kripos (2018) har imidlertid utarbeidet en nasjonal veileder for bruk av åpne internettkilder i politiet. Kriposveilederen etablerer en definisjon av søk på åpne kilder til politimessige formål. Denne definisjonen presenteres i kapittel 2 om teori, og danner utgangspunktet for juridiske og etiske drøftinger av politiets utnyttelse av informasjon som er åpent tilgjengelig på internett. Formålet er å se mulige konsekvenser for empirien generert i gruppeintervjuene, og tjene som et grunnlag for å forstå funnene som presenteres i kapittel 4. Ved å se denne relativt ferske nasjonale fagstandarden opp mot erfaringene fra intervjugruppene, kan man få en pekepinn på hvor langt implementeringen har kommet, og hvordan den videre metodeutviklingen kan tilrettelegges.

[1] https://www.nrk.no/trondelag/1.13850967
[2] https://www.ssb.no/teknologi-og-innovasjon/artikler-og-publikasjoner/fire-av-fem-nordmenn-bruker-sosiale-medier

Politiets implementering av åpne kildesøk kan utfordres av uklare definisjoner og grensedragninger relatert til begrep som datakriminalitet, hacking, ulovlig fildeling, cyberkriminalitet og så videre (Gordon & Ford, 2006). Og selv om klare definisjoner etableres, krever den raske utviklingen jevnlig sammenslåinger og oppdateringer av definisjonene (Moore, 2011, s. 5). Slik usikkerhet kan bidra til å heve terskelen for politifolk uten særkompetanse til å iverksette internettetterforskning, selv om man ser fordelene ved metoden. Fristelsen for å henvise alt som har med internettundersøkelser å gjøre til en spesialist, kan dermed bli stor.

Andelen ansatte politiet definerer som spesialister innen dataetterforskning er imidlertid veldig lav. I 2012 var antallet av det som ble beskrevet som «dataetterforskere» mellom null til tre i hvert politidistrikt, med unntak av Oslo, som hadde 14 stillinger av denne typen (Politidirektoratet, 2012). Men er etterforskning på internett et særfenomen for spesialister? Bilder, video i både opptak og sanntid, geografisk posisjon og personrelasjoner er eksempler på data som de aller fleste av oss, bevisst eller ubevisst, legger ut åpent tilgjengelig på sosiale medier og andre deler av internett hver dag. Dette er informasjon som kan utgjøre et verdifullt bidrag i nærmest alle typer kriminalsaker.

Selv om antallet dataetterforskere har økt siden 2012, virker det rimelig å anta at spesialistene raskt vil bli (eller allerede er) overveldet dersom de alene skal foreta bevissikring fra internett i alle saker hvor det er hensiktsmessig. «Kapasiteten (på dataetterforskere, min anmerkning) er under kritisk størrelse», heter det i Politidirektoratets datakrimstrategi (2015, s. 13). Gitt dette er det forståelig dersom spesialistene dedikeres de mest alvorlige sakene og vanskeligste tekniske utfordringene. Men hva gjør det med hverdagskriminaliteten? Politiets strategiplan for 2017-2025 (Politidirektoratet, 2017, s. 26) sier:

> *Et nytt landskap for kriminalitet og politiarbeid har over tid vært under utvikling som følge av den teknologiske utviklingen i samfunnet. (…) At ny teknologi og nye arenaer raskt tas i bruk til ulovlige formål gjør det krevende å utvikle vår kapasitet for å møte utviklingen. Nettkriminalitet blir i liten grad anmeldt og innbyggerne har lave forventninger til politiet på dette området.*

En begrunnelse for avhandlingen er at dersom søk på åpne internettkilder kan bli mer utbredt blant politiansatte generelt, kan det frigjøre spesialister åpne kildesøk ganske mange i teorien kan gjøre selv. Økt etterforskning av internettrelatert hverdagskriminalitet kan også føre til at en større andel av denne typen kriminalitet både anmeldes og oppklares. Mindre mørketall kan gi et mer nøyaktig grunnlag for videre forsking og bekjempelsesstrategier, og ivareta publikums tillit til at politiet skal kunne hjelpe dem – også på nett. Internettsøk på åpne

kilder, med tilhørende dokumentasjon og rapportering, kan bli et første steg etterforskere uten særlig spesialisering kan ta for å bli mer fortrolige med internettetterforskning. Å ta i bruk åpne nettkilder kan slik utgjøre en grunnsten i politiets overordnede innsats på å hente inn kompetansegapet til digitaliseringen av samfunnet og bygge effektive bekjempelsesstrategier mot kriminalitet, både på internett og ellers.

Hvordan får man så etterforskere uten særlig forkunnskap eller interesse i informasjon- og kommunikasjonsteknologi til å ta i bruk åpne internettkilder som en arbeidsmetode? Dette spørsmålet formet problemstillingen presentert innledningsvis. Et nyttig sted å starte kan nemlig være å øke forståelse for hva etterforskerne selv tenker om å bruke åpne internettkilder. Hvilke grunner oppgir de for å bruke, eller ikke bruke, internett i sitt etterforskningsarbeid?

1.3. Tidligere forskning

Politiets bruk av åpne kilder på internett har ikke vært gjenstand for mange empiriske undersøkelser. Det ble i 2014 gjennomført en spørreundersøkelse i USA av forskningsselskapet LexisNexis om politiets bruk av sosiale media til polisiær virksomhet – både operativ virksomhet, etterforskning, etterretning og forebygging. Respondentene var fra ulike politiorganisasjoner og nivåer – fra lokalt, regionalt og føderalt. Spørreundersøkelsen viste at 81% av polititjenestepersoner i USA aktivt benyttet sosiale medier som et verktøy i sitt arbeide. Rapporten påpeker at man til tross for utbredt bruk har få politiavdelinger med etablerte standarder og metoder for bruk av sosiale medier til etterforskning (LexisNexis, 2014, s. 8).

Det virker usikkert hvorvidt funnene i USA er overførbare til norske forhold. Systemforskjellene er nærliggende å påpeke - USA og Norge har ulike lovverk for å regulere etterforskning. USA har imidlertid også signert og ratifisert den såkalte Budapest-konvensjonen, så noen av de juridiske rammene er de samme som Norge har forpliktet seg til. Budapest-konvensjonen omhandles nærmere i teorikapittelets del 2.4.

I tillegg viser LexisNexis i sin rapport til flere menneskelige faktorer som påvirker hvorvidt en etterforsker vil bruke sosiale medier i jobben sin – eksempelvis internettilgjengelighet på jobb, kunnskapsnivå, oppfatning av nytteverdi og relabilitet av sosiale medier (LexisNexis, 2014, s. 7). lignende faktorene finnes også i UTAUT-modellen brukt i denne undersøkelsen.

Studien fra USA kan gi en pekepinn på hvor utbredt internettsøk til etterforskningsformål er blant etterforskere i Norge. Tiden siden undersøkelsen ble gjennomført kan også være en faktor, da tilgang til og bruk av internettjenester øker raskt – antallet Facebook-brukere har for eksempel økt med ca. 722 millioner fra 3. kvartal 2014 til 3. kvartal 2017 på verdensbasis[3].

2. Teori

Avhandlingen startet med søk etter litteratur som kunne hjelpe meg å bedre forstå hva åpne internettkilder til etterforskning innebærer. Dette kapittelet utgjør på mange måter resultatet av de litteratursøkene. Kapittelet tar utgangspunkt i en definisjon av åpne kildesøk på internett, utarbeidet av politiet selv. Fra denne definisjonen utledes praktiske, juridiske og etiske perspektiver på politiets bruk av internett til etterforskning. Hensikten er å gi både meg som forsker og avhandlingens lesere et grunnlag for å forstå den empiriske undersøkelsen, som å gjenkjenne årsaker eller mønstre i de data som generes fra intervjuene.

Kapittelet er strukturert ved å først etablere en definisjon på hva åpne internettkilder er (del 2.1). Som det sentrale begrepet i problemstillingen, er det viktig å tidlig få på plass en avklaring som avgrenser hvilken teori som er relevant og fokuserer den empiriske undersøkelsen. Definisjonen utforskes nærmere ved å bryte den ned i sine bestanddeler. Hver del av definisjonen brukes som tittelen på sitt respektive underkapittel (fra del 2.2 til 2.6), hvor det utdypes hva den delen av definisjonen betyr, og drøfter den opp mot relevant juridisk eller etisk teori. Hvert underkapittel avsluttes med å se fremover, på hvilke funn eller mønstre man kan forvente å finne i den empiriske undersøkelsen som en konsekvens av den teoretiske drøftingen.

2.1. Definisjon av åpne internettkilder

Norsk politi hadde ingen entydig beskrivelse av innhenting av informasjon fra åpne kilder på internett inntil Kripos i november (2018) gav ut den første nasjonale veilederen for intern bruk i politiet. Som nasjonalt fagansvarlig organ for etterforskningsmetodikk i Norge, yter Kripos spesialisert bistand til resten av politietaten blant annet innen datatekniske

[3] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

undersøkelser og etterforskningsstøtte for spor på internett[4]. Veilederen deres brukes her som en politifaglig forankring og et grunnlag for videre drøfting. Den definerer politiets søk på åpne kilder slik (Kripos, 2018, s. 6):

«Metoder for innhenting av åpent tilgjengelig informasjon på internett til politimessige formål»

Definisjonen alene utgjør ikke et tilstrekkelig teoretisk fundament i denne sammenhengen. Juss og forståelsen av hvordan loven bør håndheves påvirker også politiets syn på, og utøvelse av, sitt arbeid. Derfor utfylles definisjonen i de neste underkapitlene ved å trekke inn relevante lovbestemmelser og faglitteratur om etiske problemstillinger som kan oppstå når informasjon fra åpne nettkilder brukes til noe annet enn det den opprinnelig var tiltenkt. Sosiale medier er kanskje blant de mest utbredte åpne internettkildene. For å lykkes, søker sosiale mediaplattformer ofte å gjøre det enklest mulig å søke opp og se forbindelser mellom brukere av plattformen. Kira Vrist Rønn og Sille Obelitz Søe (2019, s. 2) stiller spørsmålet:

> *Although the information can easily be accessed, the pressing question is whether and under which circumstances it is morally permissible for government authorities to gain access to personal social media accounts and exploit the information for safety and security issues.*

Rønn og Søe argumenterer at myndigheter har et særlig moralsk ansvar når de utnytter opplysninger fra sosiale media om personer for sikkerhets- og tryggingsformål. Siden det er en ulovfestet metode (se del 2.3), er ikke søk på åpne kilder underlagt forhåndskontroll av påtalejurist eller domstol. I praksis ligger ansvaret for å vurdere etikken ved innhenting og bruk av åpen kildeinformasjon den enkelte.

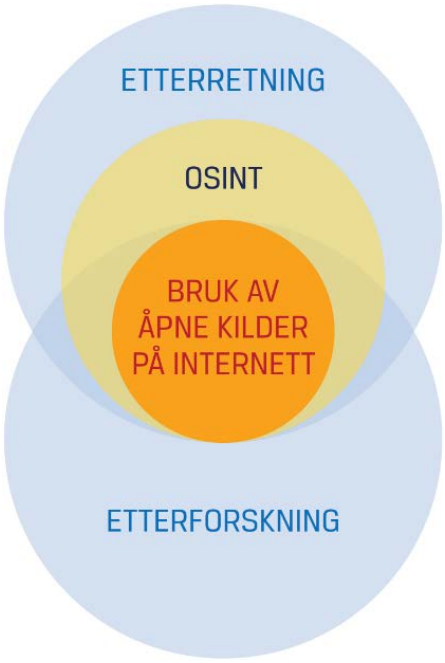
Resten av dette kapittelet deles i underoverskrifter etter setningsoppbyggingen i definisjonen, med det unntak at begrepet «politimessige formål» virker hensiktsmessig å starte med, slik:

2.2. Politimessige formål, 2.3. Metoder, 2.4. Innhenting, 2.5. Åpent tilgjengelig, 2.6. Informasjon på internett.

[4] https://www.politiet.no/om/organisasjonen/sarorganene/kripos/kripos-hovedarbeidsomrader/

2.2. Politimessige formål

Bruk av åpne kilder på internett er et verktøy som er aktuelt for hele politietaten, ikke bare etterforskning. Begrepet politimessige formål defineres i politiregisterloven (2010) § 2 nr. 13 som: «politiets kriminalitetsbekjempende virksomhet, herunder etterforskning, forebyggende arbeid og ordenstjeneste, politiets service- og bistandsfunksjon samt føring av vaktjournaler». Kriposveilederen (ibid.) skiller mellom bruk av åpne nettkilder til etterforskning og etterretningsdisiplinen «OSINT» - et engelsk akronym for «Open Source Intelligence». OSINT begrepet brukes i flere land og fagmiljøer, både innen militær- og politiorganisasjoner, så vel som i sivile bransjer innen media og teknologi. OSINT er opprinnelig et etterretningsbegrep, og referer til et mye videre omfang av åpent tilgjengelig informasjon, også fra åpne kilder utenfor internett (Steele, 2009). Siden OSINT favner så vidt, er det ikke ensbetydende med Kripos sin definisjon av politiets bruk av åpne internettkilder. Figur 1 illustrerer forholdet mellom etterretning, OSINT, åpne internettkilder og etterforskning.



Figur 1 – Forholdet mellom etterretning, OSINT, åpne internettkilder og etterforskning (Kripos, 2018)

Dette skillet er viktig å presisere fordi lovverket regulerer politiets etterretningsarbeid annerledes enn etterforskning. Etterretning er ikke et lovbestemt begrep som det av rettslige grunner er nødvendig å klarlegge i detalj i denne sammenheng (Riksadvokaten, 1999, s. 3). Etterforskning på sin side, defineres i straffeprosessloven (1981) § 226, hvor det listes hvilke mulige formål etterforskning kan ha: å avgjøre spørsmål om tiltale, forberede rettens

behandling av skyldspørsmål og eventuell reaksjon, avverge eller stanse straffbare handlinger, fullbyrde straff og andre reaksjoner, gjøre undersøkelser for videre behandling i barnevernet eller i konfliktrådet.

Riksadvokaten (1999) utfyller og støtter opp om § 226 ved å si at det er formålet med en politiaktivitet som avgjør hvorvidt det er etterforskning, ikke typen aktivitet i seg selv. Alle undersøkelser av åpne kilder på internett som politiet gjør med noen av formålene fra straffeprosesslovens § 226 er altså å regne som etterforskning. Dette har betydning for hvem som har det overordnede ansvaret for virksomheten – altså påtalemyndigheten ved Riksadvokaten, ikke Justis- og beredskapsdepartementet. Søk på åpne internettkilder som etterforskningsmetode kan da også utløse bestemmelser i straffeprosessloven og påtaleinstruksen om habilitet, taushetsplikt, klage, vitneplikt, innsyn (for mistenkte) og underretning om påtaleavgjørelser, og stiller krav til at politiet har notoritet på de søkene som gjøres som del av en etterforskning (Riksadvokaten, ibid.).

2.2.1. Empirikonsekvens: etterforskning eller etterretningsvirksomhet

Skillet mellom etterforskning og etterretning kan fremstå som uklart i praksis. Det kan dukke opp spørsmål blant etterforskerne om hvorvidt søk de gjør på åpne nettkilder er å regne som etterforskning, eller om de ser på det som mer innledende undersøkelser og bakgrunnsinformasjon som ikke kreves inntatt i sakens dokumenter eller føres notoritet på. Det kan dermed være både etisk og juridisk utfordrende dersom politiet foretar søk på åpne kilder i en etterforskning og ikke dokumenterer dette – betydningen av notoritet drøftes nærmere under begrepet «innhenting» i del 2.4.2.

2.3. Metoder

Kriposveilederen (ibid.) spesifiserer begrepet metoder som de innhentingsmåter, teknikker, prosedyrer og verktøy som benyttes for å søke frem, identifisere, sikre og lagre informasjon fra internett.

Søk på åpne kilder på nett kan metodisk ses som en variasjon av politispaning (Bjerknes, Fahsing, & Bergum, 2018), hvor politiet samler informasjon gjennom diskret observasjon av offentlige steder eller følger enkeltpersoners bevegelser. I likhet med tradisjonell spaning er søk på åpne kilder en såkalt ulovfestet metode, juridisk hjemlet i den såkalte alminnelige handlefrihet. Metodekontrollutvalgets nasjonale offentlige utredning (2004, s. 45) beskriver den alminnelige handlefrihet slik:

> *Alle har i utgangspunktet rett til å oppholde seg i det offentlige rom. De har også rett til å lese aviser og eventuelt klippe ut og lagre den informasjon som står der. (...) Det tradisjonelle syn har vært at politiet uten lovhjemmel kan gjøre det samme.*

Den alminnelige handlefrihet tilsier altså at politiet uten lovhjemmel kan oppholde seg i offentlige rom og observere og notere seg det som skjer der. To av medlemmene i Metodekontrollutvalget, Ingvild Bruce og Geir Sunde Haugland, skriver i sin bok (2014) om forventningsprinsippet: I hvilken grad vi i en gitt situasjon rimelig kan forvente at våre handlinger overvåkes eller registreres. Jo lenger ut i en allment tilgjengelig sfære man beveger seg, jo mindre inngripende vil overvåkning oppleves.

2.3.1. Offentlig rom og privat sfære

Når man snakker om internett som et offentlig rom, tar forventningsprinsippet en litt annen form. Internett blir en boble av offentlighet midt i hjertet av den private sfæren. Normen og forventningen kan på den ene siden være at både privatpersoner, kommersielle interesser og andre aktører i prinsippet kan observere det man foretar seg på det åpne internettet, selv om man fysisk ligger hjemme på sofaen. Annabelle Lever (2016, s. 138) argumenterer på sin side at forventningsprinsippet i det digitale rom mer komplekst enn bare skillet mellom offentlig og privat sted:

> *If we would be troubled by the routine presence of unidentified police officers in health-clinics or public libraries, we should be uncomfortable with the suggestion that no special justification or supervision is required for police scrutiny of, and participation in, debates on public websites.*

Levers argumenterer for at den alminnelige handlefrihet har sine begrensninger, også på internett, og særlig for staten. Metodekontrollutvalget anerkjente i sin rapport fra 2004 lignende innsigelser fra henholdsvis Eckhoff (1979) og Garver (2002) – at når staten overvåker en, er det mer ubehagelig enn tilsvarende observasjon gjort av for eksempel naboen. Levers sitat over problematiserer også når politiets tilstedeværelse i det offentlige rom på internett foregår skjult. Videre ser vi på noen konsekvenser dette kan ha.

2.3.2. Skjulte søk

Politiet har et uttalt mål om økt synlig tilstedeværelse og publikumskontakt på internett (Politidirektoratet, 2017), og har innført tiltak som for eksempel nettpatruljer[5]. Men selv om nettpatruljer både kan og bør benytte åpne internettkilder i sitt forbyggende og tillitsskapende arbeid, er det tilfeller hvor politiet bør skjule søk på åpne kilder som gjøres i pågående etterforskninger. Ett hensyn vil være operasjonell sikkerhet - at politiet har kontroll med når og hvordan en person får vite at de er under etterforsking. Svikt i operasjonell sikkerhet kan føre til at bevis går tapt eller blir forspilt av personer som ønsker å motarbeide etterforskningen (Kripos, 2018).

Et annet argument for å skjule internettaktiviteten sin er risiko for angrep; fra tilfeldige virus, til en motpart som kartlegger bevegelsesmønstre og gjennomfører mer målrettede cyberangrep. Alle politiansatte som driver med åpne kildesøk, både åpne og skjulte, bør bruke datamaskiner og enheter som ikke er direkte tilknyttet politiets øvrige nettverk for å redusere risikoen for slike angrep (Conteh & Schmick, 2016). Av samme hensyn bør heller ikke ansatte i politiet benytte profiler og enheter som kan knyttes til dem som privatpersoner når de gjør søk på åpne kilder til politimessige formål.

Den amerikanske sosiologen Gary Marx (1988) illustrerer politiets åpne og skjulte arbeidsformer ved å sette dem på de to aksene synlig/skjult og sannferdig/forledende. Den norske utgaven av Marx sin fremstilling er hentet fra Asbjørn Rachlews Phd-avhandling (2009, s. 124) og gjengitt i tabell 1:

POLITIETS HANDLING	Sannferdig	Forledende
Synlig	a) Åpen etterforskning	b) Løgn og manipulasjon
Skjult	c) Observasjon / overvåkning	d) Infiltrasjon og informantbehandling

Tabell 1 – Marx' modell av politiets virksomhet

Rachlew kommenterer i sin avhandling at Marx' modell gjør det enklere å forholde seg til de ulike handlingene politiet gjør ved å stille spørsmålene: Opptrer politiet sannferdig, eller forleder de publikum? Opptrer politiet åpent, eller skjuler det seg?

[5] https://www.politiet.no/aktuelt-tall-og-fakta/aktuelt/nyheter/2018/09/04/politiets-nettpatrulje-oslo-er-lansert/

Dersom politiet benytter en uniformert profil til sine åpne kildesøk, slik som nettpatruljen nevnt tidligere, vil det falle under kategori a) i tabellen. Dette er søk politiet ønsker skal være synlig. Eksempelvis at en uniformert profil fra politiet melder seg inn i grupper på sosiale media som uttrykker ekstremistiske holdninger. Synlig tilstedeværelse og dialog og kan tenkes å ha en forebyggende effekt – også på medlemmer i gruppen politiet ikke når direkte.

For å forstå kategori b) i Marx' modell, kan vi tenke oss at nettpatruljen i forrige eksempel delte falsk eller misvisende informasjon i gruppene de har fått innpass i, i håp om å skape interne konflikter og redusere samhandling eller medlemstall i gruppa. Selv om det kunne svekket gruppene på kort sikt, ville slike tilnærminger over lengre tid kunne undergrave allmennhetens tillit til politiet. Rachlew (ibid.) viser til forbudet mot at politiet bruker løfter, uriktige opplysninger, trusler eller tvang under avhør[6], og utleder fra dette at norsk politi generelt ikke kan forlede ved løgn og manipulasjon når det opptrer synlig.

Dersom politiet derimot skjuler sin identitet i kontakt med andre, kan det være lovlig å forlede under reglene for infiltrasjon og informantbehandling, som illustrert under kategori d) av Marx' modell. Dette er etterforskningsmetoder underlagt Riksadvokatens ansvar, som øverste myndighet for hvordan etterforskning utføres (som nevnt i del 2.2). Riksadvokaten definerer infiltrasjon slik (2018, s. 6):

> *«Med infiltrasjon menes (...) at politiet samler informasjon ved å ha direkte kontakt med enkeltpersoner, herunder ved å innarbeide seg i ulike miljøer, uten å gi seg til kjenne som polititjenestepersoner eller en som opptrer på vegne av politiet. Som infiltrasjon regnes også overtakelse av en annens identitet eller rolle på internett.*

Altså kan politiet opptre forledende i sin direkte kontakt med andre, så lenge de samtidig ikke påberoper seg å være politi. Infiltrasjon regnes som en mer inngripende metode enn søk på åpne kilder. Infiltrasjon beskrives ikke i større detalj her, men generelt er vilkårene for bruk strengere, og er underlagt kontroll fra påtale og domstol.

Den gjenværende kategorien i Marx' modell er da c) observasjon og overvåking. Her opptrer politiet skjult, men forleder ikke aktivt i direkte kontakt med en motpart. Vi ser at spaning, som beskrevet i del 2.3, passer denne beskrivelsen. Riksadvokaten (ibid., side 2) trekker grensen mellom infiltrasjon og spaning slik:

> *Infiltrasjon har (...) en nedre grense mot ulike former for spaning, som kjennetegnes ved at politiet mer passivt samler informasjon ved å være fysisk eller*

[6] I følge straffeprosessloven (strpl.) § 232, 2. ledd, jf. § 92, 2. ledd og påtaleinstruksen § 8-6, 6. ledd

> *virtuelt tilstede, men uten å ha direkte kontakt av noe særlig omfang med den som observeres».*

Riksadvokaten skiller altså infiltrasjon fra spaning ved å definere sistnevnte som mer passiv innhenting av informasjon. Gjennom den den teknologinøytrale formuleringen «fysisk eller virtuelt tilstede» dekkes også skjulte søk på åpne internettkilder under spaningsbegrepet, slik som Bjerknes et al. (2018) i del 2.3. det er altså en begrepsforskjell mellom Marx' modell, hvor skillet går mellom sannferdig og forledende handling, og Riksadvokatens direkte kontakt og passiv innsamling, men begge synes å beskrive den samme dynamikken.

I praksis vil da en etterforsker som søker på åpne kilder med en nøytral nettprofil uten polititilknytning gå over til infiltrasjon idet hun går i direkte kontakt med enkeltpersoner eller aktivt innarbeider seg i miljøer eller grupper uten straks å gi seg til kjenne som polititjenesteperson. En klar forståelse av disse grensedragningene fremstår som essensiell for å sikre at metodebruken er hjemlet i lovverket.

2.3.3. Ulovlige søk

Noen typer søk på åpne kilder er det ikke tilstrekkelig å skjule. Av hensyn til taushetsplikten politiet er underlagt[7], bør de ikke foretas i det hele tatt. Politiregisterloven (2010, § 23) er særlig veiledende i denne sammenheng:

> *Enhver som er ansatt i eller utfører arbeid for politiet, plikter å hindre at andre får adgang eller kjennskap til det man i forbindelse med tjenesten eller arbeidet får vite om noens personlige forhold. Taushetsplikten gjelder også for opplysninger som det ut fra hensynet til etterforskningen i den enkelte sak, hensynet til spanings- og etterretningsvirksomheten eller hensynet til politiets operative virksomhet og organiseringen av denne er nødvendig å holde hemmelig.*

Søk foretatt i åpne nettjenester så som søkemotorer, sosiale medier, bildesøk, kartsøk, språkoversettelser og andre former for automatiserte spørringer over internett kan komme ut - for eksempel ved lekkasje eller datainnbrudd hos leverandørene av slike tjenester eller deres samarbeidspartnere. Taushetsbelagt eller annen sensitiv informasjon kan derfor ikke benyttes i slike spørringer (Kripos, 2018). Eksempelvis kan ikke politiet bruke søkemotorer på det åpne internettet for reverserte video- og bildesøk på personlig materiale beslaglagt fra en person. Ei heller materiale som er sensitivt av andre grunner, som for eksempel overgrepsmateriale. Selv om et slikt søk kunne tenkes å gi verdifull informasjon på en enkel måte, ville man løpe risikoen for utilsiktet eller ulovlig spredning av materialet man søker på.

[7] Politiregisterloven kapittel 5 og 6 regulerer politiets taushetsplikt i straffesaksarbeid

Av samme grunn kan ikke politiet benytte allment tilgjengelige språktjenester på internett for å oversette dokumenter eller tekst som ville regnes som brudd på taushetsplikten dersom innholdet ble gjort tilgjengelig for uvedkommende.

2.3.4. Empirikonsekvens: grenseganger til skjulte metoder

Litteraturen referert til i dette kapittelet (Bruce & Haugland, 2014; Politidepartementet, 2004; Rachlew, 2009; Riksadvokaten, 2018) illustrerer at skjulte etterforskningsmetoder er tydelig definert innen etterforskning. Som vi har sett, grenser søk på åpne kilder til den skjulte etterforskningsmetoden infiltrasjon. Hvor infiltrasjon er lovregulert, anses søk på åpne kilder som en variasjon av spaning, og er ikke lovregulert. Dette kan føre til at noen etterforskere ser søk på åpne kilder under samme kategori som skjulte etterforskningsmetoder, og føre til at man unngår å bruke dem fordi man ikke tror det er hjemmel for å slik metodebruk i den aktuelle saken. Motsetningsvis kan empirien vise tilfeller hvor etterforskere har gjort søk på åpne kilder med nøytrale profiler, tatt direkte kontakt med personer uten å tilkjennegi seg som politi, og dermed krysset over grensen til infiltrasjon uten at man er bevisst på dette.

2.4. Innhenting

Kriposveilederen (ibid.) utdyper ordet innhenting slik det brukes i definisjonen som søk, sikring og lagring av informasjon fra internett. Behovet for å koordinere lovverk og kunnskap om datainnhenting til kriminalitetsbekjempelse har vært et internasjonalt anerkjent i flere tiår. I 2001 gav det opphav til den første internasjonale konvensjonen om cyberkriminalitet (Clough, 2014). Den er kjent som Budapestkonvensjonen (Europarådet, 2001), og ble ratifisert og trådte i kraft i Norge i 2006[8]. Konvensjonen sier følgende om innhenting (artikkel 32, litra a, s. 17): "A Party may, without the authorisation of another Party access publicly available (open source) stored computer data, regardless of where the data is located geographically". Så lenge data er offentlig tilgjengelige, uavhengig av hvor de er lagret geografisk, har altså enhver adgang til dem uten å måtte innhente noen videre tillatelse. Vi ser parallellene til den metodiske drøftingen om politiets rett til å gjøre observasjoner i det offentlige rom (se del 2.2.1). Budapestkonvensjonen bidrar på samme måte til et formelt juridisk grunnlag for politiets datainnhenting fra åpne kilder på internett. Men kan denne økte tilgjengeligheten til data utgjøre en utfordring?

[8] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

2.4.1. Tilgjengelighet og retten til å bli glemt

Datamengden kombinert med at informasjon sjelden forsvinner når den først har funnet veien til internettet, kan i seg selv være en utfordring i innsamlingen og tolkingen av data fra åpne kilder. Det kan være vanskelig å avgjøre om man finner «hele bildet» (Minas, 2010) – eller om man blir misledet i et «ekkokammer», hvor tilsynelatende bred enighet om et tema i realiteten er flere kilder som refererer til samme subjektive enkeltkilde (Eijkman & Weggemans, 2012).

Bruce & Haugland (2014) påpeker konsekvenser av å sette informasjonsbiter man samler inn i en større helhet. Enkeltstående opplysninger trenger ikke være sensitive, men ved å sammenstille informasjon fra ulike kilder, vil ende opp med et bilde som er langt mer detaljert, intimt og kompromitterende enn det personen som gav opplysningene vil være komfortabel med. Dette er det Inge Marie Sunde (2013) omtaler som «Økosystemeffekten». Selv om Sunde primært omtaler retten til personvern borgene har ovenfor hverandre, har hennes argument om «retten til å bli glemt» også stor relevans for hvordan politiet vurderer informasjon de samler inn fra åpne kilder på internett, der data nærmest aldri blir slettet. EUs personvernforordning (ofte kalt GDPR, utdypes i del 2.5.1), som ble innført i Norge i 2018, har tydelige reguleringer for å ivareta retten til å bli glemt, slik at også lovgivers intensjon på dette spørsmålet er tydelig. Alle som samler inn og behandler åpent tilgjengelige data bør derfor ta høyde for retten til å bli glemt i sine analyser og eventuelle presentasjoner.

2.4.2. Notoritet – rettssikkerhet og tillit

Riksadvokaten (1999) presiserer at det skal være notoritet på all etterforskning politiet foretar seg, uavhengig av om den leder til opprettelsen av en straffesak eller ei. Dersom politiet foretar søk på åpne internettkilder med etterforskningsformål, må det altså finnes notoritet for dette i ettertid, også fordi personene man søker på eventuelt siden skal kunne få innsyn i hvilken informasjon politiet samlet om dem.

«If you don't write it down, it didn't happen» skriver John Sammons (2015, s. 51) når han beskriver viktigheten av å føre fortløpende notater om datatekniske undersøkelser. Slik notoritet vil også være viktig når en etterforsker søker på åpne kilder – særlig dersom undersøkelsene får betydning som bevis i retten. Ved for eksempel å føre en nøyaktig logg over tidspunkt, søkeord, skjermbilder og fremgangsmåter, vil andre enn politiet kunne se hva som er gjort, påpeke eventuelle mangler og kunne gjenskape undersøkelsen for å se om de får

samme resultat. Dette vil kunne styrke bevisverdien av undersøkelsene spesielt, og politiets metoder generelt. Motsatt vil utilstrekkelig eller manglende notoritet i bruken av åpne kilder kunne svekke tilliten til at politiet forvalter innhenting av åpent tilgjengelig informasjon på en forsvarlig måte.

2.4.3. Empirikonsekvens: informasjonsoverflod og manglende notoritet

Mengden tilgjengelig informasjon kan virke avskrekkende for etterforskere, og dermed bli et tema i den empiriske undersøkelsen. Utfordringen med store datamengder vokser i takt med lagringskapasiteten på de elektroniske databærerene politiet beslaglegger som potensielle bevis (Sunde, 2015). Det kan derfor være en stor nok utfordring for en etterforsker å analysere data tatt i beslag, om man ikke skal måtte analysere åpne kildedata fra internett i tillegg.

Som nevnt innledningsvis i del 1.2., kan bekvemmeligheten og brukervennligheten av åpne kilder lede til at man bare «tar et kjapt søk for å sjekke», uten at man dokumenterer slike søk i saken. Usikkerhet om grensegangen til etterretning og mer regulerte etterforskningsmetoder som infiltrasjon, kan være en årsak til underrapportering av åpne nettkildesøk til etterforskningsformål.

2.5. Åpent tilgjengelig

Når det gjelder hvilken type informasjon som er regnet som åpent tilgjengelig, viser Kripos sin veileder (ibid.) til straffeloven (2005, §10) sin definisjon av offentlig sted og offentlig handling:

> *«Med offentlig sted menes et sted bestemt for alminnelig ferdsel eller et sted der allmennheten ferdes. En handling er offentlig når den er foretatt i nærvær av et større antall personer, eller når den lett kunne iakttas og er iakttatt fra et offentlig sted. Består handlingen i fremsettelse av en ytring, er handlingen også offentlig når ytringen er fremsatt på en måte som gjør den egnet til å nå et større antall personer».*

Kriposveilederen (ibid.) supplerer at nettsteder som begrenser tilgang ved for eksempel å kreve betaling eller opprettelsen av en brukerkonto og passord også regnes som åpne kilder, forutsatt at enhver uten videre kan skaffe seg slike tilgangsrettigheter. Som eksempel vises det til arkivtjenesten Retriever[9], som gjør tilgjengelig artikler fra publikasjoner fra mange tiår

[9] https://www.retriever.no/

tilbake. Selv om tjenesten koster penger regnes den fortsatt som en åpen kilde, fordi alle i prinsippet kan kjøpe seg tilgang. Mange av de mest utbredte sosiale medier – som for eksempel Facebook, Instagram og Snapchat – er gratis, men krever en e-postadresse i opprettelsen av profil for å få tilgang til å søke opp andre brukere og ta del i tjenesten. En e-postadresse kan imidlertid opprettes uten videre rettigheter eller tilganger, og disse sosiale mediene defineres derfor også som åpne kilder.

2.5.1. Nedkjølingseffekten

Uansett hvor lovlig befestet og forventet den er – kan overvåkning og systematisk informasjonsinnhenting av åpent tilgjengelig informasjon ha negative effekter? «Nedkjølingseffekten» argumenterer for at det er tilfelle. Nedkjølingseffekten har sin opprinnelse fra et USA engasjert i kald krig på 50- og 60-tallet, hvor flere domstolsavgjørelser ble avsagt ut i fra idéen om at enkelte handlinger av staten kan «kjøle ned» eller avskrekke borgernes lovlige uttrykk av meninger eller utøvelse av friheter (Penney, 2016). Nedkjølingseffekten ble tidlig forsket på av Frederick Schauer (1978). Han beskriver nedkjøling som folks frykt for å bli anklaget av staten, kombinert med en mistro til rettsvesenets evne å beskytte deres uskyld. Så selv om en praksis er definert som lovlig, kan den utøves på en måte som allment oppleves som et overtramp, eller ikke står i samsvar med publikums forventinger til sine myndigheter.

I senere tid har forståelsen av nedkjølingseffekten blitt utvidet til å inkludere overvåkning og datainnsamling på internett. Frykten assosiert med denne moderne nedkjølingseffekten er at sensitiv data samlet inn om en selv skal misbrukes enten av den som samlet den inn eller ved lekkasje til tredjepart – med påtvungen konformitet og selv-sensur på internett som en konsekvens (NorSIS, 2018; Solove, 2005). Her kan man også se likheter med retten til å bli glemt, som drøftet under del 2.4.1.

Kira Vrist Rønn & Sille Obelitz Søe (2019) problematiserer også at myndighetene kan oppfattes å utnytte generell uvitenhet blant folk om hvordan mange internettjenester faktisk fungerer. Innstillingene for hvem som kan se informasjon man legger ut på sosiale medier kan for eksempel være vanskelige å både finne og forstå for mange av oss, og de færreste har nok lest, langt mindre forstått, sluttbrukeravtaler i sin helhet når man installerer programvare eller besøker en nettside. Mange vil altså dele data i god tro om at den kun kan ses av en lukket forsamling. Denne tanken uttrykkes også i GDPR ved at det stilles krav til at avtaler en tjenestetilbyder forholder sine brukere skal være «forståelig for målgruppen, og ha klart språk

og god struktur» (Datatilsynet, 2018). Solove (2008) argumenterer at selv uten komplekse brukeravtaler, vil folk godta at sensitive data samles inn simpelthen fordi de ikke vil være blant minoriteten, utelatt fra fellesskapet og kommunikasjonen som det moderne informasjonssamfunnet tilbyr. Dette kan bety at det ikke er et reelt og frivillig samtykke for delingen av all den informasjonen man kan finne på åpne kilder. Og at lovlighet alene ikke garanterer allmenn aksept blant befolkningen til at myndigheten kan samle inn og bruke slik informasjon til et annet formål enn det den opprinnelig var tiltenkt.

2.5.2. Empirikonsekvens: lite fokus på etiske hensyn

Problematiseringen av statens utnyttelse av offentlig tilgjengelig data om mennesker, kan være vanskelig å ta inn over seg – nettopp fordi dataen *er* offentlig tilgjengelig. Som etterforsker, var jeg selv ikke bevisst på at samtykket til å dele persondata kanskje ikke er så fritt i praksis, hvis prisen for å ikke samtykke til brukeravtaler er ekskludering fra store sosiale arenaer og informasjonskanaler. Jeg ble ikke fullt oppmerksom på at dette kan påvirke undersøkelsene jeg gjør på jobb før jeg var godt i gang med denne avhandlingen. Det vil ikke være urimelig å forvente at andre etterforskere, kanskje de fleste jeg prater med, ikke ser slike problemstillinger heller.

2.6. Informasjon på internett

I Kriposveilederen (ibid.) sin definisjon forstås informasjon som alle former for opplysninger i alle formater, inkludert alle former for bærere av opplysninger, formidlingssystemer for opplysninger og fragmenter av opplysninger. Informasjon vil i denne sammenhengen også kunne innbefatte overordnede strukturer som enkeltnettsider, domener og nettverksarkitektur. Informasjon kan også være metadata, altså opplysninger om dataene i en fil som oftest ikke er umiddelbart synlige for brukeren (Brand, Daly, & Meyers, 2003). Også informasjon om datasystemer, som internettadresser og domenenavn, vil falle inn under informasjonsbegrepet.

Internett i denne definisjonen omfatter alle deler av nettet der det kan finnes åpent tilgjengelig informasjon, uavhengig av tilgangsmetode. Altså både via tradisjonelle nettlesere på datamaskiner, så vel som mobiletelefoner og tilhørende applikasjoner. Politiet bør også kunne lete etter åpent tilgjengelig informasjon på det som kalles «det dype nettet» - deler av internett som er passivt skjult, fordi det ikke omfattes av kommersielle søkemotorer – så vel som på «det mørke nettet» - deler av det dype nettet som er aktivt skjult ved kryptering og

anonymisering av både nettsider, brukerne og deres aktiviteter[10]. Det mørke nettet eksemplifiseres ofte ved markedsplasser for overgrepsmateriale, narkotika og ulovlige våpen, men er også et verktøy for informasjonsfrihet og meningsytring for mennesker under diktatoriske regimer (Gehl, 2016).

2.6.1. Personvern

Innsamling og bruk av persondata fra internett av ulike kommersielle, politiske og offentlige aktører begynner å bli allmennkunnskap, om ikke nødvendigvis allment akseptert, som nevnt i del 2.5.1. Flere studier har vist at vi har sterke forventninger til vern og eierskap av våre personlige data eller personopplysninger, selv om den dataen faktisk er offentlig tilgjengelig (Boyd & Marwick, 2011; Lüders, 2011; Walther, Van Der Heide, Kim, Westerman, & Tong, 2008). Enhver diskusjon om politiets informasjonsinnhenting fra åpne internettkilder ville vært ufullstendig uten å inkludere personvernhensyn.

Juridisk er personvernet i dag omfattende regulert, både gjennom norsk lov[11] og internasjonale forpliktelser[12]. Selv om det har eldre røtter i filosofi og samfunnsvitenskap, brukes personvernbergrepet i dag oftest som et juridisk begrep i Norge, tradisjonelt med analyser av hvor vi setter grensene for statens legitime innblanding i private liv og hva slags informasjon borgerne er pliktige å gi til hvem (Norges offentlige utredninger, 2009).

Behovet for privatliv og en privat sfære hvor vi kan være i fred fra andre er en naturlig del av sosiale interaksjoner i alle samfunn. Innholdet i personvernbegrepet vil altså endres sammen med den øvrige samfunnsutviklingen (Moor, 2006). Hurtige teknologiske fremskritt og fremveksten av sosiale medier har i senere tid utvidet personvernet til å inkludere hvordan våre personopplysninger behandles. Personopplysninger defineres i GDPR (også kalt EUs personvernforordning i norsk lovverk) artikkel 4[13]:

> *Enhver opplysning om en identifisert eller identifiserbar fysisk person (...) en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet.*

[10] https://coar.risc.anl.gov/coar-attends-department-of-homeland-security-hosted-darknet-summit/
[11] Lov om behandling av personopplysninger (Personopplysningsloven) av 2018
[12] Europeiske menneskerettighetskonvensjonen (EMK) av 1950, særlig artikkel 8
[13] https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

Datatilsynet utfyller definisjonen ved å spesifisere at opplysninger om atferdsmønstre, som hvor du fysisk beveger deg i løpet av en dag og hva du søker etter på nettet, også er personopplysninger[14]. Datatilsynet gjør dette for å møte en av de nye utfordringene til personvernet i den digitale tidsalder - nemlig omfanget av spor vi etterlater oss på internett, ofte uten å vite om det eller tenke på det. Det vil ofte være disse digitale fotsporene politiet ønsker å dra nytte av i etterforskningsarbeid gjennom søk på åpne kilder. Det at åpne kilder gir en ulovfestet og forholdsvis enkel tilgang på disse fotsporene, kan medføre at de håndteres på en mindre strikt måte enn øvrige personopplysninger og annen informasjon tilegnet gjennom etterforskningsmetoder som er underlagt strengere regulering eller hemmelighold (Cross, 2011).

2.6.2. Empirikonsekvens: behandling av personopplysninger

Forsvarlig behandling av personopplysninger er noe som kreves i alle etterforskninger, uavhengig av kilde og innsamlingsmetode – pasientjournaler etter formell anmodning til et sykehus, straffehistorikk fra politiets egne systemer eller personbilder fra en Facebook-profil etter åpne kildesøk. Det kan derfor forventes at de fleste som jobber med etterforskning ikke vil problematisere sin håndtering av personopplysninger.

Samtidig virker det rimelig å se behandling av personopplysninger i sammenheng med hvilken notoritet politiet fører over søk på åpne kilder. Fordi uten oversikt over når, hvor, hvordan, hvorfor og hvem man har søkt etter, vil det nemlig være umulig å garantere senere innsyn for berørte personer, eller at personopplysninger som resulterer av søkene behandles i henhold til regelverket.

3. Metode

«What you ask, how you ask it and who you ask can determine the difference between novel insight and wasted time" (Lazar, Feng, & Hochheiser, 2010, s. 178).

Å redegjøre for designet av forskningsprosjektet og de metodiske veivalgene jeg har gjort er temaet i dette kapittelet. Hensikten er gi andre innsikt i hvordan jeg har generert de dataene som ligger til grunn for analysen og de funn som presenteres i neste kapittel. Ved å bruke

[14] https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/

forskningsmetoden fokusgrupper intervjuet jeg 4 grupper, bestående av totalt 22 politiansatte som jobber med etterforskning til daglig. Jeg rekrutterte intervjugruppene gjennom et opplæringsprogram innen etterforskning som politiet innførte nasjonalt i 2018.

Kapittelet er inndelt i underkapitler, som hvert representer valg og andre faktorer jeg mener har påvirket prosjektet. Rekkefølgen er mest mulig lik kronologien i min faktiske arbeids- og beslutningsprosess. Først beskrives idéopphavet for temaet, utviklingen fra konsept til et prosjektdesign som var mulig å gjennomføre for én forskernovise. Neste del tar for min forforståelse og deretter valget av forskningsmetode, etterfulgt av betraktninger om det som kalles aksjonsforskning. Så gjennomgås strategien min for å finne intervjudeltakere. Deretter beskrives teori jeg har brukt fra feltet teknologiakseptanse, intervjuguiden utarbeidet fra dette, og hvordan guiden fungerte i praksis under selv gjennomføringen. Avslutningsvis gjøres noen refleksjoner om hvordan mine personegenskaper påvirket undersøkelsen og øvrige etiske betraktninger om prosjektet. Helt til slutt beskrives metodikken jeg benyttet for å omdanne lyd- og videopptak fra gruppeintervjuene til data for koding og analysering.

3.1. Prosjektdesign

Idéen for avhandlingen ble i hovedsak til da jeg var på et par ukers hospitering høsten 2016 ved Kripos sin seksjon for internettrelatert etterforskningsstøtte (forkortet IRES). Hospiteringen var, i likhet med denne avhandlingen, en del av Politihøgskolens mastergradsprogram innen etterforskning. IRES jobbet i denne perioden med å utvikle metodikk for politiets bruk av åpne kilder på nett, og jeg fikk gjennomføre test-versjonen av et kurs i åpne kildesøk med IRES sine fagspesialister. Jeg fikk øynene opp for søk på åpne nettkilder som et verktøy med stort potensiale for etterforskningsfaget, ikke minst fordi det ikke krever spesialkompetanse. Metoden kan i prinsippet brukes av alle som driver med etterforskning, siden bruk av sosiale medier og informasjonssøk på nett har blitt hverdagskunnskap for de aller fleste, inkludert politiansatte.

At søk på åpne kilder er så likt hverdagslig internettbruk til private formål, tror jeg var grunnen til at jeg før IRES-kurset ikke anså det som en legitim etterforskningsmetode. Informasjonen man finner er jo åpent tilgjengelig for alle andre også, og det gjør det kanskje lett å derfor lett å undervurdere verdien av den. Etter kurset om åpne kilder, og ettersom jeg orienterte meg i litteraturen, begynte jeg også å forstå åpne kilders begrensninger og de prinsipielle etikkspørsmålene som drøftes i teorikapittelet. Jeg begynte å lure på hvor mange av mine kollegaer som tenker slik jeg gjorde? Hvor mange brukte åpne nettkilder til

etterforskning, uten å se det som en etterforskningsmetode, med tilhørende juridiske og etiske grenser? Eller var det vanlig å avfeies åpne kildesøk med tanken om at det neppe kan ligge særlig verdi i informasjon som er lagt ut offentlig for alle å se?

Første design var derfor en kvantitativ studie for å kartlegge politiets kunnskapsnivå og bruk av åpne internettkilder på landsbasis. En slik studie kunne støtte opp om arbeidet politiet nå gjør for å implementere en beste praksis og kunnskapsbase for etterforskning på internett. Jeg synes fortsatt at en slik kartlegging vil kunne være et nyttig forskningstema, som kan hjelpe nasjonal implementering og opplæring i bruk av åpne internettkilder. Men høsten 2017, ett års tid etter IRES hospiteringen og arbeidet med prosjektdesign var i gang for mitt vedkommende, fikk jeg flere e-poster adressert til hele eller store deler av politietaten. Det var spørreundersøkelser for kartlegging og evaluering av den pågående politireformen[15], med flere purringer grunnet lav svarprosent. Risikoen fremstod da som betydelig for at spørreundersøkelsen jeg hadde tenkt å sende ut på sammen måte nok kunne forsvinne i mylderet, eller ignoreres av utslitte respondenter (Bradley & Daly, 1994). Med den konsekvensen at svarprosenten ville bli så lav at de resulterende dataene ville bli vanskelige å jobbe videre med.

Beslutningen om å forkaste det kvantitative survey-formatet satt ganske langt inne for meg. Men etter gode råd fra veileder og andre som hadde erfaring med kvalitative studier, begynte jeg å se fordelene ved en mer fenomenologisk tilnærming. Som et kvalitativt forskningsdesign innebærer fenomenologien «å utforske og beskrive mennesker og deres erfaringer med, og forståelse av, et fenomen», ifølge Johannessen, Christoffersen og Tufte (2010, s. 82). De viser til at datainnsamlingen i slike prosjektdesign gjerne gjøres gjennom dyptgående intervjuer av individer med tilknytning til fenomenet man vil utforske. Men når jeg vurderte bruken av dybdeintervjuer så innså jeg at det ikke harmonerte en oppfatning jeg hadde formet tidligere – at åpne internettkilder burde bli en metode for alle som driver med etterforskning, ikke kun de med størst tilknytning og kunnskap om metoden i dag. Dette kalles også forforståelse, og kan bygge på faglitteratur, egne erfaringer eller andre undersøkelser (Holter, 1996). Videre beskrives denne forforståelsens betydning for prosjektdesignet.

[15] https://www.regjeringen.no/no/tema/lov-og-rett/kriminalitet-og-politi/innsikt/narpolitireformen/id2398914/

3.2. Forforståelse

Hospiteringen hos IRES i 2016 bidro til at jeg formet egne oppfatninger om hvordan politiet bør ta i bruk åpne internettkilder. Denne forforståelsen er vanskelig å legge helt bort når jeg senere skal fatte beslutninger om hvordan jeg vil forsk på temaet. Den påvirker, og er kanskje en forutsetning for, både de spørsmålene jeg stiller informantene, så vel som meningene jeg tolker ut av svarer de gir meg. Siden den ikke kan legges bort, er det viktig at den erkjennes (Fog, 2004; Johannessen et al., 2010). Man kan fremme argumentet at jo mindre slik forforståelse jeg har, jo mindre påvirkes mine fortolkninger, som igjen gjør dem mer allmenngyldige. Men forforståelse følger nødvendigvis av læring og engasjement. Uten teorigrunnlaget og de praktiske erfaringene jeg selv har hatt, tror jeg mine forutsetninger for å planlegge, gjennomføre og tolke resultater av en empirisk undersøkelse vill vært dårligere.

Dersom jeg hadde valgt å basere hele det empiriske grunnlaget for avhandlingen på kun et fåtall dybdeintervjuer, ville jeg nok i tillegg følt presset på at hvert dybdeintervju måtte generere tilstrekkelig med brukbare data – som igjen kunne gjøre det fristende å kun prate med eksperter, eller i det minste de menneskene i politiet som allerede er mest motiverte og klare til å bruke åpne kilder. Etter å ha hospitert i et spesialistmiljø, tror jeg at intervjuer med spesialistene ville kunne gitt gode argumenter for hvorfor resten av politiet burde bruke åpne kilder på nett. Jeg hadde jo allerede lest om slike argumenter i faglitteraturen, og hørt dem fra fagmiljøet. Men jeg tror ikke intervjuer jeg kunne gjennomført med dem ville kommunisert de argumentene bedre enn IRES og de øvrige ekspertene allerede gjør selv.

I stedet ville heller se hvilke forutsetninger etterforskere som ikke var en del av spesialistmiljøene innen data og internett hadde for å ta i bruk åpne kildesøk. Synspunkter fra de som etterforsker det store flertallet av straffesaker hver dag, og som kanskje kan utgjøre den største samlede effekten av å systematisk bruke åpne kilder. Forforståelsen min hadde altså på sett og vis utelukket to metoder, nemlig spørreundersøkelse og dybdeintervju. Neste del tar for seg forskningsmetoden jeg endte opp med å bruke.

3.3. Forskningsmetode

Siden jeg hadde valgt bort bredden av et kvantitativt surveydesign, men heller ikke var komfortabel med å gå i dybden gjennom en-til-en intervjuer, fremstod det såkalte fokuserte gruppeintervjuet (Merton & Kendall, 1946), også kalt en fokusgruppe, som en gylden middelvei mellom bredde og dybde på de data jeg ønsket. Her ser vi derfor nærmere på hva

fokusgrupper er, og hvordan jeg tenker denne forskningsmetoden harmonerer med avhandlingens tema, design og problemstilling.

Fokusgruppeformatet brukes til kartlegging av meninger om tema og produkter, populært siden 1950-tallet innen markedsføring og politikk (Merriam & Tisdell, 2016). Fokusgruppens kartlegging skiller seg fra den survey-kartleggingen gjennom spørreskjema jeg først vurderte. Hvor en survey er bra for å generere statistisk data og kan teste forhåndsbestemte variasjoner av et gitt scenario, er fokusgruppen ofte anbefalt for forskning som er eksplorerende – å utarbeide ny innsikt om et smalere tema som er lite dokumentert tidligere (Brandt, 1996; Stewart & Shamdasani, 2014). Eksploreringen kan også tjene som en forundersøkelse som genererer hypoteser som senere kan testes kvantitativt (Johannessen et al., 2010). Slik kan denne metoden kanskje senere kombineres med mitt opprinnelige ønske om en type survey om bruk av åpne kilder i politiet, siden jeg ikke så muligheten til å gjøre det selv ved denne anledningen.

I praksis innebærer fokusgruppen å samle en mindre gruppe mennesker som innenfor en tidsbegrensning diskuterer ett eller flere tema gitt av en moderator. Temaene er fokuset for samtalen, mens formålet er å hente data ut av diskusjonen deltakerne har seg i mellom (Wibeck, 2010). Det kan være en effektiv metode, fordi man får generert data fra flere informanter samtidig (Krueger & Casey, 2015; Tjora, 2012). Dette virket betryggende siden jeg valgte å utelukke ekspertene, og måtte dermed påregne at enkelte informanter kanskje ikke hadde så mye å bidra med i alle diskusjonene.

Meningene fremsatt i en gruppesetting vil kanskje ikke ha samme graden av tillit og intimitet man kan få i et dyptgående en-til-en intervju, men ved å eksponere dem for kritisk diskusjon kan man heve kvaliteten på meningene og begrunnelsene for dem (Nemeth, 2018). Gruppeformatet har også en fordel for de informantene ikke bruker åpne kilder: Det blir mindre anklagende for informantene å drøfte årsaker til ikke-bruk som en gruppe, enn om de skulle sittet i et en-til-en intervju (Barbour, 2014).

3.4. Aksjonsforskning og metodealternativ

Gruppedebatt kan ha en aktiviserende og mobiliserende effekt på deltakerne – skape ny bevissthet og engasjement for temaet utover forskningsprosjektet de bidrar til (Brandt, 1996). Dette samsvarer godt med mitt ønske om å spre bevissthet blant mine kollegaer om potensialet som ligger i åpne kilder til etterforskning. Et så klart ønske om at prosjektet skal

medvirke til en konkret endring av måten å jobbe på, kommer nært det som kalles aksjonsforskning: «Research carried out in an organizational or work setting (often done by practitioners) with the express aim of effecting change» (Barbour, 2014, s. 332).

Fullverdig aksjonsforsking involverer imidlertid organisasjonen eller miljøet som er gjenstand for forskningen mer aktivt over lengre tid enn hva som har vært tilfelle i denne studien. Man snakker nærmest om å forske *sammen*, i stedet for å forske *på* (Wibeck kaller det faktisk deltagendeforskning), og forholdet mellom forsker og en type oppdragsgiver eller interesseaktør er mer formalisert (Wibeck, 2010). Dette prosjektet og jeg har ingen formell relasjon til politidistriktene, utover at jeg oppfyller mine forpliktelser om tillit og konfidensialitet ovenfor de politiansatte som har bidratt som informanter (se 3.9). Det at jeg er en yrkesutøver som forsker på min egen profesjon med en slik endringsagenda får imidlertid også etiske konsekvenser, som omhandles i del 3.9.3.

Barbour (2014) påpeker også at utøverne av aksjonsforskning ofte har spesielt gode tilganger og innsidekunnskap som taler for å bruke observasjon som metode. Observasjon gir førstehåndsdata om en situasjon, i motsetning til annenhåndsbeskrivelser fra intervjudeltakerne: «Observasjon studerer det folk gjør, mens man i intervjuer studerer det folk sier at de gjør» (Tjora, 2012, s. 46). Men i tilfellet åpne kildesøk på nett kan det være vanskelig å fysisk se forskjell på ulike arbeidsformer som gjøres på en datamaskin og mobiltelefon – i hvertfall uten å supplere med en type selvrapportering eller monitorerende programvare. Å bruke programvare som monitorer databruk vil være langt utenfor både min tekniske kompetanse og hvilken tilgang til politiets systemer som er forsvarlig. Og som nevnt i del 1.3 vites lite om i hvilken grad politiet faktisk bruker åpne kilder, så man kan risikere å ikke se noe til fenomenet man ønsker å studere. Fravær av et fenomen kan, som jeg argumenterer senere i avhandlingen, være et interessant funn. Men det vil sannsynligvis kreve omfattende mengder observasjon for å underbygge at noe ikke forekommer. I sum virker observasjon å være lite egnet for å belyse akkurat denne problemstillingen.

3.5. Utvalg og rekruttering

Den teoretiske populasjonen i mitt prosjektdesign, altså hvem jeg ønsker at studien skal si noe om (Johannessen et al., 2010), er alle politiansatte i Norge som har etterforskning som en vesentlig arbeidsoppgave. Dette fordi jeg antar at de som kan si mest om åpne kilder til etterforskningsformål er de som jobber med etterforskning. Dette kalles intern validitet eller

intern gyldighet – en logisk sammenheng mellom hvem man intervjuer og den underliggende problemstillingen prosjektet søker svar på (Johannessen et al., 2010; Tjora, 2012).

I skrivende stund er det 5288 årsverk som jobber med etterforskning i politiet (Politidirektoratet, 2019); åpenbart en for stor populasjon til at jeg kan undersøke den direkte gjennom fokusgrupper. I stedet foretok jeg et utvalg av populasjonen jeg mente kunne gi meg best mulig forståelse for politiets oppfatning av åpne internettkilder til etterforskning. Denne måten å velge populasjon og utvalg til en kvalitativ undersøkelse kalles «purposeful sampling», altså et strategisk utvalg (Patton, 1990). Utvalg gjort slik kan ikke påberope seg å representere hele populasjonen, men søker heller å være hensiktsmessige for å kunne besvare en problemstilling som angår populasjonen (Johannessen et al., 2010). Videre vil jeg redegjøre mer konkret for hvordan jeg foretok dette utvalget og rekrutterte fokusgruppene.

Alle fokusgruppene ble rekruttert fra prosjektet «obligatorisk årlig opplæring for etterforskere» (forkortet OÅO). Det var særlig tre fordeler jeg så ved dette: For det første har OÅO har samme målgruppe som studiepopulasjonen, altså politiansatte som primært jobber med etterforskning. OÅO er nemlig del av en bredere kompetansehevingsinnsats for etterforskningsfeltet kalt «Etterforskningsløftet» (Politidirektoratet, 2016).

For det andre gjennomførte OÅO-deltakerne mye av opplæringen ved å møtes i grupper for diskusjon og gi hverandre tilbakemeldinger på utført arbeid. Størrelsen på disse OÅO-gruppene var kompatible med fokusgruppeformatet – mellom 4 og 8 individer per gruppe. Dette er få nok til at alle kan inkluderes i samtalen, og store nok til å sikre mangfold i meninger og diskusjoner (Barbour, 2014; Krueger & Casey, 2015; Tjora, 2012). Antallet grupper jeg intervjuet ble begrenset av at OÅO-gruppesamlingene måtte være gjennomført i løpet av våren 2018, senest innen fellesferiestarten. Jeg ønsket også å kunne avgrense antallet grupper ved såkalt teoretisk metning – når ytterligere intervjuer ikke genererer nye tema eller problemstillinger (Kitzinger, 1994).

For de tredje er OÅO, som navnet tilsier, obligatorisk. Hvert enkelt politidistrikt og særorgan pliktet å tilrettelegge for at de ansatte fikk gjennomføre OÅO-møter. De ansatte var på sin side forpliktet til å delta. Dette var fordelaktig for denne studien, fordi det førte til høy gruppedeltagelse, og tilsvarende større rekrutteringsgrunnlag.

Politihøgskolen har et nasjonalt overordnet ansvar for OÅO-programmet, og gjennom Politihøgskolen fikk jeg oversikt over og tillatelse til å kontakte lokale OÅO-koordinatorene utpekt i hvert politidistrikt og særorgan. Jeg sendte informasjonsskriv (se vedlegg 1) til disse

lokale koordinatorene, som igjen formidlet kontakt med de gruppene som var villige til å delta i studien etter å ha lest informasjonsskrivet.

Jeg rekrutterte grupper fra ulike politidistrikt. Jeg ba de lokale OÅO-koordinatorene finne grupper som varierte i kjønn, alder og erfaring. Dette omtales som et homogent utvalg, og brukes ofte med forskningsmetoden fokusgrupper – nemlig at alle deltakerne har noe til felles, som må samsvare med undersøkelsens formål, samtidig som de er tilstrekkelig varierte på andre måter til å skape meningskontraster (Johannessen et al., 2010; Krueger & Casey, 2015). I dette tilfellet jobbet alle deltakerne med politietterforskning uten særkompetanse innen IKT, men varierer i kjønn, alder, yrkeserfaring og arbeidssted. Dette harmonerer også med UTAUT-modellen, som peker på kjønn, alder og erfaring som moderatorer i vår oppfatning av ny teknologi, og bidrar til meningsforskjeller (se del 3.6.2).

Som begrunnet tidligere (se del 3.2), ønsket jeg å unngå deltakere med spesialistkompetanse på IKT. Spesialister kan være greit å unngå i gruppeintervjuer også. Hvis én person blir oppfattet som en ekspert på temaet som debatteres (enten av personen selv eller av gruppa), kan noen gitt slik status bevisst eller ubevisst påvirke konsensus, overstyre uenighet eller hemme diskusjon i gruppa (Stewart & Shamdasani, 2014).

Det kunne også vært interessant å ha ulike kategorier av intervjugrupper, bestående av forskjellige interessenter i hver gruppe (Krueger & Casey, 2015; Lazar et al., 2010). Etterforskning er jo som sagt en formålsstyrt aktivitet (se del 2.1), og det er oftest andre interesserte i formålet med en etterforskning enn bare etterforskere. Man kan tenkte seg at ofre, tiltalte, nærstående, domstolene og publikum kan ha ulike synspunkter på politiets bruk av åpne nettkilder. Jeg kunne i stedet for mitt homogene utvalg av politiansatte hatt én gruppe bestående av forsvarsadvokater, én av dommere, én med publikum, og så videre. Et slikt prosjektdesign i denne avhandlingen kunne ha belyst politiets bruk av åpne nettkilder fra et bredere samfunnsperspektiv.

Men et bredere perspektiv kunne kanskje gått på bekostning av en dypere innsikt i hvilken virkelighet etterforskere fra ulike arbeidsmiljøer står i. Som nevnt i del 2.3, vil forsvarlig bruk av åpne kilder som en ulovfestet metode i stor grad avhenge den enkelte etterforskes evne til å gjøre etiske og juridiske vurderinger. Dermed kan etterforskernes oppfatninger om åpne kilder være særlig nyttig for videre opplæring og implementering av metoden. For å forstå disse oppfatningene, er det viktig å fange opp begrunnelsene for dem. Jeg forsøkte å oppnå dette ved å på forhånd bestemme meg for et analytisk rammeverk – altså et felles teoretisk

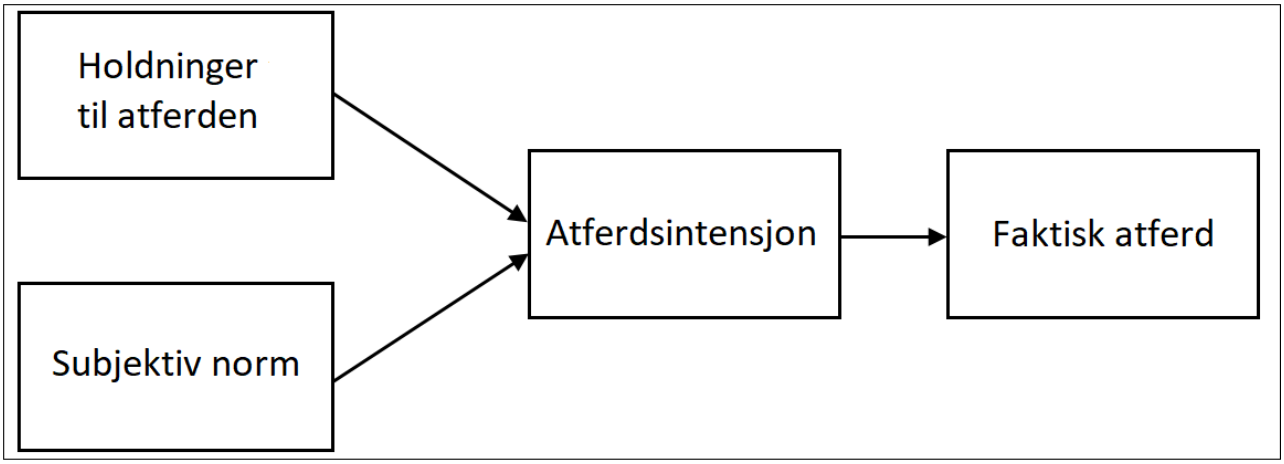
grunnlag for å finne gode tema og spørsmål til i intervjugruppene, og å kunne sette svarene inn i et system som et utgangspunkt for videre analyse og tolkning. Den analytiske rammen omtales i neste del.

3.6. Analytisk ramme

Begrunnelser for våre valg og preferanser er et sentralt tema innen atferdsforskning. Dette feltet har i de siste tiår avstedkommet en mer teknologisk spisset underdisiplin kalt teknologiakseptanse (Lai, 2017). Jeg ønsket å finne forklaringsmodeller innen teknologiakseptansefeltet som kunne hjelpe meg å identifisere tema og spørsmål som ville være relevante i den empiriske undersøkelsen. Jeg vurderte flere ulike modeller før jeg valgte én modell, kalt UTAUT. Modellen ble brukt både som et rammeverk til intervjuguiden og i den påfølgende analysen av intervjudata som presenteres i kapittel 4. Selve intervjuguiden presenteres i senere i dette kapittelet (del 3.7), men først kan det være nyttig å se nærmere på teorien og modellen som utgjør den analytiske rammen.

3.6.1. Teknologiakseptanse

En av de tidligste studiene som la grunnlaget for teknologiakseptansefeltet ble gjort av sosialpsykologene Martin Fishbein og Icek Ajzen i 1967. Med utgangspunkt i atferdsforskningsstudier fra perioden 1910-1960 utviklet de en modell for å forutse, forklare og påvirke alle typer menneskelig atferd (Momani & Jamous, 2017). Fishbein og Ajzens publikasjon (1975) døpte den «Theory of Reasoned Action», forkortet TRA. Den gjengis i figur 2, med norsk oversettelse av meg.

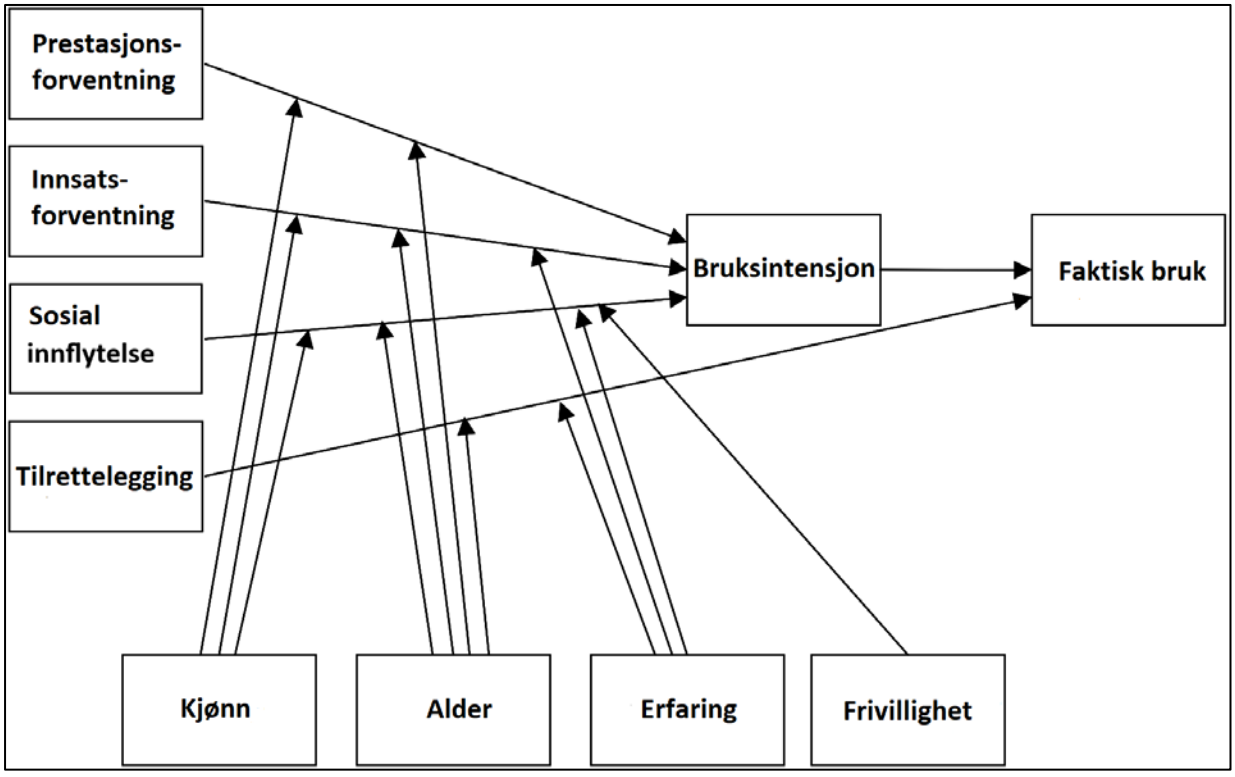


Figur 2 – TRA-modellen (Fishbein & Ajzen, 1975, min oversettelse)

Figur 2 viser at TRA-modellen setter intensjon som den primære drivkraften for atferd. Intensjon formes av egne holdninger til atferden, kombinert med en subjektiv oppfatning av hvilke normer som gjelder (Sharma & Mishra, 2014). Selv om TRA-modellen brukes for å forklare flere ulike former for menneskelig atferd, er den ikke utviklet for å si noe spesifikt om forventet bruk av ny teknologi (Lai, 2017). Av denne grunn vurderte jeg aldri å bruke TRA-modellen direkte i min undersøkelse. Den inkluderes allikevel her fordi UTAUT-modellen bygger på den samme kjerneidéen om intensjon som forløper for atferd. UTAUT tilfører imidlertid en mer detaljert nedbrytning av hva som former holdninger og normer – altså begrunnelser for bruk eller ikke bruk av teknologi.

3.6.2. UTAUT-modellen

I et forsøk på å harmonisere den voksende mengden litteratur innen teknologiakseptanse, utviklet Viswanath Venkatesh, Michael Morris, Gordon Davis og Fred Davis (2003) en modell de døpte «Unified Theory of Acceptance and Use of Technology», forkortet UTAUT. Den integrerer 8 tidligere modeller innen teknologiakseptanse. Modellen er gjengitt i Figur 3, og er oversatt fra engelsk til norsk av meg.



Figur 3 – UTAUT-modellen (Venkatesh et al., 2003, min oversettelse)

Vi ser umiddelbart at UTAUT består av langt flere bokser med begreper enn TRA-modellen. De to boksene merket faktisk bruk og bruksintensjon står lengst til høyre, og kan sees som et

sluttprodukt: Modellen søker altså å beskrive hva som skaper og påvirker vår intensjon om å bruke (kalt bruksintensjon) og faktisk bruk av teknologiske verktøy. Legg merke til pilen fra bruksintensjon til faktisk bruk. Dette indikerer intensjon som en primær drivkraft for bruk, som vi også så i TRA-modellen, men med det mer generelle ordet «atferd» i stedet for faktisk bruk av en bestemt teknologi.

De resterende 8 boksene deles i to ulike grupper: 4 konstruksjoner, samlet vertikalt i kolonnen til venstre. Siden UTAUT er bygget på flere tidligere modeller, er konstruksjonene sammenslåinger av flere lignende eller overlappende begreper fra disse tidligere modellene. Konstruksjonene hevdes å direkte forårsake bruksintensjon og faktisk bruk. De 4 siste boksene kalles moderatorer, og er samlet horisontalt i en rekke nederst i modellen. Dette er målbare størrelser: kjønn, alder og erfaring. Venkatesh et al. (2003) mener disse har en indirekte funksjon – variasjoner i dem svekker eller styrker nemlig effekten konstruksjonene har på bruksintensjon og dermed faktisk bruk av teknologien.

Tabell 2 er også fra Venkatesh et al. (2003) og forklarer boksene i UTAUT modellen og pilene mellom dem. Venstre kolonne i tabellen lister de 4 konstruksjonene – det er viktig å merke seg at de listes fra størst til minst effekt på bruksintensjon, altså påvirker prestasjonsforventning bruksintensjon sterkest. Tilrettelegging påvirker faktisk bruk direkte, uavhengig av bruksintensjon. Midtre kolonne definerer hver konstruksjon og i høyre kolonne listes de korresponderende moderatorene og deres innflytelse over effekten konstruksjonen har på bruksintensjon eller faktisk bruk. Oversettelsen til norsk er gjort av meg.

Konstruksjon	Definisjon	Modererende effekt
Prestasjonsforventning	I hvilken grad man tror at bruken av teknologien vil bidra til økt jobbprestasjon.	Kjønn og alder. Effekten av prestasjonsforventning på bruksintensjon er sterkere for menn, og for yngre ansatte.
Innsatsforventning	I hvilken grad man tror innsats vil kreves for å ta i bruk teknologien.	Kjønn, alder og erfaring. Effekten av innsatsforventning på bruksintensjon forsterkes for kvinner, yngre ansatte og uerfarne ansatte.
Sosial innflytelse	I hvilken grad man oppfatter at signifikante andre personer mener at man burde ta i bruk teknologien.	Modereres av kjønn, alder, frivillighet og erfaring. Sosial innflytelse har sterkere effekt på bruksintensjon hos kvinner, eldre ansatte, uerfarne ansatte, og særlig når det er obligatorisk å bruke teknologien.
Tilrettelegging	I hvilken grad man tror det finnes organisatorisk og teknisk struktur for å støtte bruk av teknologien.	Tilrettelegging vil ikke påvirke bruksintensjon, men påvirker i stedet faktisk bruk direkte. Alder og erfaring vil moderere effekten av tilrettelegging på faktisk bruk, slik at den er sterkere for eldre brukere, og for de med mer erfaring.

Tabell 2 – Konstruksjoner i UTAUT med definisjoner og moderatorer (Venkatesh et al., 2003)

Venkatesh et. al (ibid.) bemerker at sosial innflytelse kun har en effekt på bruksintensjon dersom det er obligatorisk å ta i bruk den nye teknologien, som er begrunnelsen for moderatoren frivillighet i modellen. Et utgangspunkt for problemstillingen er jo nettopp at bruk av åpne kilder ikke har en etablert felles praksis i norsk politi, og derfor ikke kan sies å være obligatorisk. Denne moderatoren illustrer også at UTAUT er ment for bruk på teknologiske verktøy i en jobbsetting; modellen mister sin forklaringskraft dersom man for eksempel anvender den på lystbetont teknologibruk, som dataspill eller andre underholdningstilbud (Lai, 2017). Allikevel inkluderer intervjuguiden spørsmål relatert til sosial innflytelse, i tilfelle det allikevel kunne lede til relevante diskusjoner i gruppene. Det var også interessant å se om sosial påvirkning allikevel hadde betydning for etterforskernes syn på åpne kilder, til tross for hva teorien indikerer. Med teknologiakseptanse og UTAUT som rettesnor, begynte jeg arbeidet med å designe en intervjuguide.

3.7. Intervjuguide

«Det er forskeren som skal generalisere i sin analyse, ikke informanten i intervjuet», konstaterer Aksel Tjora (2012, s. 137). For mest mulig pålitelighet i utsagnene bør fokuserte intervjuer søke å få frem konkrete opplevelser og erfaringer fra informantene, ikke bare nøye seg med generelle betraktninger. Intervjuguiden kan i så måte hjelpe intervjueren å opprettholde fokuset på det som er relevant, og om nødvendig fungere som en sjekkliste på at man i det minste har vært innom de tema man hadde planlagt før intervjuet startet. Guiden fremstod derfor som en betryggende «jukselapp» og sufflør for meg under intervjuene.

Intervjuguiden slik den så ut da jeg brukte den ligger i vedlegg 2. Tabellen består av fire kolonner. Hovedtema står i første kolonne, lengst til venstre. Hovedtemaene var kjent av intervjugruppene på forhånd, fordi de er oppgitt i informasjonsskrivet (vedlegg 1) sendt ut i forbindelse med rekrutteringen. Tilhørende konstruksjoner og moderatorer fra UTAUT-modellen står i kolonnen lengst til høyre. Tanken med dette oppsettet var at jeg i alle intervjuer som et minimum skulle innom alle 5 hovedtemaene i venstre kolonne. Hvor langt mot høyre og antall eksempelspørsmål som var nødvendige varierte, og ble tilpasset til hvordan samtalen og diskusjonsnivået artet seg til enhver tid.

Jeg ønsket at spørsmål og problemstillinger i størst mulig grad ble introdusert av informantene selv, ikke fra meg. Samtidig måtte jeg holde intervjuet innfor hovedtemaene relatert til problemstillingen. Dette omtales også gjerne som en balanse mellom frihet og struktur: Et fullt strukturert fokusgruppeintervju ville foregått nærmest som en spørreundersøkelse lest opp av moderator, hvor informantene gir sine muntlige svar i tur og orden. En god intervjuguide må derfor være kortfattet og langt mindre strukturbundet enn dette (Stewart & Shamdasani, 2014). Lavere strukturnivå, gir mindre innblanding fra moderator, som igjen tilrettelegger for friere diskusjon (Wibeck, 2010). Men en helt ustrukturert tilnærming kan på sin side gjøre det vanskelig å sammenligne data mellom de ulike fokusgruppene, fordi det ikke er noen garanti for felles holdepunkter i samtalene (Lazar et al., 2010). Jeg ønsket flest mulig diskusjoner om ett tema for å forsøke å få frem hele meningsspekteret rundt det, som er en fordel ved fokusgrupper beskrevet i del 3.3. Derfor valgte jeg å bruke den samme guiden i alle intervjuene, i motsetning til å diskutere forskjellige tema i hvert intervju.

Det første hovedtemaet «Om deg og din bakgrunn» samsvarer bra med moderatorene alder og erfaring i UTAUT-modellen, men tjener først og fremst for å kunne referere anonymt til

informantene når de siteres i funnkapittelet. De er også nyttige som enkle og kjappe oppvarmingsspørsmål for å etablere litt mer kjennskap og fortrolighet innad i gruppen mot meg som moderator (Tjora, 2012, s. 131; Wibeck, 2010, s. 73). Jeg startet alltid dette temaet med å presentere meg selv og min bakgrunn, og presiserte at jeg var der fordi jeg ville lære av dem, ikke være belærende. Min rolle som kollega var nok mye av grunnen til at jeg i det hele tatt fikk prate med dem i denne settingen, men jeg ville ikke at det skulle føre med seg inntrykket av at jeg var der for å kritisk evaluere enkeltpersoner på noen måte. Dette reflekteres mer over i del 4.4.1.

De fire påfølgende hovedtemaene ble innledet av at jeg stilte et par åpne spørsmål, kalt undertema i intervjuguiden. Hvert undertema hadde eksempler på noen spesifikke, mer lukkede spørsmål jeg kun stilte dersom de ikke var besvart innen vi skulle skifte hovedtema, eller samtalen stoppet opp. De 4 første hovedtemaene ble utledet fra UTAUT-modellen. Det siste temaet omhandlet etikk. Jeg tok dette temaet til slutt for å se hvorvidt noen av de etiske problemstillingene ble tatt opp av gruppa selv i diskusjoner av de forutgående temaene. Jeg la mye innsats ned i å få en guide som resulterte i intervjuer på mellom 60-90 minutter. Dette fordi jeg var redd for å slite ut informanter som allerede hadde brukt flere timer like forut på diskusjon, og fordi gruppeformatet i seg selv gav mye data på kort tid.

Tidlige utkast av intervjuguiden la opp til at jeg under intervjuet skulle søke opp meg selv på diverse åpne nettkilder, slik at deltakerne kunne diskutere søkeresultatene og metodene jeg brukte. Barbour (2014) kaller dette «stimulus materiale», og sier det kan være en engasjerende måte å få i gang diskusjon. Jeg forkastet imidlertid bruken av stimuli fordi, som Barbour (ibid.) også advarer, stimuli kan trekke fokuset bort fra de sentrale intervjutemaene, og i dette tilfellet også tok verdifull tid som kunne vært brukt til å diskutere fokustemaene.

Spørsmålene i seg selv bør være stimulus for informantene, argumenterer Krueger og Casey (2015). Åpne spørsmål med spørreordene hva, hvem, hvor, hvordan, hvorfor og når forutsetter mindre på vegne av den som skal svare, engasjerer vedkommende og gir mer rikholdige svar enn lukkede ja-eller-nei spørsmål. Det er viktig å unngå positivt eller negativt ladde spørsmålsformuleringer som avslører for informanten hva jeg synes eller ønsker å høre. Lukkede spørsmål har allikevel sin funksjon dersom det er nødvendig å få klarhet i en diskusjon, men man bør som regel starte med de generelle og bevege seg mot de spesifikke spørsmålene (Stewart & Shamdasani, 2014). Derfor var også de mest generelle temaene lengst til venstre i guiden, med mer spesifikke lukkede spørsmål mot høyre.

Neste del beskriver hvordan intervjuguiden ble nyttet i praksis, og hvordan gjennomføringen av gruppeintervjuene artet seg.

3.8. Praktisk forberedelse og gjennomføring

Selve intervjuundersøkelsen med alle fire fokusgruppene ble gjennomført på forsommeren 2018, i løpet av det som opplevdes som 6 korte og intense uker. Jeg hadde i perioden forut for dette innhentet tillatelse til å gjennomføre undersøkelsen fra Politidirektoratet og NSD (se vedlegg 3 og 5). Jeg hadde også etablert kontakt med OÅO-nettverket for å sette opp intervjuavtaler. Først gjennom Olav Dahl ved Politihøgskolen i Oslo, som var delprosjekteier med ansvar for OÅO-prosjektet nasjonalt. Han satte meg i kommunikasjon med lokalt OÅO-ansvarlige i ulike politidistrikt, og det var de lokalt ansvarlige hadde initialkontakt med gruppene og fant de som var interesserte i å delta.

Det var utfordrende å holde styr på kalenderen min i denne perioden – det var ofte kort varsel fra en gruppe hadde akseptert min invitasjonen til dagen gruppen hadde satt av til OÅO-møtet sitt. Det var viktig å rekke frem dit gruppen møttes i god tid før de forventet å være ferdige med OÅO-møtet. Jeg tror og håper jeg klarte å være på plass slik at ingen av gruppene måtte vente på meg. Informantene i alle gruppene fremstod som trygge og bekvemme allerede fra starten av intervjuene. Å intervjue gruppene der de var kan ha bidratt til dette, da det anses å være en viktig positiv miljøfaktor til intervjusituasjonen (Krueger og Casey, 2015; Wibeck, 2010).

Informantenes tilsynelatende bekvemmelighet virket heller ikke påvirket av at jeg hadde rigget opp et lite videokamera og hadde en diktafon på bordet som en sikkerhetskopi. Jeg var takknemlig for diktafonen, fordi jeg mistet endel video da jeg måtte bytte til en eldre kameramodell, med filsystem som viste seg å ikke støtte videofiler over en viss størrelse. Det tok mye lengre tid å transkribere fra kun lydopptak, fordi det var krevende å høre hvilken deltaker som sa hva, i stedet for å se videobilder. Nettopp det å kunne tilskrive utsagn til riktig informant, var årsaken til at jeg valgte å dokumentere intervjuene på video.

Antallet fokusgrupper jeg rakk å intervjue ble begrenset av at OÅO-gruppene var pålagt å ha gjennomført alle møtene sine før fellesferien 2018, og mange møter fant sted samtidig eller så nært hverandre i tid at jeg kun rakk å være til stedet på ett av dem. Jeg intervjuet gruppene fortløpende etterhvert som jeg fikk tilbakemelding fra en villig gruppe, så jeg bestemte ikke rekkefølgen på intervjuene. Jeg begynte å se antydninger til teoretisk metning (se del 3.5.)

under det fjerde og siste intervjuet. Det ble gjennomført siste dag før ferien, så jeg sa meg fornøyd.

Den første fokusgruppen jeg intervjuet, var egentlig ment å være en pilotgruppe for å teste intervjuguiden og øvrig format. Gruppa ble imidlertid inkludert i datagrunnlaget, etter å ha innhentet nytt samtykke fra samtlige av informantene i gruppa om dette. Pilotgruppa gav veldig gode refleksjoner, og deres data var et kjærkomment tilskudd, men beslutningen om å inkludere dem i studien ble først og fremst gjort fordi det ble nødvendig. Dette fordi jeg måtte avslå å intervjue en planlagt femte gruppe. Årsaken til avslaget var at dette distriktet ikke hadde noen OÅO-grupper tilgjengelig i det aktuelle tidsrommet. Den lokalt ansvarlige OÅO-koordinatoren var imidlertid flink og initiativrik, og presenterte et alternativ – ledelsen ved en av etterforskningsmiljøene i distriktet var villig til å avse tid ut over OÅO-programmet for to grupper med ansatte jeg kunne intervjue. Grunnet høy turnover ved avdelingen, var det god variasjon i alder og erfaring, fikk jeg opplyst. Ledelsen anmodet også at jeg kunne holde en presentasjon om bruk av åpne internettkilder til etterforskning når jeg var der.

Dette var den vanskeligste metodiske beslutningen jeg tok i løpet av prosjektet. Dilemmaet for meg var at disse gruppene ville ha blitt valgt ut på en annet grunnlag enn de øvrige gruppene. Jeg var bekymret for at det kunne bli problematisk å presentere funn og analyser fra én gruppe sammensatt av en arbeidsgiver spesifikt for mitt prosjekt, med grupper sammensatt på et uavhengig grunnlag som OÅO-programmet. Jeg tviler overhodet ikke på at tilbudet ble gitt i beste mening om å være så imøtekommende som mulig – det var rett og slett min egen usikkerhet på forskningsmetodikk som gjorde at jeg valgte å takke nei. Hadde situasjonen oppstått nå, med bare den lille ekstra erfaringen jeg har med forskningsmetodikk, ville nok svaret mitt vært annerledes. Neste del tar for seg retningslinjer for forskere bør være bevisst på for å ha en god etisk standard på sitt arbeide.

3.9. Forskningsetikk

Den nasjonale forskningsetiske komité for samfunnsvitenskap og humaniora (NESH) har laget en veileder med retningslinjer som utøvende forskere innen feltet er forpliktet å følge (NESH, 2016, s. 5). De forskningsetiske hensyn jeg har tatt i løpet av prosjektet er hovedsakelig identifisert herfra, og gjennomgås under tre tema: Konfidensialitet, samtykke og det jeg omtaler som innsideforskning.

3.9.1. Konfidensialitet

Jeg tok opp gruppeintervjuene på lyd og video for å fange opp rekkefølgen i diskusjoner til transkribering i etterkant, og noterte i tillegg kjønn og alder på hver informant. Slik informasjon defineres som personopplysninger (se del 2.6.1.), og skal som hovedregel behandles konfidensielt (NESH, 2016, s. 16). Jeg så ikke behov for å fravike denne hovedregelen, da problemstillingen etterspør det samlede synet fra politietterforskere på åpne kilder, og «den spesifikke personen som intervjues er mindre viktig enn teksten som produseres» ifølge Aksel Tjora (2012, s. 160-161). Alle referanser til informantene i notater, transkripsjoner og sitat er derfor anonymisert med en referanse bestående av gruppenummer, deltakernummer, kjønn og alder (mer om dette i del 4.4).

«Det deltakerne forteller forskeren, forteller de samtidig de andre i gruppen», skriver Berit Brandth (1996, s. 146). Til tross for at jeg legger opp til konfidensialitet, har jeg liten kontroll over hva informantene i ettertid velger å dele med andre om hva de har sett og hørt under intervjuet. Å sikre 100% anonymitet vil i praksis aldri være oppnåelig (Kvale, Brinkmann, Anderssen, & Rygge, 2015; Wibeck, 2010). Temaene fra intervjuguiden berører ikke områder som er åpenbart dypt personlige eller sensitive – hvis de var det ville jeg nok vurdert en annen innsamlingsmetode enn gruppeintervju. Hovedtemaene stod også i informasjonsskrivet sendt ut på forhånd (vedlegg 1), slik at informantene hadde konkret informasjon om hva intervjuet innebar da de tok stilling til hvorvidt de ville delta. Samtlige deltakere i denne studien hadde jo også sittet i gruppediskusjoner med OÅO-programmet like forut for intervjuet, og kunne dermed tilvenne seg gruppediskusjon-formatet før undersøkelsen startet. Fokusgrupper legger oftest opp til at deltakerne bare bidrar med meninger de er villige til å gå ut og forsvare offentlig (Barbour, 2014, s. 134). Dette utelukker ikke at informanter kan har opplevd det som vanskelig å for eksempel erkjenne kunnskapshull eller rette kritikk mot kollegaers praksis i gruppeintervjuene, men dette drøftes mer i analysen av funn (4.4.1).

3.9.2. Samtykke

Forskning som omhandler personopplysninger krever også at deltakerne gir samtykke. For å anses gyldig må samtykket «være fritt, informert og uttrykkelig» (Barbour, 2014; NESH, 2016). Forskningsprosjekt som nytter personopplysninger må også meldes til Norsk senter for

forskningsdata[16] (forkortes NSD). For å oppfylle kravene til gyldig samtykke tilbyr NSD en brevmal med relevant informasjon for utdeling til potensielle deltakere før en undersøkelse. Jeg benyttet denne malen til mitt informasjonsskriv (se vedlegg 1).

Skrivet ble sendt noen dager i forveien til de aktuelle OÅO-gruppene til støtte i avgjørelsen om de ville delta i undersøkelsen. Da jeg møtte gruppene, ba jeg om deltakernes signatur på det samme informasjonsskrivet hvor de forsikret meg om at innholdet var kjent. Til tross for slike forberedelser advarer Tjora (2012, s. 41):

> *«(...) relasjonen forsker-informant er ikke symmetrisk. Selv om deltakerne i forskningsprosjektet er opplyst om sitt informerte samtykke og retten til å trekke seg på et hvilket som helst tidspunkt, er det mye mulig at de etter det direkte møtet med forskeren vil vegre seg mot å svikte».*

Et informasjonsskriv, uansett hvor velformulert, fritar altså ikke meg som forsker å være oppmerksom på andre forhold som kan påvirke deltakerne negativt, enten i beslutningen om samtykke, under intervjuet, eller i etterkant. Kanskje særlig det at deltakerne hadde vært forpliktet til å møte opp i OÅO-gruppene like i forkant kunne gjøre det vanskelig for enkelte å trekke seg fra fokusgruppen med sine kollegaer til stede. Jeg forsøkte å imøtekomme dette med å stresse frivillighet i deltakelsen, og at det var veldig forståelig dersom noen hadde jobbforpliktelser eller bare var slitne etter nettopp å ha gjennomført OÅO-møtet. Det var totalt to-tre personer fordelt på de 4 intervjugruppene som valgte å ikke bli med etter at jeg hadde sagt dette. Det er jeg takknemlig for, så langt det kan indikere at de som ble igjen og gjennomførte følte seg mindre presset.

3.9.3. Innsideforskning

Med utgangspunkt i NESH sine retningslinjer fremhever Rachlew (2010) etiske problemstillinger som blir spesielt aktuelle når man forsker på sine egne. Forskere med bakgrunn fra feltet kan ha særlig utfordring med å gå ut fra sin yrkesrolle, etablere en kritisk distanse til egen profesjon, og opprettholde avstanden gjennom alle faser av prosjektet. Jeg har ikke opplevd objektivitet spesielt krevende i dette prosjektet. Oppgaven omhandler et relativt nytt fenomen, så det virker ikke å ha etablert seg sterke holdninger eller praksis i politiet som undersøkelsen eventuelt kunne ha havnet i opposisjon til. Dette kan også skyldes at det skjer i regi av Politihøgskolen og ikke min arbeidsgiver direkte. Jeg er takknemlig for

[16] https://nsd.no/

den rollen skolen tar i det som sikkert tidvis kan være et krevende spenningsfelt mellom akademia, politisk ledelse og den praktiske utførelse av politiets samfunnsoppdrag.

Jeg kan se to klare fordeler av min innsiderrolle som forsker under dette prosjektet – både veilederen for politiets bruk av åpne internettkilder (Kripos, 2018) og OÅO er såpass nye initiativer som enda er under utvikling at jeg ikke tror jeg ville ha fanget dem opp uten å selv være en del av målgruppen de retter seg mot. Rachlew (2010) argumenterer med utgangspunkt i egne erfaringer at de forskerne som starter som innsidere, må være spesielt oppmerksomme på blindsoner mot faget sitt. Slike blindsoner skapes av kunnskap og erfaring som er så internalisert at man ikke er bevisst hvordan den preger hele ens tilnærming, langt mindre evner å balansere den mot eventuell motstridene kunnskap forskningen kan avdekke. Rachlews svar på denne utfordringen var rigid testing av spørsmålene sine opp mot eksisterende forskning og teori. På samme måte har teknologiakseptanse sammen med øvrig forskning og litteratur om etikk rundt bruk av åpne kilder hjulpet meg å oppnå et litt mer objektivt perspektiv. Dette betyr ikke at jeg kan overkomme mine bias helt, mer enn noen av oss kan. Rachlew viser til Liv Finstads formulering (2000, s. 351) «Ingen posisjoner er privilegerte utkikkspunkter», og at det beste forskere kan gjøre er å redegjøre for sin egen posisjon – ikke nødvendigvis som en feilkilde, men fordi åpenhet om den kan styrke tilliten til arbeidsmetodikken og resulterende funn.

3.10. Analyse av empiriske data

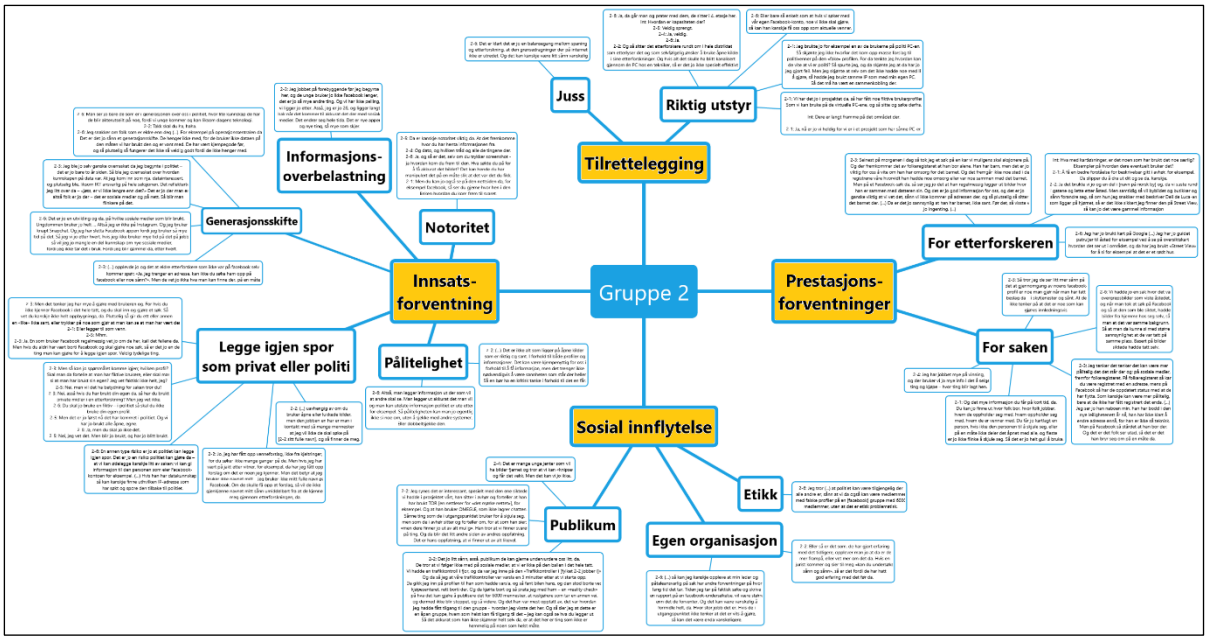
For å kunne presentere funnene i neste kapittel, måtte jeg først systematisere og analysere rådataene fokusgruppeintervjuene hadde generert. Rådataene var video- og lydopptak, hvor samtalene var delvis strukturert rundt hovedtemaene fra intervjuguiden. For å komme meg fra rådata til funn og en konseptualisering, brukte jeg Aksel Tjoras (2012) stegvis-deduktive-induktive metode, forkortet SDI. SDI har som mål å «gjøre det mulig for en leser av forskningen å få økt kunnskap om saksområdet det forskes på, uten selv å måtte gjennomgå de data som er generert» (Tjora, s. 174, ibid.).

Selv om prosessen er langt fra lineær, søker SDI generelt å gå fra empiriske rådata mot å kunne utvikle konsepter og teori. Første steg for meg var å transkribere lyd- og videoopptakene i sin helhet. Å gå fra lyd og video til skrevet tekst kan i seg selv ses som en ganske massiv reduksjon i datamengde (Barbour, 2014). Kompleksiteten av data som kan finnes i ansiktsuttrykk, kroppsspråk og tonefall var for eksempel blitt borte i min transkripsjon. Men formålet med analysen er å redusere kompleksitet for å øke forståelse.

Neste steg ble å forsøke å legge bort mine egne tema, teori og forutinntagelser som lå til grunn for intervjuguiden, og i stedet lese hvordan informantene faktisk ordla seg – en såkalt tekstnær koding, ifølge SDI metoden.

De tekstnære kodene kjennetegnes ved at de bare kunne vært hentet fra denne konkrete empirien, altså koder mest mulig formet av informantenes egne ord og uttrykk (Tjora, 2012, s. 184). Fordelen med de tekstnære kodene er å redusere effekten av mine egne bias, og beskriver langt bedre hva som faktisk foregikk i intervjuet enn intervjuguiden som representerer den generelle analyserammen jeg hadde laget på forhånd. Ulempen er at det blir for mange tekstnære koder til å kunne gjøre videre analyser – jeg fant 60-70 koder i mine transkripsjoner. Neste steg i SDI-metodikken er derfor kategorisering, hvor overlappende tekstnære koder slås sammen i kategorier, og de kodene som ikke bevarer problemstillingen legges bort. På dette stadiet skifter altså analysen fra å være helt empiristyrt, til å påvirkes av problemstillingen.

For å videre integrere teorien med empirien visualiserte jeg hvert av de 4 gruppeintervjuene i en slags flytdiagram, eller tankekart. Figur 4 er ment som et eksempel, og viser kartet for intervjugruppe 2. Kartet ordner såkalte «meningsbærende elementer» (Johannessen et al., 2010, s. 174), som er sitater fra transskripsjonene brukt i den tekstnære kodingen under kategoriene de var med på å forme. I henhold til SDI utvikles dataene nå videre ved å koble kategoriene til relevant teori – i mitt tilfelle teknologiakseptanse. Derfor ble de 4 konstruksjonene fra UTAUT-modellen (del 3.6.2, figur 3) – prestasjonsforventning, innsatsforventing, sosial innflytelse og tilrettelegging – integrert i kartet som fire grunnstammer som kategoriene springer ut av.



Figur 4 – Eksempel SDI kategorier fra fokusgruppedata kombinert med UTAUT konstruksjoner

Figur 4 viser UTAUT konstruksjonene i gult, og kategoriene står i hvite bokser med fet skrift. Figuren går ikke i detalj på alle de meningsbærende elementene, som er her representert med boksene lengst fra senter, med liten uleselig tekst. Disse presenteres i stedet som sitater i neste kapittel om funn. Hovedfunnene ble bestemt ved å sammenligne kartene for de 4 gruppeintervjuene og se på hvilke kategorier som dukket opp i alle. Noen kategorier funnet i én til tre grupper er tatt med for å nyansere og balansere hovedfunnene. Noen av de meningsbærende elementene som var grunnlaget for funnet ble deretter sitert, med referanse tilbake til gruppe og informant. Alle gruppene er representert med sitater til hovedfunn.

SDI-metoden brukes også i neste kapittel til å utlede en typologisk modell ved å kombinere funnene med elementer av UTAUT-modellen (del 4.5). SDI skisserer enda et steg etter dette, fra modeller til mer overordnet teoriutvikling. Men som Tjora (2012, s. 189) kommenterer, er dette mest aktuelt å snakke om i arbeider med større omfang og datamateriale, og var ikke aktuelt i denne studien.

4. Funn

Dette kapittelet presenterer funn fra den empiriske undersøkelsen beskrevet i kapittel 3. Del 4.1 og 4.2 beskriver to hovedfunn fra alle fire intervjugruppene. Del 4.3 redegjør for mindre utbredte funn jeg ikke så i alle gruppene, men som allikevel tjener som nyanseringer og motvekt til hovedfunnene.

Kapittelet inneholder sitater fra intervjuene. For å ivareta anonymitet, men samtidig forankre sitatet i empirien, refereres informantene til slik: 1-6, k45 betyr at informanten var i intervjugruppe 1, hvor hun hadde deltakernummer 6, og er en kvinne på 45 år. På samme måte vil m26 referere til en 26 år gammel mann. Deltakernummer brukes siden én intervjugruppe kan ha to jevnaldrende deltakere av samme kjønn. Mine tilføyelser til sitater er synliggjort i klammeparenteser [slik]. Ellipser i parentes (…) indikerer at jeg har fjernet innhold, fordi det ikke ble vurdert som direkte relevant i den sammenhengen sitatet brukes. Sitater fra flere informanter som del av en diskusjon er forbundet med en heltrukket vertikal linje på venstre side av sitatene.

4.1. Hovedfunn 1: Åpne kilder til bekymring for å gjøre feil

Det jeg opplevde oftest, i alle fokusgruppene, var diskusjoner som bunnet i bekymring hos informantene om å gjøre noen feil når de brukte åpne kilder til etterforskning. Typen feil varierte mellom ulike grupper og deltakere: å legge igjen spor, enten som politi eller som privatperson, tråkke over juridiske grenser og problemer med å bedømme påliteligheten av informasjon fra åpne kildesøk på nett.

4.1.1. Å legge igjen spor, som politi eller privatperson

Alle gruppene så faren for å legge igjen spor etter seg når de bruker på åpne kilder til etterforskning. Dette var det temaet som ble diskutert oftest, og som derfor presenteres først. Flere informanter så det som en fare mot operasjonell sikkerhet (se del 2.3.2) – altså å utilsiktet å legge igjen spor som kan fanges opp av søkssubjektet, og dermed avsløre at de er under politietterforsking:

> *2-6, m33: En annen type risiko er jo at politiet kan legge igjen spor. Det er jo en risiko politiet kan gjøre da – at vi kan ødelegge kanskje litt av saken; vi kan gi informasjon til den personen som eier Facebook-kontoen for eksempel. (…) Hvis han har datakunnskap, så kan kanskje finne ut hvilken IP-adresse som har søkt og spore den tilbake til politiet?*

3-5, k47: Jeg vet ikke hvor fort det skjer jeg, om jeg har søkt opp han én gang. Men koblingen registreres jo. Og hvis jeg bruker min telefon for å ringe ham, og så søker jeg ham opp på Facebook, så kommer han vel opp som venneforslag ganske fort, vil jeg tro?

3-2, m56: Da tenker jeg på det som [3-3] sa, at vi er litt flink med innstillingene, altså hvordan har vi innstilt profilene våre.

3-5, k47: Men der er jo … hvertfall min kompetanse, eeh …

3-2, m56: Ja. Det er der det stopper.

1-1, m35: IP-adressen er jo lik. Og det kan jo knyttes opp til deg, så hvis noen vet hva de driver med, så er det jo ikke vanskelig å se hvem som har vært inne på serveren deres, og vært inn på de åpne kildene og sett ting. (…) Så vi må jo være litt vare på det også, for man legger jo igjen spor på alt man gjør.

2-3, m26: Men det tenker jeg har mye å gjøre med brukeren og. For hvis du ikke kjenner Facebook i det hele tatt, og du skal inn og gjøre et søk. Så vet du kanskje ikke helt oppbygninga, da. Plutselig så gir du en eller annen en «like» ikke sant, eller trykker på noe som gjør at man kan se at man har vært der.

2-1, k24: Eller legger til som venn

2-3, m26: Ja. En som bruker Facebook regelmessig vet jo om de her, kall det fellene da. Men hvis du aldri har vært borti Facebook og skal gjøre noe søk, så er det jo en del ting man kan gjøre for å legge igjen spor. Veldig tydelige ting.

Andre var bekymret for å eksponere seg som privatperson ovenfor dem man etterforsker, eksempelvis ved bruk av ens egne personlige brukerkonti på sosiale media til å søke på personer under etterforskning:

3-5, k47: Men vi blander jo privat og jobb uansett, når du bruker din egen Facebook-profil og søker opp. For det gjør vi jo støtt og stadig.

4-2, k27: Og hvis jeg skal på Facebook da, hvordan går jeg frem der uten å gjøre noe feil? For jeg ønsker ikke å eksponere meg selv, for det har jo hendt at jeg har lagt til folk som venn med et uhell.

3-3, k41: Altså hvis vi bruker facebook aktivt til etterforskning med vår private … eller har vi en annen bruker? Det er en problemstilling som er interessant synes jeg. For vi legger jo igjen spor, da (…) Det har jeg registrert selv hvertfall – at personer som har roller i straffesak dukker opp som venneforslag. Da vil jeg jo tro at dersom en ikke kan nok om innstillingene sine, så kan jeg dukke opp som venneforslag hos de jeg søker på også. Har vi bevissthet rundt det? Hvordan er det det fungerer egentlig?

3-5, k47: Går det an å få bort det, tror du?

3-3, k41: Det gjør visstnok det da. Jeg tør ikke søke med min egen bruker på noen som har rolle i straffesak.

1-2: Hvis man søker på navnet mitt, så ligger det ikke noen bilder eller noe ute. Det er som oftest telefonnummer eller adresse. Nesten daglig må du oppgi hvertfall navnet ditt. Og hvis du treffer rette person da, så kan livet ditt plutselig bli ubehagelig, eller hvertfall ta en annen retning.

Alternativet til å bruke sine private profiler – altså fiktive, nøytrale profiler – ble også diskutert:

1-6, k42: Så leste jeg i veilederen [Kriposveilederen (2018)] blant annet om at man kunne opprette en falsk facebook-profil. Og jeg scrolla gjennom hele, men kjente underveis at, åh, jeg kan for lite (...) For meg så er det et hinder. At man tenker man ikke får det til.

2-3, m26: Men så kan jo spørsmålet komme igjen; hvilken profil? Skal man da fortelle at man har fiktive brukere, eller skal man si at man har brukt sin egen? Jeg vet faktisk ikke helt, jeg?

2-5, k38: Nei, men vil det ha betydning for saken tror du?

2-3, m26: Nei, asså hvis du har brukt din egen da, så har du brukt private midler i en etterforskning? Men jeg vet ikke.

2-6, m33: Du skal jo bruke en fiktiv – i politiet så skal du ikke bruke din egen profil.

2-5, k38: Men det er jo først nå det har kommet i politiet. Og vi har jo brukt alle åpne, egne.

2-6, m33: Ja, men du skal jo ikke det.

2-5, k38: Nei, jeg vet det. Men blir jo brukt, og har jo blitt brukt.

Bekymringen for å legge igjen spor når man etterforsker med åpne kildesøk, enten som politi eller privatperson, ble ofte begrunnet i mangelfullt utstyr. Flere informanter peker på behovet for terminaler som er frittstående fra det øvrige politi-nettverket, og tilgang til fiktive, nøytrale profiler anses å være nødvendige for å unngå å legge igjen spor. Dette samsvarer da bra med teorikapittelets del 2.3.2, om at politiet bør kunne skjule søk på åpne kilder ved saklig behov. Slike verktøy omtales imidlertid som mangelvare:

4-4, k33: Har ikke vi oppretta en sånn egen facebook profil da? Var det ikke du som sa det? [indikerer 4-1].

4-1, m29: Tror ikke jeg har sagt det.

4-4, k33: Det var noen som sa det. For politiet i [informantens politidistrikt]? Så man kan bruke den til å søke.

4-2, k27: For det er jo også et hinder, da. For nå vet ikke jeg …

4-3, k26: Er det greit?

4-2, k27: Nei, jeg tror ikke det er greit, skjønner du.

4-3, k26: Det tror ikke jeg heller.

4-2, k27: La oss si jeg ville spane på en person, da. Altså legge en til som venn, fordi de ikke har så mye åpent, da.

4-4, k33: Nei, ikke legge til som venn – bare for å søke, for jeg har ikke lyst å bruke min egen profil til det.

4-2, k27: Ja, da er det kanskje greit. Men har i hvertfall hørt at hvis du oppretter en profil, som ikke er deg, men som du disponerer, for å kunne gå inn på for eksempel Instagram da, for å følge, så får du opp bilder og …

4-4, k33: Nei, det var ikke sånn. Ikke noe venner eller noe sånn. Det var bare for å kunne gå … og kikke. Ikke for å bli venn med noen eller sånne ting.

4-2, k27: Mmm … For det er klart at det er et hinder, hvis du skal rundt og søke med din egen profil.

4-3, k26: Du må jo opprette en falsk profil, da – for du kan jo ikke hete «[Stedsnavn] politistasjon».

1-6, k42: Jeg er redd for å legge igjen spor med min egen profil, fordi vi ikke har noe stasjonert på bygget som vi kan bruke

Én informant hadde nødvendig utstyr, men at det var et unntak fra det hun oppfattet som normalen, og var begrunnet i et prosjekt hun var med i:

2-1, k24: Vi har det jo i det prosjektet da, så har vi fått noen fiktive brukerprofiler. Som vi kan bruke på de virtuelle PC-ene, og så sitte og søke derfra.

Andre informanter erfarte nærmest det motsatte - å bli aktivt utstengt fra enkelte åpne kilder via politiets nettverk:

4-3, k26: Det som er da, er at vi har ikke tilgang til å gå inn på Youtube da, for eksempel, på jobb PC-en. Og det vil jo kanskje vært interessant hvis det er noen som har filmet en hendelse da, for eksempel, og så får du ikke gått inn og sett på det.

4-1, m29: Ja. Jeg vet ikke om det på grunn av kapasitet, eller hva det er for noe, jeg.

4-4, k33: Mmm.

4-2, k27: Nja, eller så er det for å hindre virus og sånt. For da er du inne på internett via politinettet.

4-1: Vi har jo bærbare PC-er, da, så vi har jo muligheten der. Jeg tror rett og slett de må gjøre det av hensyn til kapasiteten, jeg.

Int: Har alle en bærbar PC?

> *4-2, k27: Nei, det er felles.*
>
> *4-3, k26: Felles.*
>
> *4-4, k33: Felles.*
>
> *4-1, m29: Vi har vel 5-6 stykker på avsnittet.*
>
> *4-2, k27: Og det er gjerne litt rot, hehe.*

Det kan se ut til at informantene over har forståelse for denne begrensningen på politinettet for å redusere risiko for angrep, og dermed identifiserer et av argumentene for skjuling av søk fra del 2.3.2. Igjen er manglende utstyr et tema; at det er relativt få bærbare datamaskiner som deles mellom flere.

4.1.2. Juridiske grenser

Uklarhet om juridiske grenser var også tema hos alle gruppene, og en kilde til bekymring om å gjøre feil. Noen informanter påpekte egen manglede forståelse av relevant juss:

> *4-2, k27: Og hvis jeg skal på Facebook da, hvordan går jeg frem der uten å gjøre noe feil? (...) Men også fordi man ikke vil gjøre noe feil juridisk. Man vil ikke tråkke over den der grensen; er dette noe vi har beslutning fra jurist på? Og kanskje man rett og slett ikke ser mulighetene?*

> *1-5, k34: Når du skal få sikret disse tingene her, så hadde det vært greit og hatt noen som kan lovverket, og som kan gå inn og bare sikre og få det gjort på en ordentlig måte, enn at man selv skal sitte og taste og trykke.*

Andre mente reglene og grensedragningene i selv er diffuse, og vanskelige å navigere i praksis. At lovverket i seg selv sees som et hinder for å ta i bruk åpne kildesøk:

> *1-7, m53: Men så kommer det jo an på prosessuelle hindringer da. Det vil si når er det spaning, når er det UC [forkortning av undercover, politiagentvirksomhet], når er det provokasjon. Som vanlig etterforsker skal man være, mener jeg da, ytterst forsiktig med å opprette falske profiler og infiltrere miljøer.*

> *1-1, m35: Man søker jo med falsk profil, så man utgir seg for å være en annen enn man faktisk er og søker om medlemskap i en lukka gruppe. Og henter informasjonen man finner der og putter det inn i en straffesak. Og på det stadiet så var man ikke offisielt i en etterforskningsfase. Og det slår jo tilbake og blir et problem, så det er jo den store smellen jeg har gått på der, som man lærer veldig mye av der og da. Det blir fort et tema i retten – har dere da sikre bevis? Hvordan gikk dere fram da? Så det er et problem.*

> *2-6, m33: Det er klart det er jo en balansegang mellom spaning og etterforskning, at den grensedragningen der på internett ikke er utredet. Og det kan kanskje være litt sånn vanskelig.*

Vi ser over at diskusjonene er inne på avhandlingens del 2.2.1 om grensedragningen etterretning versus etterforskning, og del 2.3.2 med skjulte søk og overgangen til infiltrasjon:

> *1-3, m28: Det som ligger åpent er jo åpent, men hvis du faktisk søker medlemskap i en gruppe eller som venn, da har du jo gått over i infiltrasjon.*
>
> *3-5, k47: Og i hvertfall hvis du er aktiv på den profilen da. Én ting er hvis du passivt overvåker, men i det øyeblikket du begynner å bruke den aktivt, da krysser du en grense, ja.*
>
> *4-1, m29: Jeg tenker at så lenge du søker på ting den personen har åpent ute, og ikke begynner å legge til og lure folk, så er det greit.*
>
> *4-3, k26: Jeg synes ikke det er greit.*
>
> *4-2, k27: Jeg tror ikke du kan bruke det i retten.*
>
> *Int: Hvorfor tenker dere det?*
>
> *4-2, k27: Det er jo egentlig mest det juridiske, ikke sant. Da må du hvertfall ha en dialog med juristen. For da er vi inne på det etterretningssporet, eller skjulte etterforskningsmetoder. For det er jo egentlig ikke åpent da, hvis du må legges til som venn for å få se det.*
>
> *4-1, m29: Ja, det er jeg enig i, men hvis det er åpen informasjon, og du er en fiktiv bruker, da tenker jeg at det er greit.*
>
> *2-6, m33: (...) politiet kan være tilgjengelig der alle andre er, sånn at vi da også kan være medlemmer med falske profiler på en [facebook] gruppe med 6000 medlemmer, uten at det er etisk problematisk.*

4.1.3. Pålitelighet og notoritet

Noe av det første som ble tatt opp av flere grupper som en mulig feilkilde ved søk på åpne kilder er at påliteligheten til informasjonen man finner kan være vanskelig å vurdere:

> *2-2, k40: (...) Det er ikke alt som ligger på åpne kilder som er riktig og sant. I forhold til både profiler og informasjoner. Det kan være kjempenyttig for oss i forhold til å få informasjon, men det trenger ikke nødvendigvis å være sannheten som står der heller. Så en bør ha en kritisk tanke i forhold til det en får.*
>
> *1-7, m53: alle har et motiv for å kunne tillegge en mening eller hendelse eller hva som helst, og det ligger et personlig motiv bak. Som gjør at det man da leser langt i fra trenger å stemme med virkeligheten.*
>
> *4-2, k27: Mmm, klokkeslett og dato kan stå der – men kan det ha blitt endret?*
>
> *4-4, k33: Du kan jo bare ta et skjermbilde av det opprinnelige bildet, for eksempel, og bare vise til datoen på når skjermbildet ble tatt, ikke sant?*
>
> *4-2, k27: Det er klart begrensninger, og jeg tror det er derfor jeg ikke bruker det, for jeg vet ikke hvordan man kan bruke det trygt.*

God notoritet tas imidlertid ofte opp i disse diskusjonene som en løsning på hvordan forholde seg til usikker informasjon:

> *2-5, k38: Da er kanskje notoritet viktig da. At det fremkommer hvor du har henta informasjonen fra.*
>
> *2-4, k36: Og dato, og hvilken tråd og alle de tingene der. [begrepet «tråd» brukes her i betydningen av flere meldinger mellom to eller flere i en diskusjonsform om samme tema].*
>
> *2-6, m36: Ja, og så er det, selv om du trykker screenshot - ja hvordan kom du frem til den. Hva søkte du på for å få akkurat det bildet? Det kan hende du har manipulert det på en måte slik at det var det du fikk.*
>
> *2-1, k24: Men du kan jo også se på den nettsiden da, for eksempel facebook, så ser du gjerne hvor hen i den linken hvordan du kom frem til svaret.*

> *4-1, m29: Ting kan endres etter at du har sett det. Så det viktig å notere seg nøyaktig når du har sett det, og hvilke nettadresser. Også kanskje sikre det du ser på ett eller annet vis – ved foto eller et eller annet.*
>
> *4-2, k27: Ja, og si rettssaken er om et år, så …*
>
> *Int: Hvordan løser dere det da?*
>
> *4-1, m29: Bilder. Skjermbilder, rett og slett, ja*

> *3-2. m56: (…) hvis det gjelder ting man velger å bruke i en straffesak, så tar man jo skjermbilde – enten fotograferer det, eller tar utskrift, eller ett eller annet sånn. Så jeg vet jo det at det er ikke uvanlig at vi legger dokumentasjon fra Facebook som et saksdokument – det har vi jo gjort mange ganger. Men da skriver vi jo hvilket tidspunkt det er hentet, og at det er fra en åpen Facebook-profil, for eksempel.*

Sitatene over kan indikere at informantene ser verdien av notoritet når åpen kildeinformasjon får betydning som bevis, og inntas som straffesaksdokument, som drøftet del 2.4.2.

4.2. Hovedfunn 2: Åpne kilder til opplysning, effektivisering og tillit

Alle gruppene hadde anekdoter og eksempler på hvordan åpen kildeinformasjon hadde bidratt til en konkret etterforskning, eller satte etterforskeren i stand til å arbeide mer effektivt. Jeg så en metodisk utfordring i dette funnet, fordi jeg selv har en klart positiv oppfatning av åpne kilder, som drøftet i del 3.2 og 3.9.3. En mulig metodisk svakhet og feilkilde kan derfor være at jeg både modererte intervjuene, og også definerte hvilke funn som presenteres. Transparens i prosjektarbeidet, med foregående teori- og metodekapitlene, er imidlertid ment å motvirke eventuelle bias jeg har i å identifisere disse funnene.

4.2.1. Til sakens opplysning

Flere informanter beskrev tilfeller hvor opplysninger fra åpne nettsøk ble sentrale for å starte en etterforskning, eller oppklare en sak:

> *4-2, k27: Vi oppklarte en ranssak hvor en 16-åring med kniv hadde truet penger fra noen. Og en kollega på det stedet hadde sett på en av disse Snapchat-gruppene at det var delt en video, og på bakgrunn av den identifiserte man raneren. Dette ble ikke lagt i saken, men det var bakgrunnen. Selve videoen var ikke direkte relevant, men det ble sagt ting på videoen som hjalp.*

> *3-4, m44: Jeg tenker på når vi fikk beslutning, om du husker, 3-3, han som kjørte fra oss nedi sentrum med motorsykkel?*
>
> *3-3, k41: [Nikker]*
>
> *3-4, m44: Og så gikk vi på Facebook-profilene deres, for vi hadde fått tips på noen personer det kunne være. Så fant vi et bilde av samme motorsykkelen på en av profilene. Og sånn fikk vi beslutning på ransaking hjemme hos vedkommende, ut i fra at han hadde kjørt i fra politiet, for det hadde han filmet. Og lagt det ut på Youtube og skrytt av det. Og så gikk vi altså på Facebook og fant bilde av sykkelen, skrev en rapport på det, og så fikk vi ransaket hjemme hos ham. Og så fant vi da de opplastede videoklippene fra Youtube på hans PC. Så da var jo saken i boks. Så det ble jo en veldig bra sak da, egentlig.*

Andre fortalte om hvordan åpen kildeinformasjon ble brukt til å styrke eller svekke en forklaring fra parter i en etterforskning:

> *4-3, k26: Hvordan det kan styrke eller svekke fornærmedes forklaring. Hun sier at hun har fått blåmerker, men hun ville ikke dra til legen etter hendelsen, så finnes ikke noe dokumentasjon. Men så har hun da lagt ut oppdatering på bloggen med bilder, dagen etter. Det vil jeg si er nyttig for saken.*

> *1-6, k42: Jeg hadde en sak der aktiviteten på Facebook ble skrevet i en rapport, ja. Gikk gjennom en brannsak egentlig, for å se om det var delt noen bilder, hvor lenge han hadde vært aktiv på Facebook, opp imot branntidspunktet da.*

> *2-6, m33: Vi hadde jo en sak hvor det var overgrepsbilder som viste åstedet. Og når man tok et søk på Facebook og så at den som ble siktet, hadde bilder fra hjemme hos seg selv, man så at det var samme bakgrunn. Så at man da kunne si med større sannsynlighet at bildene var tatt på samme plass. Basert på bilder siktede hadde tatt selv.*

En spesifikk type åpne kilder som flere informanter hadde god erfaring med, var legale markedsplasser på nett (det norske markedsplassen www.finn.no refereres til som «finn» eller «finn.no» i informantenes sitater videre). Også sosiale medier brukt til omsetning av ulovlige varer og tjenester – narkotika, heleri, forsikringssvindel og prostitusjon:

> *4-3, k26: Men med tanke på etterforskning da, så vil jo kanskje finn.no være veldig ålreit – Si det er et tyveri da, av de-og-de tingene. Så kan man kanskje gå inn på finn da, og se at «Oj, han der la jo dem ut for salg i går». Så da vil jo det være et lurt etterforskningsskritt.*
>
> *1-7, m53: Så kan du jo bruke det hvis du får en tyverisak da – snøfreser stjålet i Ole Brumms vei. Javel, så går du inn på Finn da, og så ser du to dager senere at noe har lagt ut en snøfreser. Da kan du kanskje bli en kjøper, og sette opp en set-up.*
>
> *2-4, k36: Jeg har jobbet mye på vinning [vinningskriminalitet, eksempelvis tyveri og heleri], og der bruker vi jo mye info i det å selge ting og kjøpe – hvor ting blir lagt hen.*
>
> *3-5, k47: Han hadde modus der han drev og solgte klokker på nett, skulle sende klokka, så kom klokka aldri frem, og så anmeldte han –forsikringsbedrageri. Og nå husker ikke jeg alle, men en av klokkene hadde han avertert gjennom finn.no hvertfall, og hevdet at det var blitt borte i posten på vei til kjøper. Og det var jo dyre klokker også – 80-90.000,- som han fikk forsikringsutbetaling for. Og der så man jo at han hadde lagt ut samme klokka igjen seinere.*
>
> *3-2, m56: Men ikke sant, vi har jo tatt narkotikaselgere ved å følge dem på Snapchat – det endte jo med at vi pågrep og ransaket hjemme hos ham. Det var jo en som brukte sin private Snapchat-konto til narkotikasalg.*
>
> *3-4, m44: Det var jo en prostitusjonssak også med det for et par år siden. Da kjørte de rundt i bobil, og solgte sex et sted ett døgn, før de kjørte videre til et annet sted. Da ble det jo søkt med en Snapchat-profil for finne ut hvor de befant seg, og jeg tror også vi fant ut hvem som hadde bestilt. Så det ble pågrepet en mann der.*

I eksemplene over kan man tenke at politiet ville fått den samme informasjonen ved å sende en anmodning til tjenestetilbyderne om å ta beslag i aktuelle brukerkonti. Det kan godt hende at det også ble gjort i disse konkrete sakene. Men slike anmodninger vil kreve en juridisk

vurdering, enten av påtalejurist i politiet, eller av domstolene[17], både i Norge og eventuelt i det landet hvor tjenesteleverandøren er basert. Slike anmodninger kan derfor bli avvist, eller i det minste ta tid, som poengtert av en informant:

> *1-3, m28: Ja, det er vel å regne som en ting, som det kan tas beslag i. (…) Jeg er jo kjent med den facebook problematikken når man skal henvende seg til Silicon Valley eller hvor nå hovedkvarteret er. Det var tema i den [navnet på avdøde] drapssaken da den gikk i retten. Da var det en facebook-profil politiet mente var opprettet og de ventet på respons fra Facebook som kom underveis i hovedforhandlingen eller ett eller annet sånn. Så selv om det er en alvorlig sak så må man vente ganske lenge.*

Som en annen informant påpekte kan åpne kilder brukes på et tidligere stadium av etterforskninger og kanskje tre i stedet for, eller i det minste foranledige og styrke grunnlaget for et senere beslag:

> *2-3, m26: Så tror jeg de ser litt mer sånn på det at gjennomgang av noens Facebook profil er noe man gjør når man har tatt beslag da – i skytjenester og sånt. At de ikke tenker på at det er noe som kan gjøres innledningsvis.*

Informantene så også situasjoner hvor åpne kilder kan gi informasjon som ville vært vanskelig å få på annet vis:

> *2-3, m26: Seinest på morgenen i dag så tok jeg et søk på en kar vi muligens skal aksjonere på. Og der fremkommer det av folkeregisteret at han bor alene. Han har barn, men det er jo viktig for oss å vite om han har omsorg for det barnet. Og det fremgår ikke noe sted i de registrene våre hvorvidt han hadde noe omsorg eller var noe sammen med det barnet. Men på et Facebook-søk da, så ser jeg jo det at han regelmessig legger ut bilder hvor han er sammen med datteren sin. Og det er jo god informasjon for oss, og det er jo ganske viktig at vi vet det, sånn vi ikke kommer på adressen der, og så plutselig så sitter det barnet der. (…) Da er det jo sannsynlig at han har barnet, ikke sant. Før det, så visste vi jo ingenting. (...).*

> *3-1, k42: Og det er stor nytte i retten også ofte, når for eksempel to [utenlandske tiltalte] står og hevder at de ikke kjenner hverandre fra før av, og at ingenting er organisert, så kan man finne masse bilder fra åpne profiler der de står med armene rundt hverandre, og har oppgitt at de kommer fra samme landsby og så videre. De er jo nesten i slekt, ikke sant. Det er gull, da. (…) For de utenlandske miljøene, vi klarer ikke etterforske det på en annen måte. Det er veldig vanskelig i hvertfall.*

En annen informant beskrev en bruk av åpne kilder han ikke hadde forsøkt, men så et stort potensial i:

> *1-1, m35: (...) på Snapchat, så har man noe som heter Snapchat Maps, som ligger åpent på internett. (…) Og hvis man da velger et geografisk område (…) så kan man se på alle My stories-ene som ble lagt ut der. For eksempel voldssituasjoner,*

[17] Politiets beslag reguleres gjennom straffeprosessloven (1981) kapittel 16

ting som skjer på byen, fester, sånne ting, så kan man faktisk jo gå inn der ganske lang tid etterpå, mange timer etterpå. Og hvis det skjer et straffbart forhold, så kan man se alle som har tatt opp mobilen og begynt å Snappe det. (...) åpent for alle til å se. Det er jo et kjempeverktøy.

4.2.2. For effektivisering

Gruppene diskuterte også måter åpne kilder, særlig karttjenester og sosiale medier, kan effektivisere politiets arbeid:

1-2, m30: Sånn det har blitt nå med de fleste straksetterforskninger med mye som skal gjøres på stedet, hva bruker du da? Jo, da bruker man mye åpne kilder hvis du trenger noe informasjon. Fordi det å begynne å jobbe på de polisiære kildene ute, det er ikke alltid helt enkelt.

2-6, m33: Jeg har jo brukt kart på Google (...) Jeg har jo guidet patruljer til åsted, for eksempel. Ved å se på oversiktskart hvordan det ser ut i området, og da har jeg brukt «Street View» for å si for eksempel at det er et rødt hus.

3-3, k41: Ja, jeg har jo en sak nå, hvor vi skal ut og pågripe en mann og ransake. En overgrepssak. Og så har vi jo forberedt en aksjon, og vi skal ut og finne ut hvor han er. Er han hjemme? (...) Og så går jeg inn på Facebook og kikker, og så viser det seg at han er på tur til [land i utlandet]. Og det var jo sånn, okey, da sender jeg ikke ut masse kollegaer og leter etter ham da.

4-1, m29: Jeg har brukt en del Google maps, faktisk. Både for det å orientere seg i et område og få inntrykk av det – der er de åpne kartene kanskje bedre enn det politiet selv har. Og se litt mer nøyaktig hvordan ting ser ut – sånn Street view. Da kan man gå inn på bakkeplan og se hvordan det ser ut. Også i avhør, og vise frem til avhørte for at de kan peke ut nøyaktig steder og sånt.

4.2.3. Publikums tillit

Gruppene opplevde vekselvis at publikum både overvurderer og undervurderer politiets bruk av åpne internettkilder. På tvers av alle gruppene ble det uttrykt bekymring for svekket tillit fra publikum, dersom politiet ikke klarer å følge opp eller gjøre de samme undersøkelsene på det åpne internettet som publikum selv kan gjøre:

1-2, m30: For det som ligger åpent, det ligger åpent. Og hvis kjeltringene kan benytte seg av det, så må vi kunne benytte oss av det (...).

1-6, k42: Det er jo nærmest dumt. Det vil iallfall fremstå dumt. Hvis ikke politiet benytter seg av de mulighetene som alle andre ville ha gjort.

4-2, k27: (...) da har de fornærmede fulgt opp, og lurt på hva som skjer, og da vet jeg at de sakene blir henlagt, med melding om at det må du ta med forsikringsselskapet ditt. Og jeg skjønner at publikum ikke synes det er greit, særlig når de har gjort jobben med å finne ut hvem som har stjålet, og så ha de kanskje selv prøvd å kontakte finn.no eller banken for mer opplysninger, men da får de jo beskjed om at de opplysningene kan de kun gi til politiet. Og så blir saken henlagt uten at de opplysningene blir innhentet av politiet.

1-5, k34: (...) det er bare sånne bitte små, helt enkle kjappe grep man kan gjøre, som ville gjort at vi hadde løst en del saker og fått litt bedre anseelse fra publikum, da. Og vi blir jo litt sånn latterliggjort i dette at vi ikke klarer å finne ut av det.

2-4, k36: Det er mange unge jenter som vil ha bilder fjernet fra nettet og tror at vi kan «knipse» og få det vekk. Men det kan vi jo ikke.

3-3, k41: (...) jeg tror også at en ganske stor andel ikke er bevisst på det i det hele tatt heller; mange man prater med, så sier de «ja, men det vet dere vel sikkert fra før av?», mens andre forklarer alt - som om vi ikke vet noe som helst. Så jeg tror det er stor variasjon på bevissthet (...).

> *4-1, m29: Jeg tror kanskje de fleste tror at vi er enda mer til stede enn vi er også – jeg tror ikke de ser problemstillingen med at vi eksponerer oss selv.*
>
> *4-2, k27: Nei.*
>
> *4-1, m29: Og publikum tenker at «jeg har jo funnet dette, hvorfor har ikke politiet?»*
>
> *4-4, k33: Jeg har jo en sak nå, hvor en har tatt seksuelt krenkende bilder, hvor hun forventer at jeg som politi skal fjerne de bildene fra internett.*

Effekten av publikums forventninger, slik informantene beskriver det over, kan sees i sammenheng med UTAUT-konstruksjonen om sosial innflytelse (se tabell 2 i del 3.6.2). Så selv om bruk av åpne kilder ikke er obligatorisk i politiorganisasjonen, virker det som om etterforskerne fortsatt opplever press på å holde tritt med generelle samfunnsutvikling og internettbruk.

4.3. Variasjoner og unntak

Skillet mellom hovedfunn og funnene i denne delen, er at hovedfunnene var gjenstand for utbredt diskusjon på tvers av alle fokusgruppene. Funnene i denne delen fikk i noen tilfeller like stort fokus som hovedfunnene, men kun i enkelte grupper. Selv om de bare ble tatt opp av en eller to grupper, utgjør de nyanser eller motsetninger til hovedfunnene som er relevante å redegjøre for.

4.3.1. Etiske vurderinger

Til tross for at dette var et tema på intervjuguiden, var det kun i én gruppe det ble noe diskusjon om etikken rundt bruk av åpne kilder til etterforskning. Gruppe 3 problematiserte et

tilfelle hvor politiet fulgte en mann på Snapchat med sine private profiler for å kunne holde oppsyn med hans interaksjon med det lokale ungdomsmiljøet, deriblant mange mindreårige.

> *3-3, k41: Det er som på Snapchat, vi har et kron-eksempel her i [by i 3-3s distrikt]. En som er veldig populær blant ungdommer, ikke sant. Så er det politifolk som følger ham da, og det og … er det rett?*
>
> *3-5, k47: Etisk, ja?*
>
> *3-3, k41: Ja, er det etisk? For vi går rett inn og henter inn opplysninger vi kan bruke i en straffesak. Det er jo åpen profil, og alt det der sikkert.*
>
> *3-2, m56: Han ble jo pågrepet han, på bakgrunn av det der.*
>
> *(…)*
>
> *3-3, k41: Men jeg tenker i forhold til Snapchat, når du ber om å bli venn, så må jo den som blir spurt også gjøre en aktiv handling for å godta forespørselen. Så da er det jo et ansvar på dem også, tenker jeg. Å vite hvem man har som følgere.*
>
> *3-5, k47: Å vite at man følges av en politimann, tenker du da, for eksempel?*
>
> *3-3, k41: Ja, det er jo ikke sikkert, men det er hans plikt å gjøre seg kjent med hvem følgerene er.*
>
> *3-2, m56: Men har man 30.000 følgere, så legger man vel kanskje til alle ukritisk?*
>
> *3-3, k41: Ja, men da bør det jo ligge et ansvar på den personen selv og, når man legger ut bilder?*
>
> *3-2, m56: Ja.*

Diskusjonen over kan settes i sammenheng med drøftingen i del 2.6 om forventninger til personvern og notoritet på behandling av personopplysninger. Det kan hende politifolkene i eksempelet over førte god arbeidslogg over undersøkelser foretatt og informasjon mottatt. Men siden det sies «flere politifolk», og mannen burde vite at han følges av politifolk, i stedet for én anonymisert profil, kan indikere en manglende plan i etterforskningen. Drøftingen i del 2.5.2, om hvor informert mannens samtykke til å gi politiet tilgang til profilen hans var, virker også relevant.

Retten til å bli glemt, fra del 2.4.1, ble også eksemplifisert av én informant på følgende vis:

> *3-5, k47: Ja, for jeg og tenker at man utfordres på tillit på en annen måte enn når man bare snakker ansikt til ansikt. Da har man litt lettere for å velge – hva vil jeg si, hva vil jeg ikke si. Det tenker man ikke på nett. (…) hvor nytt og ferskt er dette, står du for det i dag? Og vi samler gjerne informasjon opp mot en hypotese. Og for 2 år siden så uttalte han sånn og sånn om den personen, og da tar vi det til*

inntekt for at dette er en hatefull person, for eksempel. Det skrevne ordets makt er mye større, liksom.

4.3.2. Lav IKT-kompetanse: Torvald Tåke og generasjonsskifte

Manglende generell forståelse av internett og sosiale medier kom nært til å defineres som et hovedfunn. Grunnen til at det ikke er definert slik, er at manglende tiltro til egne eller kollegaers kompetanse kan sees som en variasjon av en mer utbredt bekymring for å gjøre feil, som beskrevet i hovedfunn 1 (del 4.1).

Informanter i gruppe 1 omtalte lav IKT kompetanse nærmest som en del av yrkeskulturen i politiet. Eksemplifisert under ved arketypen «politibetjent Torvald Tåke»; en gjenganger i norsk politikultur ofte brukt for å gi et selvironisk bilde av seg selv eller kollegaer. Torvald Tåke beskrives av Liv Finstad (2000, s. 87) som den «enkle og litt dumme bonden i byen, som ikke vet opp og ned på hverken håndjern eller datamaskiner».

> *1-1, m35: Og hvis du sitter på arbeidsstasjonen din, som alle vi «Torvalder» gjør, så har vi en falsk facebook-profil og vi driver og bruker den og skal være smarte og liksom jobbe i det skjulte selv om vi er på åpne kilder.*

> *1-7, m53: I tredje etasje på skjult [etterforskning] så hadde man frittstående internett PC-er med gul kabel, hehe. Så satt man på gul kabel, så var det frittstående.*
>
> *1-1, m35: Mmm, hos politifolk så bør jo vel nesten bare skjermen være gul, og hele PC-en, for å være sikker på at det er rett PC.*

Dette kan indikere et ganske dystopisk syn på kompetansenivået innen data og internett i politiet. Heldigvis virket denne diskusjonen å foregå med et glimt i øyet, og flere av gruppemedlemmene smilte da Torvald-referansen dukket opp i samtalen over. Andre informanter så etterslepet innen politiets internettkunnskap mer som et generasjonsskifte – hvor de yngre politiansatte, som i større grad har vokst opp med internett som en naturlig del av sin hverdag, bør ta ansvar for å ta i bruk åpne kilder i sitt etterforskningsarbeide:

> *3-2, m56: Sånn generelt, så opplever jeg at de etterforskerne som er en generasjon yngre enn meg, de søker på facebook automatisk nærmest, bare for å se.*

> *1-6, k42: Vi har nesten til enhver tid studenter [politistudenter i praksis], vi bruker dem sikkert alt for dårlig. De er sikkert 10 ganger så flinke som meg på alt dette her. Sosiale medier og hvordan man kan hente ut ting.*
>
> *1-1, m35: Hvertfall nå, når noen av dem er 19 år gamle.*

> *2-6, m33: Man ser jo bare de som er i generasjonen over oss i politiet, hvor lite kunnskap de har – de blir akterutseilt på noe, fordi vi unge kommer og kan liksom dagens teknologi.*
>
> *2-2, k40: Takk skal du ha, haha.*
>
> *2-6, m33: Jeg snakker om folk som er eldre enn deg (...). For eksempel på operasjonssentralen da. Det er det jo sånn et generasjonsskifte. De henger ikke med, for de bruker ikke dataen på den måten vi har brukt den og er vant med. De har vært kjempegode før, og så plutselig så fungerer det ikke så veldig godt fordi de ikke henger med.*

4.3.3. Drukningsfare og kilder i stadig endring

Den potensielle informasjonsmengden man kan få ut av åpne kildesøk beskrives av noen informanter som et hinder i seg selv:

> *1-7, m53: Benytter du alle muligheter, så får du en enorm datamengde, som politiet må nyttiggjøre seg, og står man da kapable til å ta hånd om all den informasjonen som man får? For dette er jo bare en brøkdel av en etterforskning; det strømmer jo til med masse annet. Som gjør at man kan drukne i informasjon, som gjør at saken kanskje blir veldig uoversiktlig å etterforske, for man sitter på så mye informasjon.*
>
> *1-5, k34: Det er jo en møysommelig jobb. Det tar jo mye tid. Om man skal sitte og finne disse koblingene, og få skrevet det ned og utarbeidet i form av rapporter eller hva det enn blir da.*

Dette speiler forventningen forespeilet i del 2.4.3 – informasjonsmengden kan like gjerne bli et problem heller enn en ressurs, dersom man ikke evner å bearbeide dataene på en god måte. I forlengelsen av dette, påpekes det at trender og bruksmønstre på sosiale medier endres raskt og ofte, særlig blant yngre brukere:

> *2-3, m26: Jeg jobbet på forebyggende [avdeling for forebygging av kriminalitet blant unge] før jeg begynte her, og de unge bruker jo ikke Facebook lenger, det er jo så mye andre ting. Og vi har ikke peiling, vi ligger jo etter. Asså, jeg er jo 26, og ligger langt bak når det kommer til akkurat det der med sosiale medier. Det endrer seg hele tida. Det er nye apper og nye ting, så mye som skjer.*
>
> *1-1, m35: Mange ganger så bør man jo nesten ha trilla hit en ungdomsskoleklasse og kunne bare spørre: hvor er det, vi er ute etter sånn, hvor er det vi må gå. For de bytter jo fora nesten kjappere enn jeg bytter sokker.*

4.3.4. Uformelle eksperter

Når gruppen hadde beskrevet eksempler på at de hadde god bruk av åpne kilder, var oppfølgingsspørsmålet mitt ofte hvor de hadde lært å gjøre dette. Svarene var ofte at lærdommen var litt tilfeldig, og hadde skjedd uformelt og tilfeldig.

> *1-1, m35: Snakke med kollegaer som jobber andre steder. Som jobber hos Kripos og som jobber i politidistriktene. Utveksle tanker og idéer. Uformell kunnskapsutveksling*

Andre viste til hjelp fra datakyndige kollegaer. Altså uformelle eksperter – ildsjeler med kompetanse fra personlig interesse for internett og teknologi, og som har funnet sine egne måter å anvende dette på til politiarbeid. Informantene med en slik ressursperson på sin arbeidsplass, beskrev det som nyttig:

> *3-5, k47: (...) For vi har jo en på kontoret, jeg vet ikke hvor mange venner han på Facebook, men han er jo venn med alle som er i våre søkelys.*
>
> *Int: Venn med dem via sin egen private identitet?*
>
> *3-5, k47: Ja, han er en som alle kriminelle i hele distriktet vårt har en relasjon til. Han har jobbet i kjempemange år, og er det mest tålmodige og snilleste vesenet man kan tenke seg. Alle skal snakke med ham, og alle er venn med ham på Facebook. Og nå igjen nå, så vi satt og diskuterte på et morgenmøte om hvor noen vi lette etter var, og denne kollegaen bare «nei, han har lagt ut på Facebook, han er der». Så det er liksom kilden hans, og det blir vår kilde og, da. Så det blandes jo sammen. Hele tiden.*

Men jo nyttigere det er, jo mer sårbart kan det bli dersom alle av åpne kildesøk avhenger av et fåtall eksperter. Hva skjer om ressurspersonen fra samtalen over for eksempel om blir utilgjengelig – er på ferie, syk, eller bytter stilling? Tilgang til dyktige kollegaer kan da bli et hinder i å bygge egen kompetanse, hvis man overlater alt til de uformelle ekspertene:

> *3-4, m44: Mmm. Men det er ikke mye som skal til for å heve kompetansen til hver enkelt av oss da? Hvor mye skal til egentlig?*
>
> *3-2, m56: Men det er ikke nok, altså. Han som er god på det hos oss, han er jo på et mye høyere nivå enn meg. Men det hadde vært greit å ha flere slike å spille på. Han rekker jo nesten ikke å gjøre noe annet enn å hjelpe med etterforskning på nett. Alle kommer og spør han.*
>
> *3-3, k41: Så blir vi jo litt sløve også på et vis også da, for da trenger vi jo ikke å lære oss det, så lenge vi har noen som kan det.*
>
> *(...)*
>
> *3-1, k42: At vi har han (...) det er jo helt tilfeldig at han jobber her, og at han er så flink på internettkilder?*

Å legge all etterforskning på internett til de mer formelle ekspertene, som dataetterforskere og andre spesialister er også vanskelig, fordi de er relativt få i forhold til den potensielle nytteverdien av åpne kildesøk i nærmest alle saker, som beskrevet i del 1.2. En av informantene hadde selv tilsynelatende fått status som en lokal ekspert på data:

> *2-3, m26: Jeg ble jo selv ganske overrasket da jeg begynte i politiet – det er jo bare to år siden. Så ble jeg overrasket over hvordan kunnskapen på data var. At jeg kom inn som nja, datainteressert, og plutselig ble jeg liksom IKT ansvarlig på hele seksjonen. Det reflekterte jeg litt over da – «jøss, er vi ikke lengre enn det?» Det er jo der man er, altså folk er jo der – på sosiale medier og på nett. Så blir man flinkere på det.*

Det hører med at informanten over altså på intervjutidspunktet var ansatt på en stor politistasjon. Hans egen overraskelse over å få rollen som en uformell IKT ansvarlig kan skyldes beskjedenhet om egne ferdigheter – men kanskje også at behovet for ansatte med datakompetanse ikke ble tilstrekkelig ivaretatt gjennom arbeidsgivers rekruttering og virksomhetsstyring.

5. Analyse av funn

Kapittelet innledes med en vurdering av hvordan funnene kan ha blitt påvirket: først av meg som person, deretter av forskningsmetoden og til sist av egenskaper ved informantene selv. Deretter følger en håndfull analysetema som søker å belyse sammenhenger mellom funn fra den empiriske undersøkelsen med teorien som utgjør grunnlaget for studien. Del 4.4 tolker funnene i lys av prosjektets teori, forskningsmetode og problemstilling. I del 4.5 konseptualiseres funnene i en modell jeg har kalt teknologiakseptanse perspektiv, eller TAP.

5.1. Refleksivitet og feilkilder

Refleksivitet innebærer at forskeren redegjør for personlige bias og forventninger til prosjektet for å øke påliteligheten til funn og fortolkningen av dem (Fog, 2004; Sim, Huang, & Hill, 2012; Tjora, 2012). Refleksivitet kan oppsummeres med spørsmålet «Hvordan påvirker jeg som person denne studien?». Det kan ikke gis et svar på i forkant av undersøkelsen, men er noe forskeren må «forholde seg til og reflektere over gjennom hele intervjuundersøkelsen» (Kvale et al., 2015, s. 87).

Forskningsdata er aldri en fullkommen gjengivelse av virkeligheten – de genereres gjennom metodiske verktøy (Johannessen et al., 2010). Jo mer pålitelig verktøy, jo mer troverdig fremstår dataene det genererer (Dahler-Larsen, 2008). Et verktøy kan styrke sin pålitelighet ved at det redegjøres for virkemåten, slik at andre i prinsippet kan reprodusere forskningsresultatene (Merriam & Tisdell, 2016). Som moderator og ordstyrer i fokusgruppen er forskeren selv verktøyet som genererer data, gjennom interaksjon med respondentene (Fog, 2004; Mason, 1996).

Jeg var selv moderator i alle fokusgruppene. Da designet intervjuguiden, måtte bestemme hvor mye jeg skulle si til informantene om meg selv. Det ville virke respektløst å ikke introdusere meg selv når jeg ber deltakerne oppgi personlig informasjon som alder og yrkeserfaring. I tillegg kjente jeg enkelte deltakere i noen av grupper fra før av, så det ville blitt forskjellsbehandling mellom gruppene. Derfor var jeg åpen med informantene om at jeg selv jobbet som etterforsker i politiet. Samtidig gjorde jeg det veldig klart da jeg introduserte meg at jeg var langt ifra noen ekspert på temaet, at jeg ikke hadde noen fasit på spørsmål og problemstillinger jeg tok opp, og at jeg var der for å finne gode diskusjoner, ikke teste deres kunnskap.

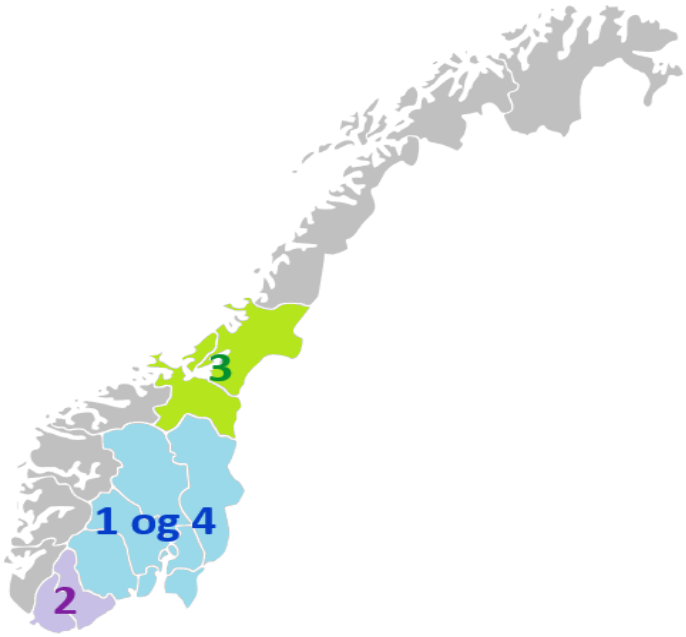
Å gjøre det tydelig for informantene at jeg selv jobber med etterforskning, kan også medføre vansker. Når jeg som etterforsker ønsker å påvirke og endre egen profesjon gjennom dette prosjektet, kommer det nært såkalt aksjonsforskning (se del 3.4). Aksjonsforskning prøver ofte å sammenligne hva som *er*, og hva som *burde være*. Dersom informantene føler seg negativt sammenlignet opp mot den endringen jeg ønsker meg, kan det lede til at de føler seg utnyttet, og at jeg som innsideforsker svikter kollegasolidariteten (Barbour, 2014, s. 98). Dette kan også sees i sammenheng med den etiske drøftingen rundt innsideforskning (del 3.9.3).

Berit Brandts (1996) observasjoner (fra 3.9.1) om at «det deltakerne forteller forskeren, forteller de samtidig de andre i gruppen», kan også indikere utfordringer med fokusgruppeformatet når diskusjoner blir kritiske til egen praksis eller kunnskap. Det kan være tøft nok å erkjenne kunnskapshull ovenfor seg selv – desto vanskeligere når det blir en plenumsøvelse, med en moderator som selv er fagutøver og noterer det som blir sagt. Slike situasjoner eksemplifiserer viktigheten av forskningsetiske prinsipper som konfidensialitet og et informert samtykke, som drøftet i del 3.9. Alle forskningsmetoder har da også sine fortrinn og svakheter, og jeg synes tidligere drøftinger om forskningsmetodikk (del 3.3) står seg:

Fordelene forskningsmetoden fokusgrupper tilførte denne undersøkelsen veier opp for muligheten om at enkelte informanter kan ha vært tilbakeholde. Jeg registrerte heller ikke tegn til ubehag, hverken under gruppediskusjonene eller senere.

Selv om jeg personlig ser åpne kilder som et potensielt netto positivt bidrag til nærmest alle typer etterforskninger, har jeg også full respekt og forståelse for bekymringer og motargumenter fremmet av intervjugruppene. Jeg opplevde velbegrunnede, nyanserte diskusjoner både for og imot bruk av åpne kilder, med et positivt debattklima i alle gruppene. Det var kanskje de nettopp de kritiske argumentene jeg lærte mest av, og jeg håper at funnkapittelet reflekterer dette.

Som påpekt i 3.5, er det i viktig at homogene grupper er tilstrekkelig varierte for å skape debatt. I denne studien varierte informantenes kjønn, alder, erfaring og arbeidssted. Det ble også påpekt relevant å kontrollere for innflytelsen av et gruppemedlem som kan få ekspert-status, fordi de kan uproporsjonalt påvirke gruppas synpunkter og hemme diskusjon. For å imøtekomme disse hensynene viser først figur 5 et norgeskart som er fargemerket i den landsdelen hvor gruppemedlemmene jobbet til vanlig, og hvor intervjuet med den aktuelle gruppen fant sted. For å kunne skille dem, ble gruppene nummeret fra 1–4 i den rekkefølgen de ble intervjuet. Tabell 3 viser fordelingen av informanter (N), kjønn, alder og erfaring, både gruppevis og for hele utvalget.



Figur 5 – Fokusgruppenes geografiske tilhørighet

	N	Kjønn		Alder (år)		Yrkeserfaring i politiet (år)	
		Kvinner	*Menn*	*Gjennomsnitt*	*Median*	*Gjennomsnitt*	*Median*
Gruppe 1	7	2	5	37	35	10,1	6
Gruppe 2	6	4	2	32,8	34,5	8,5	11
Gruppe 3	5	3	2	46	44	20,8	19
Gruppe 4	4	3	1	28,75	28	3,25	3,5
Total	**22**	12 **55 %**	10 **45 %**	**36,4**	**35,5**	**10,9**	**11,0**

Tabell 3 – Demografisk fordeling av utvalget

Utvalget består altså av 22 informanter totalt. Begge kjønn er representert i alle grupper, med en ganske balansert gjennomsnittlig kjønnsfordeling. En gjennomsnittlig informant er ellers i midten av 30-årene, med rundt 11 års erfaring i politiyrket. Hver informant introduserte seg med sin stilling innledningsvis i intervjuet, og utvalget bestod av hovedsakelig av etterforskere, men også etterforskningsledere, påtalejurister, samt operatører fra operasjonssentraler og ordenspoliti som for tiden hospiterte ved en etterforskningsavdeling.

Potensiell «ekspert-effekt» kan tenkes å oppstå i grupper hvor én informant har betydelig høyere alder, lengre yrkeserfaring enn resten av gruppa. Derfor beregnes alder og yrkeserfaring med både gjennomsnitt og medianverdier. Dette er fordi gjennomsnittet vil være høyere enn medianen dersom én informant i gruppa har mye høyere alder eller mer yrkeserfaring enn resten av gruppa – også kalt et skjevt utvalg[18]. Tabell 3 viser en slik differanse for yrkeserfaring i gruppe 1, hvor gjennomsnittet på 10,1 år er nesten det dobbelte av medianberegningen på 6 år. Allikevel var debatten jevnt fordelt mellom gruppemedlemmene, og det virket ikke som noen fikk en ekspert-status i gruppa.

Til sist er det verdt å merke seg at innen teknologiakseptanseteorien undersøkelsen støtter seg til, ikke er relevant hvor korrekt informantenes forståelse av en gitt teknologi er. Eksempelvis hvordan Facebook genererer venneforslag, eller muligheter for IP-sporing av politiets bevegelser på internett. William og Dorothy Thomas sa det på følgende måte allerede i 1929 (sitert i Barbour, 2014, s. 21): «If people believe things to be real, then they are real in their consequences», og Barbour (ibid., s. 22) følger opp med «Misconceptions may have their own internal validity, and public or lay perspectives can be very sophisticated».

[18] https://web.ma.utexas.edu/users/mks/statmistakes/skeweddistributions.html

Det interessante i studien er altså informantenes oppfatninger, fordi de former deres holdninger, som igjen uttrykkes ved adferd – i dette tilfellet bruk av åpne internettkilder til etterforskning. Resten av analysen fokuserer på oppfatninger jeg har formet gjennom arbeidet med dette prosjektet.

5.2. Usikkerhet rundt regelverk og grenser

Teorien pekte ut tre områder hvor regelverket kan være vanskelig: Først å kunne skille søk på åpne kilder til etterforskning fra politiets etterretningsvirksomhet (2.2.1). Deretter å forstå grensegangen mellom ulovfestet spaning på internett til de mer lovregulerte skjulte etterforskningsmetodene som infiltrasjon og informantbehandling (2.3.4). Og til sist reglene som gjelder for politiets behandling av personopplysninger (2.6) og faren for at personidentifiserende informasjon kan havne på avveie, for eksempel dersom de søkes med på åpne kilder (2.3.3).

Her samsvarer teori og empiri relativt godt. Intervjugruppene identifiserte ikke utfordringer med at søk på åpne kilder kan bryte med personvernlovgivningen. Men det er kanskje forståelig, fordi et hovedfunn var at informanter beskriver at de mangler kunnskap om reglene, eller at reglene i seg selv er diffuse og vanskelig å forholde seg til i praksis. (4.1.2).

5.3. Manglende praktisk tilrettelegging

Et annet sentralt hovedfunn et at informantene savner struktur i politiorganisasjonen som legger til rette for å bruke åpne internettkilder til etterforskning (4.1.1). Dette står i direkte kontrast til teorien, hvor en sentral litteraturkilde er felles veileder for politiets bruk av åpne kilder til politimessige formål (Kripos, 2018), som er tilgjengelig på politiets intranett over hele landet. Kun én av informantene refererte eksplisitt til denne under intervjuene (del 4.1.1, side 50). Dette kan tyde på at søk på åpne nettkilder som en faglig forankret etterforskningsmetode med nasjonale standarder fortsatt er helt i startfasen.

I tillegg etterlyser informantene utstyr, som frittstående datamaskiner, dedikerte internettlinjer og nøytrale nettprofiler, slik at de kan søke på åpne kilder uten å legge igjen uønskede spor. Dette er spor informantene tenker kan eksponere dem som privatperson, utsette politiets nettverk for dataangrep, eller risikere etterforskningens operasjonelle sikkerhet. Teorien anerkjenner også nødvendigheten av at politiet under noen omstendigheter skjuler sin opptreden på internett (2.3.2).

Det kan det være betryggende at informantene er nølende med å ta i bruk en metode de ikke helt kan se omfanget eller konsekvensene av. Det fremstod for meg som det var profesjonalitet og et ønske om å jobbe forsvarlig som lå til grunn for mye av informantenes skepsis til bruk av åpne kildesøk til etterforskning. Dette er også i samsvar med UTAUT-modellen, hvor konstruksjonen «Tilrettelegging» direkte påvirker på «faktisk bruk» av en teknologi (se figur 3 i del 3.6.2). Altså vil selv de sterkeste intensjoner blant politifolk om å bruke åpne internettkilder ikke føre til mye faktisk bruk, så lenge det ikke tilrettelegges for i organisasjonen.

5.4. Usikkerhet og notoritet

Teorien spår utfordringer med politiets evne til å sile anvendelig informasjon og bevis ut av stadig større mengder tilgjengelig data (2.4.3). Enkelte informanter så den potensielle informasjonsmengden fra internett som et hinder for å bruke av åpne kilder – både fordi de mente saken kan blir veldig uoversiktlig og vanskelig å etterforske, og fordi det krever mye tid og ressurser å bearbeide slike datamengder (4.3.3).

Teorien viser til at notoritet derfor er nødvendig for å beholde oversikt og kontroll, og poengterer at det også er pålagt ved søk på åpne kilder til etterforskningsformål (2.4.2). Notoritet ble også drøftet av informantene, men de tok det opp med en litt annen vinkling, nemlig for å håndtere upåliteligheten de assosierte med allment tilgjengelige nettkilder (4.1.3). Samlet sett kan man si at både store informasjonsmengder og det å skulle vurdere pålitelighet begge dreier seg om å redusere usikkerhet gjennom god notoritet.

5.5. Få etikkdiskusjoner

Jeg fant kun én diskusjon relatert til etikken i bruk av åpne kilder (4.3.1) Jeg kunne ønsket det var flere. Teorikapittelet utledet flere moralske og etiske konsekvenser jeg synes er interessante og viktige, og informasjonsskrivet til deltakerne (vedlegg 1) presenterte derfor etikk som et hovedtema. Men manglende diskusjon om et tema sees som et funn i seg selv. Som nevnt i 2.5.2, ble jeg ikke selv bevisst på mange av de etiske problemstillingene rundt politiets bruk av åpne kilder, kanskje særlig sosiale media, til å etterforske personer. Jeg tror ikke det er dekning i intervjudataene til å konkludere, men man kan tenke seg flere årsaker til lite etikkdiskusjon: At metoden er relativt ny eller lite brukt. Oppfatninger om at enhver er ansvarlig for hva man velger å dele om seg selv på nett, og konsekvensene som følger. Eller kanskje at politiet er såpass vant med å samle inn og anvende sensitiv personinformasjon fra

andre kilder i etterforskningen, eksempelvis avhør eller beslaglagte mobiltelefoner, at etiske vurderinger rundt åpne kildesøk blir trivielle.

5.6. Metodetillit, selvtillit og publikums tillit

Fokusgruppenes oppfatninger av fordelene med åpne kilder var oppløftende, særlig fordi det ikke begrenset seg til generell synsing, men også var basert på konkrete eksempler på hvordan åpne kilder hadde vært avgjørende i både oppdagelse og oppklaring av straffesaker (4.2.1), og som et nyttig hverdagsverktøy generelt (4.2.2).

Men det kanskje mest interessante funnet var at alle fokusgruppene poengterte viktigheten av å innfri publikums forventninger til at politiet må kunne etterforske på internett (4.2.3). Hvis vi tolker publikumsforventinger som sosial innflytelse, avviker dette funnet nemlig sterkt fra UTAUT-modellen (3.6.2), som sier at sosial innflytelse ikke vil ha effekt på bruksintensjon når bruk av teknologien ikke er obligatorisk. Ingen av gruppene virket å anse bruk av åpne kilder som obligatorisk på sin arbeidsplass. Oppfatninger om arbeidsgivers manglende tilrettelegging for søk på åpne kilder (del 5.3) indikerer heller kanskje det motsatte – at åpne kildesøk er reservert for politifolk med spesialistkompetanse og eget utstyr.

Til tross for opplevd manglende tilrettelegging så flere informanter nødvendigheten av at politiet må kunne gjøre undersøkelser som kan gjøres av enhver i besittelse av en mobiltelefon og litt kunnskaper om hvordan internett fungerer. Det kan vitne om en vilje til å ta personlig ansvar for yrket sitt når etterforskerne føler press på å bli bedre på dette området. Den enkle løsningen kunne kanskje være å skylde på systemet og byråkratiet. I stedet ser man i undersøkelsen fenomenet uformelle eksperter (4.3.4), som tar initiativ til å gjøre internettundersøkelser, uten at det trenger å stå «dataetterforsker» i stillingsbeskrivelsene deres.

Glimt i øyet til tross, kan «Torvald Tåke» diskusjonen også være uttrykk for reell teknologipessimisme fra intervjudeltakerne som ser politiet generelt som en tungrodd og lite tilpasningsdyktig institusjon, som aldri vil klare å holde tritt med det digitale samfunnet. På en annen side virker det som det å søke informasjon fra internett blir stadig mer normalisert, slik at terskelen for å ta i bruk åpne kilder vil bli tilvarende lavere med tiden.

For andre informanter virket det som om skepsisen til å bruke åpne kilder skyldes personlige forutsetninger, som for eksempel en oppfatning om at de var dårlige på IKT og internett generelt. Men lavere tro på egne forutsetninger utelukket imidlertid ikke at man samtidig

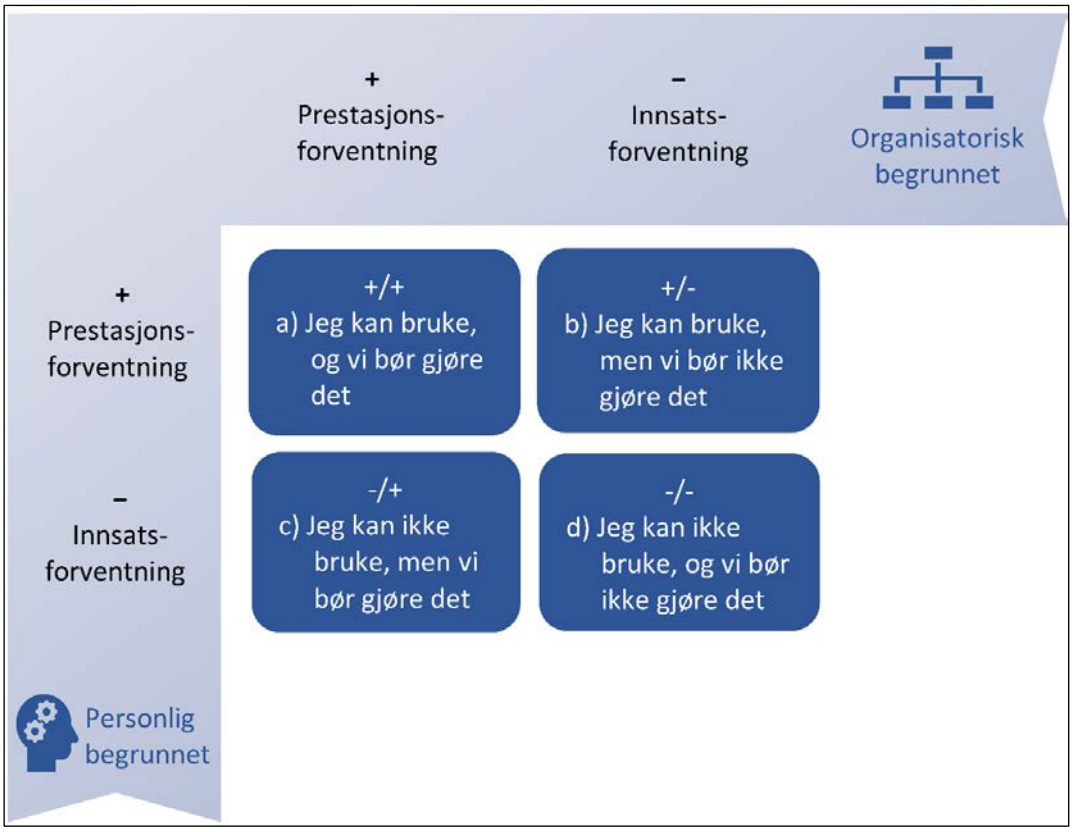
kunne synes at kollegaer burde bruke metoden, og at åpne nettsøk kan lette etterforskningsarbeidet generelt. Denne tosidigheten i deltakernes perspektiver dannet grunnlaget for den neste og siste delen av kapittelet, hvor funnene oppsummeres i en typologi jeg har kalt teknologiakseptanse perspektivmodellen (TAP-modellen).

5.7. Teknologiakseptanse perspektiver

Begrunnelsene informantene har oppgitt for å bruke eller ikke bruke åpne kildesøk kan generelt deles i to kategorier:

1. Personlige begrunnelser, relatert til den enkeltes forutsetninger og egen arbeidssituasjon. For eksempel prestasjonsforventning om å spare tid og innsats i sin egen arbeidshverdag ved å benytte åpne nettkilder. Eller innsatsforventing fordi man tenker man kan for lite om sosiale medier eller juridiske grenser til å gjøre åpne kildesøk på en god måte.
2. Organisatoriske begrunnelser, som stammer fra forhold og strukturer utenfor en selv. Prestasjonsforventninger som at politiet bør nyttiggjøre seg av informasjon som «alle og enhver» har tilgang til. Innsatsforventning grunnet i arbeidsgivers manglende opplæring og utstyr til å kunne forsvarlig etterforske på internett. Også etiske motforestillinger, som for eksempel at politietaten systematisk nytter informasjon ment for sosiale media til kriminaletterforskning, kan sees som en innsatsforventning i denne kategorien.

Figur 6 kombinerer disse personlige og organisatoriske begrunnelsene med to av UTAUT-modellens konstruksjoner, prestasjonsforeventing og innsatsforventning. Altså henholdsvis positive forventninger om hvilke prestasjoner man kan oppnå, og negative forventninger om hvilken innsats som kreves (som definert i tabell 2 i del 3.6.2). Slik kan det oppstilles en matrise av 4 hovedtyper av perspektiver på bruk av åpne internettkilder til etterforskning.



Figur 6 – Teknologiakseptanse perspektiver (TAP-modellen)

TAP-modellen beskriver perspektivene med to komponenter – «Hva jeg kan» som ansatt, og «hva vi bør gjøre» som en organisasjon. Avhandlingen gir ikke grunnlag for å si noe om utbredelsen av de 4 perspektivene, hverken blant totalpopulasjonen eller utvalget i studien (se del 3.5). Hensikten er heller å sammenfatte empirien fra undersøkelsen. TAP-modellen kan også skissere noen mulige fremtidige tiltak politiet kan iverksette for å øke sin etterforskningskapasitet på internett ved å få flere etterforskere til å gjøre åpne kildesøk. Dette drøftes i neste og avsluttende kapittel.

6. Avslutning

6.1. Oppsummering av funn og analyse

Undersøkelsen fant at de som jobber med etterforskning i politiet er bekymret for å bruke åpne internettkilder på feil måte. Det var tre hovedtyper feil alle intervjugruppene uttrykte bekymring for: (1) Å legge igjen spor på internett som kan eksponere dem som privatpersoner eller ødelegge etterforskningen. (2) Å tråkke over juridiske grenser grunnet uklarhet om reglene som angår bruk av åpne kilder. (3) Feilvurderinger grunnet vansker med å vurdere informasjonspåliteligheten fra åpne internettkilder. Samtidig verdsettes også de åpne kildene: De tilbyr rask og enkel tilgang til informasjon, som kanskje ikke finnes i offentlige databaser. Åpne kilder ble beskrevet som avgjørende i oppdagelsen og oppklaringen av flere kriminalitetstyper. Disse fordelene skaper også forventinger, både fra publikum og de politiansatte om at politiet skal kunne etterforske og håndheve loven på internett.

Etikkdiskusjoner om bruk av åpen kildeinformasjon til politiformål var fraværende i mesteparten av fokusgruppene. Mer data om dette temaet hadde vært ønskelig. Allikevel kan manglende diskusjon om et tema sees som et funn i seg selv. Andre, mindre utbredte funn var oppfatningen av at politifolk ofte er dårlige på å forstå og ta i bruk ny teknologi, eksemplifisert ved arketypen «Torvald Tåke». Enkelte informanter mente den tilgjengelige informasjonsmengden fra internettundersøkelser i seg selv kan bli uhåndterbar. Andre beskrev at kollegaer eller de selv hadde fått status som uformell ekspert på datarelatert etterforskning; oftest grunnet personlig initiativ og interesse, snarere enn formalkompetanse og stilling. Disse uformelle ekspertene verdsettes av informantene, men noen så også faren for at ekspertene kan bli en «sovepute» som hindrer dem å bedre sin egen IKT-kompetanse.

Usikkerhet om regelverket gikk tydelig igjen i undersøkelsen – fra å se forskjellen på åpne kildesøk til etterforskning og politiets etterretningsvirksomhet, til å forstå grensegangen mellom ulovfestet spaning på internett til de mer lovregulerte skjulte etterforskningsmetodene som infiltrasjon og informantbehandling.

En annen tolkning av hovedfunn er at det mangler praktisk tilrettelegging for åpne kildesøk ved avdelingene. Samtlige intervjugrupper mente de manglet utstyr før de kunne gjøre søk på åpne kilder på en måte som beskyttet både den politiansattes privatliv, etterforskningens operasjonelle sikkerhet og politiets datanettverk fra trusler som virus eller cyberangrep. Teori

innen forskningsfeltet teknologiakseptanse brukes som et analytisk rammeverk for undersøkelsen, og viser til at slik mangel på tilrettelegging vil forhindre selv høyt motiverte ansatte fra å ta i bruk søk på åpne kilder i sitt arbeide.

Internett utfordrer tradisjonelle syn om etterforskning med åpen tilgang til enorme datamengder. Gruppene så utfordringen med å skulle bearbeide disse mengdene til nyttig informasjon uten å miste tråden i etterforskningen, eller å bruke uforholdsmessig mye tid og ressurser. Teorien peker også på utfordringen med at informasjon sjelden forsvinner fra nettet, og at politiet vil måtte forholde seg til stadig økende datamengder i tiden fremover. For å beholde kontrollen, peker teorien på viktigheten av god notoritet for alle undersøkelser politiet gjør. Informantene tok også opp notoritet i intervjuene, men da først og fremst som et verktøy for å øke påliteligheten av informasjon som samles inn via åpne kilder.

Gruppene hadde flere eksempler på at verktøy som karttjenester satte dem i stand til å jobbe mer effektivt, samt tilfeller hvor åpne nettkilder som sosiale medier var avgjørende for å oppdage straffbare forhold, så vel som å løse dem. Flere informanter beskrev også et forventningspress fra publikum om at politiet i minste fall må kunne foreta de samme undersøkelsene på internett som alle andre. Dette står i kontrast til UTAUT-modellen innen teknologiakseptansen. UTAUT indikerer at et slikt forventningspress fra publikum i teorien ikke burde påvirke politifolkenes intensjon om å bruke åpne kilder, så lenge det frivillig. I lys av den manglende tilretteleggingen fra arbeidsgiverne, oppfattet ingen informanter bruk av åpne kilder som obligatorisk.

6.2. Veien videre

Dette prosjektet startet som et vagt konsept for rundt 3 år siden, da jeg først begynte å bruke åpne internettkilder og frem til i dag. Erfaringene jeg har gjort meg siden oppstarten har overbevist meg om at det finnes en videre vei å gå, selv om dette prosjektet avsluttes med innleveringen av denne avhandlingen.

Første steg på den videre veien kan kanskje starte fra en av de siste i dette prosjektet, nemlig TAP-modellen (5.7, figur 6). TAP sier at politifolks perspektiver på åpne kilder kan begrunnes i enten det organisatoriske eller personlige. Første prioritet bør være å adressere de organisatorisk begrunnede innsatsforventingene, fordi basert på analysen av funn (5.3), bør de kunne reduseres betraktelig ved at de ansatte får tilgang til internettilkobling og datamaskiner som er frittstående fra politinettverket. I første omgang vil det kunne aktivisere

de som allerede har tilstrekkelig personlig kunnskap og interesse, slik som de uformelle ekspertene (4.3.3). Med støtte i Kriposveilederen (2018) bør de deretter kunne starte med åpne kildesøk, og drive opplæring av kollegaer, som kan redusere deres personlig begrunnede innsatsforventninger.

Som illustrert i empirien endres stadig hvilke åpne kilder som er aktuelle for politiet, og hvilke metoder som er best for å sikre mulige bevis fra dem. De vil derfor være viktig at den nasjonale standarden etablert med den første Kriposveilederen (ibid.) oppdateres og distribueres ved behov, for å sikre kvalitet og etterrettelighet ved metoden. Det kan kanskje også være fordelaktig at kommunikasjonen om slik utvikling av metoden kan gå begge veier, for å sikre størst mulig grunnlag for erfaringslæring.

Gitt den lille mengden tidligere forskning, fremstår kunnskapshullene i forskningen som åpenbare. Min anbefaling til videre forskning vil derfor være å kartlegge faktisk bruk av åpne kilder i norsk politi. Å kunne tegne opp noen grenser, for å en bedre forståelse av omfanget av fenomenet, vil kunne være til stor hjelp dersom man ønsker å implementere åpne kilder som en utbredt etterforskningsmetode i hele landet.

Den overordnede målsettingen for det videre arbeidet skissert i dette delen vil være at politiet først øker sin kapasitet til å etterforske på internett ved å sette flere ansatte i stand til å foreta åpne kildesøk. Økning i denne kapasiteten, supplert med oppdatert kunnskap om fenomen og arbeidsmetoder vil kanskje sette politibetjent Torvald Tåke i kontakt med den teknologiske utviklingen i samfunnet – eller i det minste redusere forspranget.

Litteratur

Barbour, R. S. (2014). *Introducing qualitative research : a student's guide* (2. utgave). London: Sage.

Bjerknes, O. T., Fahsing, I. A., & Bergum, U. (2018). *Etterforskning : prinsipper, metoder og praksis*. Bergen: Fagbokforlaget

Boyd, D. & Marwick, A. E. (2014). Networked privacy: How teenagers negotiate context in social media. *New media & society, 16(7)*, 1051-1067.

Bradley, M., & Daly, A. (1994). Use of the logit scaling approach to test for rank-order and fatigue effects in stated preference data. *Transportation, 21*(2), 167-184.

Brand, A., Daly, F., & Meyers, B. (2003). Metadata demystified. *Bethesda, MD*, 1-19. Hentet fra https://www.niso.org/sites/default/files/2017-08/Metadata_Demystified.pdf

Brandt, B. (1996). Gruppeintervju: perspektiv, relasjoner og kontekst. I H. Holter & R. Kalleberg (Red.), *Kvalitative metoder i samfunnsforskning* (2. utg., s. 145-165). Oslo: Universitetsforlaget.

Brandtzæg, P. B. (2013). Big Data – på godt og vondt. Hentet fra https://www.sintef.no/siste-nytt/big-data-pa-godt-og-vondt/

Bruce, I., & Haugland, G. S. (2014). *Skjulte tvangsmidler*. Oslo: Universitetsforlaget

Chilton, M. A. (Ed.). (2013). *Knowledge Management and Competitive Advantage: Issues and Potential Solutions*. Hentet fra https://www.researchgate.net/profile/Neeta_Baporikar/publication/297364708_Organizational_barriers_and_facilitators_in_embedding_knowledge_strategy/links/5b9f9b4492851ca9ed112c26/Organizational-barriers-and-facilitators-in-embedding-knowledge-strategy.pdf

Clough, J. (2014). A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation. *Monash UL Rev.*, 2014, 40: 698. Hentet fra https://www.researchgate.net/profile/Jonathan_Clough/publication/277892666_A_World_of_Difference_The_Budapest_Convention_On_Cybercrime_And_The_Challenges_Of_Harmonisation/links/55765ddc08ae75363751ab41/A-World-of-Difference-The-Budapest-Convention-On-Cybercrime-And-The-Challenges-Of-Harmonisation.pdf

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, 6(23), 31. https://doi.org/10.19101/IJACR.2016.623006

Cross, M. A. K. D., & Mai'a, K. (2011). EU intelligence sharing & the joint situation centre: A glass half-full. I: *delivery at the Meeting of the European Studies Association*.

Dahler-Larsen, P. (2008). *At fremstille kvalitative data* (2. utg). Odense: Syddansk Universitetsforlag.

Datatilsynet. (2018, 1. juni). *Virksomhetens plikter: Informasjon og åpenhet*. Hentet fra https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/gi-informasjon/

Eckhoff, T. (1979). Rettslige sider ved overvåkning og sikkerhetstjeneste. *Jussens venner, 1979*, s. 35 Oslo: Universitetsforlaget.

Eijkman, Q., & Weggemans, D. (2012). Open source intelligence and privacy dilemmas: Is it time to reassess state accountability. *Sec. & Hum. Rts.*, 23, 285. Hentet fra http://www.upeace.nl/cp/uploads/publications/03_Eijkman_Weggemans_v2%5B1%5D_1367418023.pdf

Convention on Cybercrime, Treaty No.185 C.F.R. (2001). Hentet fra https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

Finstad, L. (2000). *Politiblikket*. Oslo: Pax.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior : an introduction to theory and research*. Reading, Mass: Addison-Wesley. Hentet fra https://philarchive.org/archive/FISBAI

Fog, J. (2004). *Med samtalen som udgangspunkt : det kvalitative forskningsinterview* (2. utg.). København: Akademisk Forlag.

Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New media & society*, 18(7), 1219-1235. https://doi.org/10.1177/1461444814554900

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, 2(1), 13-20. https://doi.org/10.1007/s11416-006-0015-z

Graver, H. P. (2002). *Alminnelig forvaltningsrett*. Universitetsforlaget.

Holter, H. (1996). Kvalitative metoder i samfunnsforskning. I H. Holter & R. Kalleberg (Eds.), *Kvalitative metoder i samfunnsforskning* (s. 9-25). Oslo: Universitetsforlaget.

Johannessen, A., Christoffersen, L., & Tufte, P. A. (2010). *Introduksjon til samfunnsvitenskapelig metode* (4. utg). Oslo: Abstrakt.

Kitzinger, J. (1994). The methodology of focus groups: the importance of interaction between research participants. *Sociology of health & illness*, 16(1), 103-121. https://doi.org/10.1111/1467-9566.ep11347023

Kripos. (2018). *Bruk av åpne kilder på internett i politiet*. Upublisert.

Krueger, R. A., & Casey, M. A. (2015). *Focus groups: a practical guide for applied research* (5th ed.). Thousand Oaks, Calif: Sage.

Kvale, S., Brinkmann, S., Anderssen, T. M., & Rygge, J. (2015). *Det kvalitative forskningsintervju* (3. Utg.). Oslo: Gyldendal akademisk.

Lai, P. (2017). The literature review of technology adoption models and theories for the novelty technology. *JISTEM-Journal of Information Systems and Technology Management*, 14(1), 21-38. http://dx.doi.org/10.4301/s1807-17752017000100002

Lazar, J., Feng, J. H., & Hochheiser, H. (2010). *Research Methods in Human-Computer Interaction*: John Wiley & Sons.

Lever, A. (2016). Democracy, privacy and security. I A. Moore (Red.) *Privacy, Security, Accountability*: Routlege.

LexisNexis Risk Solutions (2014). *Social Media Use in Law Enforcement*. Hentet fra https://risk.lexisnexis.com/insights-resources/white-paper/law-enforcement-usage-of-social-media-for-investigations

Lüders, M. (2011). Why and how online sociability became part and parcel of teenage life. I R. Burnett, M. Consalvo & C. Ess (Red.) *The handbook of internet studies*, (s. 452-469): Wiley-Blackwell.

Marx, G. T. (1988). *Undercover : police surveillance in America*. Berkeley: University of California Press.

Mason, J. (1996). *Planning and designing qualitative research*. London: Sage.

McPherson, S. S. (2009). *Tim Berners-Lee: Inventor of the World Wide Web*: Twenty-First Century Books.

Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research : a guide to design and implementation* (4. Utg.). San Francisco, CA: Jossey-Bass, a Wiley Brand.

Merton, R. K., & Kendall, P. L. (1946). The focused interview. *American journal of Sociology*, 51(6), 541-557. https://doi.org/10.1086/219886

Minas, H. (2010). Can the open source intelligence emerge as an indispensible discipline for the intelligence community in the 21st century? *Research Institute for European and American Studies*, 139. https://doi.org/10.1.1.605.2359

Momani, A. M., & Jamous, M. (2017). The evolution of technology acceptance theories. *International Journal of Contemporary Computer Research (IJCCR)*, 1(1), 51-58. Hentet fra https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2971454

Moor, J. H. (2006). Using genetic information while protecting the privacy of the soul. I H. T. Tavani (Red.) *Ethics, Computing, and Genomics* (s. 109-119). Sudbury, MA: Jones and Bartlett.

Moore, R. (2011). *Cybercrime : investigating high-technology computer crime* (2. utg.). London: Routledge.

Nemeth, C. (2018). *In Defense of Troublemakers: The Power of Dissent in Life and Business*: Basic Books.

NESH - Den nasjonale forskningsetiske komité for samfunnsvitenskap og humaniora (2016). *Forskningsetiske retningslinjer for samfunnsvitenskap, humaniora, juss og teologi* (4. utg.). Hentet fra https://www.etikkom.no/globalassets/documents/publikasjoner-som-pdf/60125_fek_retningslinjer_nesh_digital.pdf

NorSIS – Norsk senter for informasjonssikring (2018). *Nordmenn og digital sikkerhetskultur 2018.* Hentet fra https://norsis.no/wp-content/uploads/2018/11/Nordmenn-og-digital-sikkerhetskultur-2018-web.pdf.

Patton, M. Q. (1990). *Qualitative evaluation and research methods*: Sage.

Penney, J. W. (2016). Chilling effects: Online surveillance and Wikipedia use. *Berkeley Tech. LJ, 31, 117*. http://dx.doi.org/10.15779/Z38SS13

NOU 2004: 6 (2004). *Mellom effektivitet og personvern - Politimetoder i forbyggende øyemed*. Hentet fra: https://www.regjeringen.no/no/dokumenter/nou-2004-6/id385309/

Politidirektoratet (2012). *Politiet i det digitale samfunnet : en arbeidsgrupperapport om elektroniske spor, IKT-kriminalitet og politiarbeid på internett*. Hentet fra https://medlem.ntl.no/Content/103500/cache=20122109105334/Politiet%20i%20det%20digitale%20samfunn%20juli%2012.pdf

Politidirektoratet (2015). *Datakrimstrategien*. Retrieved from https://www.regjeringen.no/contentassets/4d2ba37bf2ae4cc9ac39afdf20a2f41b/datakrimstrategi_2015.pdf

Politidirektoratet (2016). *Handlingsplan for løft av etterforskningsfeltet*. Hentet fra https://www.politiet.no/globalassets/05-om-oss/03-strategier-og-planer/handlingsplan-for-loft-av-etterforskningsfeltet.pdf

Politidirektoratet (2017). *Politiet mot 2025 - politiets virksomhetsstrategi*. Hentet fra https://www.politiet.no/globalassets/05-om-oss/03-strategier-og-planer/politiet-mot-2025---politiets-virksomhetsstrategi.pdf

Politidirektoratet. (2019). *Kapasitetsvurdering av etterforskningsområdet*. Hentet fra https://www.politiet.no/aktuelt-tall-og-fakta/aktuelt/nyheter/2019/02/20/kapasitetsundersokelsen/

Politregisterloven (2010). Lov om behandling av opplysninger i politiet og påtalemyndigheten (LOV-2010-05-28-16). Hentet fra https://lovdata.no/lov/2010-05-28-16

Rachlew, A. (2009). *Justisfeil ved politiets etterforskning : noen eksempler og forskningsbaserte mottiltak*. (Doktoravhandling, Universitetet i Oslo). Hentet fra http://urn.nb.no/URN:NBN:no-23961

Rachlew, A. (2010). Å forske på sine egne: Metodiske og etiske utfordringer knyttet til forskning på egen profesjon. I T. Myklebust & G. Thomassen (Red.) *Arbeidsmetoder og metodearbeid i politiet: Forskningskonferansen 2010* (s. 127-149). Oslo: Politihøgskolen.

Riksadvokaten (1999). *Rundskriv fra Riksadvokaten nr. 3*. Hentet fra https://www.riksadvokaten.no/wp-content/uploads/2017/09/Rundskriv-1999-3-Etterforskning.pdf.

Riksadvokaten (2018). *Rundskriv fra Riksadvokaten nr. 2*. Hentet fra https://www.riksadvokaten.no/wp-content/uploads/2018/11/Rundskriv-2-2018-Infiltrasjon-og-provokasjon-.pdf.

Rønn, K. V., & Søe, S. O. (2019). Is social media intelligence private? Privacy in public and the nature of social media intelligence. *Intelligence and National Security*, 34(3) (s. 362-378). https://doi.org/10.1080/02684527.2019.1553701

Sammons, J. (2015). *The basics of digital forensics : the primer for getting started in digital forensics*: Elsevier.

Schauer, F. (1978). Fear, risk and the first amendment: Unraveling the chilling effect. *Boston University Law Review*, 58, (s. 685-732). Hentet fra https://scholarship.law.wm.edu/facpubs/879

Sharma, R., & Mishra, R. (2014). A review of evolution of theories and models of technology adoption. *Indore Management Journal*, 6(2), (s. 17-29). Hentet fra https://www.researchgate.net/profile/Rajesh_Sharma80/publication/295461133_A_Review_of_Evolution_of_Theories_and_Models_of_Technology_Adoption/links/56caa1ea08ae5488f0d94ea7.pdf

Sim, W., Huang, T. C., & Hill, C. E. (2012). Biases and Expectations. I C. E. Hill (Red.), *Consensual Qualitative Research : A Practical Resource for Investigating Social Science Phenomena*. Washington, D.C.: American Psychological Association.

Solove, D. J. (2005). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154, (s. 477-558). Hentet fra https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2074&context=faculty_publications

Solove, D. J. (2008). *Understanding privacy (Vol. 173)*. Cambridge, MA: Harvard university press. Hentet fra http://www.academia.edu/download/43383679/Understanding_Privacy.pdf

Steele, R. D. (2007). Open source intelligence I Johnson, L. K. (Red.) *Handbook of intelligence studies* (s. 129-147): Routledge.

Stewart, D. W., & Shamdasani, P. N. (2014). *Focus groups: Theory and practice*: Sage publications.

Straffeloven (2005). Lov om straff (LOV-2005-05-20-28). Hentet fra https://lovdata.no/lov/2005-05-20-28

Straffeprosessloven (1981). Lov om rettergangsmåten i straffesaker (LOV-1981-05-22-25). Hentet fra https://lovdata.no/lov/1981-05-22-25

Sunde, I. M. (2013). Økosystemeffekten – Om personvernet i sosiale medier. *Lov og rett*, 52(01) (s. 85-102). Hentet fra https://phs.brage.unit.no/phs-xmlui/bitstream/handle/11250/174698/oekosystemeffekten.pdf?sequence=1

Sunde, I. M. (2015). Databevis. I R. Aarli, M.-A. Hedlund, & S. E. Jebens (Red.) *Bevis i straffesaker* (s. 599-633). Oslo: Gyldendal juridisk.

Tjora, A. (2012). *Kvalitative forskningsmetoder i praksis* (2. utg.). Oslo: Gyldendal akademisk.

NOU 2009: 1 (2009). *Individ og integritet : personvern i det digitale samfunnet*. Oslo: Departementenes servicesenter Hentet fra https://www.regjeringen.no/no/dokumenter/nou-2009-1/id542049/

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS quarterly*, (s. 425-478). https://doi.org/10.2307/30036540

Walther, J. B., Van Der Heide, B., Kim, S.-Y., Westerman, D., & Tong, S. T. (2008). The role of friends' appearance and behavior on evaluations of individuals on Facebook: Are we known by the company we keep? *Human communication research*, 34(1), (s. 28-49) https://doi.org/10.1111/j.1468-2958.2007.00312.x

Wibeck, V. (2010). *Fokusgrupper : om fokuserade gruppintervjuer som undersökningsmetod* (2. utg.). Lund: Studentlitteratur.