Pålogga politi

En studie av muligheter og utfordringer med digitalt forebyggende politiarbeid

Helene Walquist

Masteroppgave
Institutt for kriminologi og rettssosiologi
Juridisk fakultet

UNIVERSITETET I OSLO

HØST 2021

Pålogga politi - En studie av muligheter og utfordringer med digitalt forebyggende politiarbeid

http://www.duo.uio.no/

Sammendrag

Tittel: Pålogga politi

Undertittel: En studie av muligheter og utfordringer med digitalt forebyggende politiarbeid

Forfatter: Helene Walquist

Hovedveileder: Katja Franko

Biveileder: Helene Gundhus

Levert ved: Institutt for kriminologi og rettssosiologi (UiO), august 2021

Digitaliseringen av samfunnet har skapt både utfordringer, men også muligheter for politiet. Internett har gitt opphav til nye former for kriminalitet, og økt rekkevidde og muligheter for allerede eksisterende lovbrudd. Mennesker blir ikke lenger bare utsatt for kriminalitet i den fysiske verden, antall lovbrudd som finner sted i den virtuelle verden fortsetter å øke. Politiet har satt det å skape trygghet i det digitale rom på dagsordenen. De har opprettet og utviklet et nasjonalt senter for datakriminalitet, og etablert patruljer i hvert politidistrikt som skal patruljere den virtuelle verden. Temaet i denne oppgaven er hvordan politiet forsøker å forebygge kriminalitet som finner sted på nett, samt hvordan de utnytter digitale verktøy til å drive forebyggende og trygghetsskapende arbeid. Gjennom kvalitative intervjuer med åtte ansatte i politiet, tilknyttet digitalt forebyggende politiarbeid, undersøker oppgaven de ansattes opplevelser av det forebyggende arbeidet, av internett som en forebyggende arena og hvilke aspekter som har påvirket utviklingen av digitalt forebyggende politiarbeid. De ansattes skildringer vil bli knyttet opp mot oppgavens bakgrunn og teoretiske rammeverk, som baserer seg på samfunnets digitalisering, teorier om kriminalitetsforebygging, perspektiver på data og kriminalitet, yrkeskulturer og strukturelle endringer innad i organisasjonen.

Funnene viser hvordan politiets digitalt forebyggende arbeid kan knyttes opp mot tradisjonelle forebyggende strategier, og at internett er en utfordrende arena å drive forebygging på. Videre finner oppgaven at politiet etablerer nye måter å kommunisere med befolkningen på, og ved å gjøre dette skaper de relasjoner med befolkningen til tross for større fysisk avstand. Det kommer frem at informantene opplever en forventing fra befolkningen om at de skal befinne seg på nett, og et behov for å skape bevissthet rundt internett og kriminalitet. Videre finner oppgaven at utviklingen på området digitalt forebyggende politiarbeid i Norge har vært treg, noe som knyttes opp mot etablerte yrkeskulturer. Funnene i oppgaven tyder på at politiet er i en integreringsprosess inn i den digitale verden, og at det over tid forekommer endringer i holdninger rettet mot digitalt politiarbeid.

Forord

Fem år på studiet er forbi, og mine dager på krimmen er over. Hva i all verden skal jeg finne på nå? Det er med en bismak i munnen jeg leverer inn masteroppgaven og takker for meg. Det var ikke slik mitt siste år som student skulle bli, et ensomt år på hjemme med liten kontakt med mine medstudenter. Til tross for dette leverer vi nå masteroppgavene våre, og jeg er utrolig stolt over at vi klarte det alle sammen!

Det er mange som fortjener en ekstra takk. Først og fremst vil jeg begynne med å takke de ansatte i nettpatruljen Vest og NC3 som deltok i prosjektet. Uten dere hadde det ikke blitt en oppgave, og jeg er veldig takknemlig for at dere ønsket å dele av deres kunnskap og erfaring.

Jeg vil rette en spesiell takk til min veileder Katja Franko. Tusen takk for gode og skarpe innspill, at du alltid har vært tilgjengelig og har hatt tro på oppgaven min hele veien. Jeg vil også takke Helene Gundhus, takk for at du tok deg tid til å hjelpe til i oppgavens innspurt!

Tusen takk til mamma for all hjelp med korrekturlesning og for at du syntes at alt jeg skriver er interessant. Tusen takk til pappa for alle støttende ord og tilrettelegging. Tusen takk til Stine for at du setter av de få frikveldene du har til å hjelpe meg med gode innspill, gjennomlesning og til å stresse ned.

Jeg vil takke alle nære og kjære for støtte og forståelse for at oppgaven har måttet komme først. Takk for at dere har laget middag, latt meg få ut frustrasjon, og flyttet lunsjer og sammenkomster i gåavstand til juridisk fakultet for at jeg skal kunne bli med. Pausene med dere har betydd mye!

Til slutt vil jeg takke mine studievenner. Tusen takk for faglige innspill, sene kvelder og mye moro – jeg har satt utrolig stor pris på å kunne sitte på master-berg-og-dalbanen sammen med dere! En spesiell takk til Siren og Victoria. Takk for at dere alltid har vært støttende og tilgjengelige, uten dere hadde masterskrivingen blitt betydelig mye tyngre.

Innholdsfortegnelse

1. Introduksjon

Verden er i kontinuerlig endring. Innføringen av nye teknologier har historisk spilt en stor rolle i disse endringene, fra innføringen av industrielle redskaper på 1700-tallet, telefonapparater på 1800-tallet, til innføringen av digitale teknologier for informasjonslagring og kommunikasjon mot slutten av det siste århundret. Samfunnet har gjennomgått et skifte fra å være basert på atomer, til å være basert på bits (Rice, Yates og Blejmar, 2020, s. 5). Det digitale skiftet vi har gjennomgått kan betegnes som en digital revolusjon, skiftet har beveget seg i en enorm fart og endringene det har ført til er altomveltende. Samfunnet vårt har blitt forvandlet til å være et teknososialt samfunn, digitale teknologier har blitt en uunnværlig del av det og gjennomsyrer nesten alt vi gjør (Powell, Stratton og Cameron, 2018, s. 4). Datasystemer preger arbeids- og skoledager, man kan bli underholdt gjennom alle døgnets tider gjennom strømming av innhold, informasjon og nyheter blir delt til publikum enten gjennom tv, radio eller som et push-varsel på telefonen. Vi lever nå i et digitalt samfunn skapt av fundamentale teknologiske, strukturelle og sosiale endringer (Powell, Stratton og Cameron, 2018, s. 4). Utviklingen har ført til grunnleggende forandringer. En bok er ikke lenger bare en fysisk gjenstand bestående av papirsider, handel skjer ikke lenger bare i fysiske butikker, og kriminalitet er ikke lenger et fenomen forbeholdt den fysiske verden.

Politirollen blir svært preget av tiden vi lever i (Finstad, 2018, s. 10). Politidirektoratet (2017, s. 5) har kartlagt hvilke utfordringer politiet vil møte frem mot 2025, og en av de fremste utfordringene er rask teknologisk utvikling. Historisk ble internett skapt for å være et fristed, et liberalt samfunn som ikke ble bundet opp av den fysiske verdens begrensninger. Internett skulle være et selv-regulerende miljø som var fylt av frie likesinnede (Aas, 2007, s. 171). Internett er ikke lenger bare for spesielt interesserte, det er en innvevd del av vår hverdag. Det er ingen tvil om at opprettelsen av internett har endret hvordan vi lever og skapt uendelige muligheter, men det har også brakt med mange utfordringer. Internett er ikke lenger et liberalt fristed, hver dag blir tusenvis av mennesker utsatt for svindel, overgrep og utnyttelser over internett. Politiets straffesaksstatistikk viser at den tradisjonelle kriminaliteten som skjer i fysiske omgivelser har vært i nedgang over flere år, mens flere kilder peker i retning av at det samtidig har skjedd en vekst i IKT-kriminalitet (Riksrevisjonen, 2021, s. 4). Dette har resultert i en økende satsning på dette området, trygghet i digitale rom er en av hovedprioriteringene til politiet frem mot 2025 (Politidirektoratet, 2017, s. 6). Som følge av denne prioriteringen ble det i 2019 opprettet en egen seksjon i Kripos som er viet fullt og helt til kriminalitet som skjer på nett, kalt Nasjonalt

Cyberkrimsenter (NC3) (Riksrevisjonen, 2021, s. 7). Til tross for den økende satsningen på håndtering og forebygging av lovbrudd som befinner seg på nett, blir befolkningens tillit til politiet på dette området målt lavere enn tilliten til håndtering av tradisjonell kriminalitet (NorSIS, 2019; Riksrevisjonen, 2021).

Prioriteringen av å skape trygghet i digitale rom endrer tradisjonelle deler av politiets arbeid. Hvis man stiller spørsmålet «hva gjør politiet?», vil et av de første svarene man får trolig være at politiet patruljerer. Patruljering er en fremtredende og institusjonelt forankret del av politiarbeidet. Patrulje er på mange måter et symbol på politiet; gjennom patruljering blir politiets tilstedeværelse synlig for publikum, det gir politiet muligheter til å kontrollere omgivelsene og være tilgjengelige for å raskt rykke ut til situasjoner der de trengs (Holmberg, 2014, s. 154). Mye av arbeidet gjort av politiet er altså forankret i patruljering som finner sted i bil, på sykkelsetet, på hesteryggen, på motorsykkel eller til fots (Holmberg, 2014, s. 154). Det skjer forandringer i måten politiet patruljerer på, og over hele landet har det de siste årene blitt opprettet innsatser som skal patruljere den digitale verden - nettpatruljer. I dag har hvert eneste politidistrikt i Norge sin egen nettpatrulje, og formålet med denne innsatsen er å ha en enhet som veileder om trygg og god nettbruk, samt å være et tilgjengelig og synlig politi på nett (Politiet, 2020). Satsningen på nettpatruljer over hele landet er et symbol på retningen politiet har valgt å ta. Idéen om at politiet skal patruljere seg gjennom bits i cyberspace og daglig ta i bruk sosiale medier er en institusjonell innovasjon – det utfordrer tradisjoner og holdninger dypt forankret i det historiske yrket.

1.1 Problemstilling

Det er derimot rettet lite akademisk oppmerksomhet mot skjæringspunktet mellom kriminalitetsforebygging, digitale utviklinger og kriminalitet som skjer på nett. I takt med utviklingen av digitalisering og teknologi i samfunnet øker også trusselen for kriminalitet knyttet til teknologi (Politidirektoratet, 2017, s. 5). Men utvikler mulighetene for å forebygge denne kriminaliteten seg i samme tempo? Det forebyggende arbeidet må tilpasses det nye kriminalitetsbildet. Fremveksten av sosiale medier gir også politiet nye verktøy for å drive forebyggende arbeid. Det åpner opp for en helt ny tilnærming og forebyggende innsatser ved bruk av digitale virkemidler. Hvordan kan vi forstå denne utviklingen? Vil tradisjonelle kriminalitetsforebyggende teorier strekke til for å forklare og utvikle også det digitale

forebyggende politiarbeidet? Oppgaven vil ta utgangspunkt i og belyse følgende problemstilling:

> *Hvordan driver politiet digitalt forebyggende politiarbeid, og hvordan opplever ansatte i politiet at de jobber mot å skape trygghet i det digitale rom?*

For å utforske oppgavens hovedproblemstilling og tematikk vil jeg også ta for meg følgende underproblemstillinger:

- *Kan teoretiske tilnærminger fra tradisjonell kriminalitetsforebygging overføres til digitalt forebyggende politiarbeid?*
- *Hvordan blir utviklingen av digitalt forebyggende politiarbeid påvirket av organisatoriske aspekter?*

Begrepet digitalt forebyggende politiarbeid omfavner flere aspekter av politiarbeidet. I denne oppgaven vil det omfatte forebyggende innsatser rettet mot kriminelle handlinger begått ved hjelp av internett. Videre vil det også omfatte forebygging rettet mot tradisjonell kriminalitet og trygghetsskapende arbeid utført ved hjelp av digitale verktøy. Digitale verktøy vil i denne oppgaven bestå i all hovedsak av sosiale medier.

1.2 Oppgavens oppbygning

Oppgaven består av åtte kapitler. Det første kapittelet som allerede er presentert, inneholder oppgavens innledning og problemstilling. I kapittel to vil oppgavens bakgrunn presenteres. Kapittelet begynner med å se på forholdet mellom internett og kriminalitet, før politiets digitale tilstedeværelse på nett, ambisjoner for bekjempelse av datakriminalitet og bruk av sosiale medier i tjenesten vil bli tatt opp. Til slutt vil nærpolitireformen fra 2015 og dens konsekvenser presenteres, for å gi kontekst til landskapet det digitale forebyggende politiarbeidet vokser frem i.

Kapittel tre tar for seg oppgavens teoretiske rammeverk. Kapittelet er delt inn i fire overordnende perspektiver som vil anvendes hver for seg, men også knyttes sammen for å tolke oppgavens empiri. Underveis i både kapittel to og tre vil tidligere forskning på feltet bli presentert tematisk. I oppgavens fjerde kapittel vil det metodiske rammeverket presenteres. Dette kapittelet vil gi en oversikt over de metodiske verktøyene og valgene som er anvendt i

oppgavens kvalitative tilnærming. Følgende presenterer kapittelet hvordan oppgavens datamateriale er behandlet, samt aktuelle etiske refleksjoner.

Kapittel fem og seks er oppgavens analysekapitler, hvor funnene blir drøftet opp mot det teoretiske rammeverket og tidligere forskning på feltet. Kapittel fem tar for seg de forebyggende praksisene og hvilke særegne preg digitalt forebyggende arbeid har. Kapittel seks tar for seg det digitale forebyggende politiarbeidet sett i lys av organisatoriske perspektiver. Kapittel syv inneholder en oppsummering av hovedfunnene i analysen og en videre diskusjon av noen av oppgavens viktigste funn, før oppgaven avrundes i kapittel åtte.

2. Bakgrunn

I denne delen vil bakgrunnen for problemstillingen og oppgavens tema bli presentert. Kapittelet vil begynne med å ta for meg innvirkningen internett har hatt på kriminalitet. Videre vil politiets rolle i den digitale verden fremheves. Her vil politiets håndtering av datakriminalitet, samt politiets nye tilstedeværelse på digitale plattformer bli presentert. Til slutt vil kapittelet ta for seg endringer politiorganisasjonen nylig har gått gjennom, og hvilke betydninger dette har hatt for forholdet mellom politi og borger. Hensikten med dette kapittelet er å kontekstualisere oppgavens problemstilling, samt å beskrive organisatoriske utviklinger og aspekter som har en betydning for de forebyggende mekanismene satt i gang av politiet. Noe tidligere forskning på feltet vil også bli presentert tematisk gjennomgående i kapittelet.

2.1 Internett og kriminalitet

For å forstå hvordan internett har hatt en innvirkning på kriminalitet, beskriver Wall (2007, s. 34) tre nøkkelegenskaper datakriminalitet innehar; globalisering, distribuerte nettverk og dataspor. Internett har bidratt til å viske ut tradisjonelle geografiske avstander. Mange former for datakriminalitet finner sted i digitale miljøer, miljøer som kan finne sted på tvers av landegrenser og rettslige jurisdiksjoner (Calderoni, 2010, s. 341). Helt grunnleggende er internett et sett av informasjonsprotokoller som kobler mennesker sammen i et nettverk (Rice, Yates og Blejmar, 2020, s. 5). Det har skapt nye, teknologiske kommunikasjonsmidler som gjør det mulig å forme sosiale nettverk på tvers av geografiske, sosiale og kulturelle grenser (Wall, 2007, s. 35). Muliggjøringen og normaliseringen av å være i kontakt med mennesker over internett kan gi nye muligheter for kriminelle handlinger. Det faktum at man kan komme i kontakt med mennesker verden over, betyr også at man kan utføre kriminelle handlinger mot mennesker verden over – og det øker risikoen for å bli et offer (Staniforth, 2017, s. 8). Alt vi gjør på internett legger igjen spor, og disse sporene kan bli utnyttet. Datasystemer oppretter og lagrer informasjon, og denne informasjonen kan være verdifull for datakriminelle (Wall, 2007, s. 36).

Internett, teknologi og data spiller ulike roller i ulike former for kriminalitet, og det er viktig å være klare på disse skillene. Datakriminalitet består av et sammensurium av ulike ulovlige aktiviteter (Staniforth, 2017, s. 29). Selv om internett gir kriminalitet de samme egenskapene, blir disse anvendt på ulike måter og i ulike former. Det er viktig å se hvilke egenskaper internett gir ulike kriminalitetsformer, og slik hvorfor kriminaliteten kan defineres som datakriminalitet, fordi det vil bidra til å forme strategier for å kriminalitetsbekjempelsen av de spesifikke

lovbruddene (Payne, 2019, s. 3). Forståelsen av datakriminalitet har blitt diskutert opp gjennom årene innenfor kriminologi (Yar og Steinmetz, 2019, s. 14). Er datakriminalitet det samme som tradisjonell kriminalitet, rett og slett «old wine in new bottles»? (Grabosky, 2001). Eller representerer det en helt ny form for kriminalitet som skiller seg fra tradisjonell kriminalitet? (Yar og Steinmetz, 2019, s. 14). I all hovedsak kan kriminalitet knyttet til internett klassifiseres i to; data-aktivert kriminalitet og data-avhengig kriminalitet. Data-aktivert kriminalitet er tradisjonell kriminalitet som finner sted på internett (Staniforth, 2017, s. 12). Handlinger som allerede var ulovlige får ved hjelp av data økt rekkevidde, økt fart og større handlingsrom for utøvelsen av lovbruddet (Williams og Levi, 2017, s. 455). Eksempler på utbredte data-aktiverte kriminalitetsformer er ulike former for svindel, hatkriminalitet, overgrep mot barn og distribusjon av overgrepsmateriale. Data-avhengig kriminalitet er den andre klassifikasjonen av datakriminalitet, og består av kriminelle handlinger oppstått som et resultat av internett og teknologi. Disse formene for kriminalitet kan kun bli begått ved hjelp av teknologi, eksempelvis hacking og skadelig programvare (Williams og Levi, 2017, s. 455). Teknologi har både bidratt til utvikling og utbredelse av kriminalitetsformer vi var kjent med fra før, samtidig som det har skapt plattformer for kriminalitetsformer særegne for det digitale. Jeg vil videre i oppgaven bruke begrepet «datakriminalitet» og lignende som samlebegrep for både data-aktivert og data-avhengig kriminalitet, og presisere når jeg kun omtaler det ene eller det andre.

2.2 Politiet og datakriminalitet

I dag driver de fleste deler av politiorganisasjonen med noe arbeid knyttet til datakriminalitet (Politidirektoratet, 2015, s. 11). I 2006 skrev Norge under på Budapestkonvensjonen, et produkt av Europarådets anerkjennelse og bekymring av datateknologiens økende rolle i samfunnet (Konvensjon om datakriminalitet, 2006). Konvensjonen tar for seg nye former for kriminalitet knyttet mot data, og hvordan stater skal håndtere og samarbeide om dette. Ratifiseringen av konvensjonen markerer begynnelsen på et nytt og fremtredende fokusområde innenfor utvikling av det norske politi. I 2013 begynte arbeidet med å få utarbeidet en helhetlig strategi for hvordan Norge skal håndtere datakriminalitet. Strategien sto ferdig i 2013, og her fastsettes det at visjonen bak strategien er at: «Norge skal være et av foregangslandene i bekjempelse av datakriminalitet», samt at Norge skal «bidra til en trygg bruk av datasystemer for å sikre verdiskapning, demokrati og velferd» (Politidirektoratet, 2015, s. 14) I virksomhetsstrategien «Politiet mot 2025» blir politiets digitale tilstedeværelse og styrking av håndteringen av datakriminalitet fastslått som et av de viktigste punktene (Politidirektoratet, 2017, s. 7).

Det er et pågående kappløp mellom politiet og datakriminelle, og i dette løpet opplever politiet mange hindre (Blakemore, 2012, s. 8). Datakriminalitet er i en økende trendutvikling og oppdatering av lovverk, strategier og metoder for å bekjempe den klarer ikke å holde følge med utviklingen (Politidirektoratet, 2015, s. 12). Den raske endringen krever god kompetanse, og politidistriktene har ikke tilstrekkelig bevissthet om datakriminalitet (Politidirektoratet, 2015, s. 12). Politiets arbeid med datakriminalitet har møtt på mye kritikk. I begynnelsen av 2021 publiserte Riksrevisjonen sin vurdering av politiets innsats mot datakriminalitet, hvor prioriteringene og resultatene av denne innsatsen får hard kritikk. Riksrevisjonen (2021, s. 5). mener blant annet at politiet mangler oversikt over datakriminalitet, i liten grad etterforsker og oppklarer ren IKT-kriminalitet, at ressursbruken kan være ineffektiv og at utfordringer ved internasjonalt samarbeid bidrar til en lav oppklaring av datakriminalitet-saker. Mens kriminelle kan tilpasse seg nye metoder og teknologier i et raskt tempo, henger rettsvesenet etter fordi de ikke er like tilpasningsdyktig. Endringer i politiet krever godkjennelse og opplæring, politiets byråkratiske strukturer setter kjepper i hjulene for å kunne utvikle seg parallelt med lovbryterne (Holt, 2019, s. 2). Riksrevisjonen (2021, s. 6) viser også til undersøkelser som understreker at tilliten til politiet er lavere for IKT-kriminalitet enn for annen kriminalitet, og dette er en årsak til hvorfor mange tilfeller av datakriminalitet ikke anmeldes.

Politiet skal ta for seg alle former for datakriminalitet og uønsket atferd på nett, men i realiteten er ikke dette mulig fordi det begås så mye kriminalitet i det digitale rom (Yar og Steinmetz, 2020, s. 218). Politiet må derfor prioritere hvor de skal sette inn sine ressurser, og dette reiser spørsmål rundt hva det er viktig at politiet setter søkelys mot. Politiets ressurser blir ofte rettet mot de største farene og mest alvorlige formene for kriminalitet (Yar og Steinmetz, 2020, s. 218). I Norge har blant annet overgrep mot og overgrepsmateriale av barn på nett vært en fanesak for politiet (Justis- og Beredskapsdepartementet, 2020, s. 59). De mest alvorlige formene for datakriminalitet, er også de som bruker mest av politiets ressurser. Alvorlig internasjonal datakriminalitet er vanskelig å etterforske, særlig når den er knyttet til land hvor bekjempelse av datakriminalitet ikke blir prioritert (Politidirektoratet, 2015, s. 12-13). I rapporten om Norges datakrimstrategi fra 2015 kom det frem at Kripos på det tidspunktet kun hadde kapasitet nok til å etterforske to til fem saker knyttet til datakriminalitet hvert år (Politidirektoratet, 2015, s. 12). Selv om dette tallet kan antas å være betydelig høyere i dag, ettersom Kripos har etablert større avdelinger med fokus på datakriminalitet, vil antallet for etterforskede saker fremdeles blekne sett opp mot hvor stort omfanget av alvorlige lovbrudd som skjer i det digitale rom er den dag i dag. Mangel på ressurser og resultater kan videre føre

til at politiet må sikte seg inn på «low hanging fruits», mindre alvorlige handlinger som således også krever mindre ressurser å etterforske (Andrews, 2005 i Yar og Steinmetz, 2020, s. 219). De krever også mindre tid og mindre teknisk kompetanse, og er slik en mer effektiv måte å håndtere datakriminalitet på. Hva er det viktigste; at politiet effektivt avdekker og etterforsker mange mindre alvorlige datalovbrudd, eller burde fokuset være på de store sakene, selv om det kan resultere i en lavere oppklaringsprosent?

2.3 Politiet og nye digitale verktøy

Det er politiets oppgave å ta fatt i samtidens utfordringer og tilpasse seg slik at de klarer å håndtere disse. 1970- og 80-tallet var preget av politiets harde hånd, og de ble fremstilt som en brutal voldsmakt i møte med demonstrasjoner og varetektsfengsling (Finstad, 2018, s. 11). Dette bilde av politiet sto stikk i strid med hvordan den samme institusjonen ble fremstilt kun et par tiår tidligere, nemlig dyktige kriminalitetsbekjempere (Finstad, 2018, s. 11). Tanken om å tilpasse seg samfunnet er forankret i idéen om at det norske politiet skal være helhetsorientert. Et helhetsorientert politi er et politi som opplever verden rundt seg og sin rolle i dette. I takt med samfunnet digitaliseres dermed også politiarbeidet. Politiet møter på utfordringer med nye kriminalitetsformer og nye plattformer der kriminalitet kan blomstre, samtidig som digitaliseringen også fører til en utvikling av it-systemer og andre tjenester arbeidet er avhengig av.

Digitaliseringen av politiarbeid kan skape en effektivisering og nye måter å utføre polititjenester på (Gundhus, Talberg og Wathne, 2019, s. 86). Men det skaper også utfordringer for politiet. Overføringer av arbeid som tradisjonelt ble utført av politibetjenter til digitale tjenester, kan skape en større avstand til publikum (Gundhus og Larsson, 2014, s. 278). Mindre synlig politi i gatene og mindre ansikt til ansikt kontakt mellom politi og publikum kan slik påvirke den gode relasjonen og tilliten som er karakteristisk for de skandinaviske landene. Det er ikke bare i relasjon med publikum at det digitale samfunnet kan ha en konsekvens for politiet. Den økende bruken av internett i dagens samfunn synliggjør et generasjonsskille. Skillet er mellom ”digital natives” - den yngre generasjon hvor teknologi er innbakt i deres oppvekst og hverdag, og ”digital immigrants” - den eldre generasjon hvor teknologi er noe fremmed og nytt som må innlæres (Bennet, Maton og Kervin, 2008 s. 776-777). Det kan derfor tenkes at nye digitale løsninger oppleves som en selvfølge av den yngre del av de ansatte, men også kan oppleves som unødvendige endringer og utfordringer for den eldre delen.

Hvilke virkemidler politiet skal ta i bruk og tradisjonelle tanker om politiets arbeid blir utfordret av det økende ønsket og behovet for tilstedeværelse av politi på internett. Utviklingen av nye medieformat og kommunikasjonsmidler, som sosiale medier, gir politiet nye verktøy å ta i bruk for å nå ut til befolkningen. Leishman og Mason (2003, s. 41) identifiserte allerede for nesten 20 år siden at sosiale medier ville gi politiet gode muligheter til å promotere deres aktiviteter og utgi informasjon i en kontrollert kontekst. Det er ikke bare særegent for Norge at politiet tar i bruk sosiale medier - over hele verden utvikles det egne sosiale medier-betjenter (Schneider, 2016, s. 15). Sosiale medier som Instagram, Facebook og Twitter blir gode informasjonskanaler, hvor politiet kan nå mange innbyggere på kort tid. Det er derimot ikke bare informasjon sosiale medier kan brukes til, det blir også en arena hvor politiet kan ha direkte kontakt med publikum ved å gi dem mulighet til å like, kommentere og sende dem meldinger (Schneider, 2016, s. 13). Intravia, Wolff og Piquero (2018) undersøkte hvilken påvirkning blant annet sosiale medier hadde på publikums holdninger mot politiet. Her fant de et positivt forhold mellom bruk av sosiale medier og tanker om politiets legitimitet, for personer uten tidligere kontakt med politiet (Intravia, Wolff og Piquero, 2018, s. 976). De trekker slik linjer mellom synligheten til politiet på nettsider som mange av oss bruker hver eneste dag, og hvordan politiets budskap og legitimitet blir oppfattet.

2.4 Politireform

En tanke som har vært historisk forankret i det skandinaviske politiet er viktigheten av nærhet til lokalsamfunn (Gundhus og Larsson, 2014, s. 277). At politiet skal være integrert i lokalsamfunnet har vært en grunnmur i ivaretakelsen av godt utførte politioppgaver. Politiet i Norge har derimot i de siste tiårene gjennomgått store strukturelle forandringer, senest nærpolitireformen vedtatt i 2015. Formålet med denne reformen var å styrke nærpolitiet, ha færre men robuste politidistrikter og øke samarbeidet mellom politi og kommune (Justis- og Beredskapsdepartementet, 2015, s. 5). Dette fordi Justis- og Beredskapsdepartementet (2015, s. 7) opplevde at politiressursene var «smurt for tynt utover» til å gi god faglig kvalitet og effektiv utnyttelse av ressurser. Hierarki, profesjonell kompetanse, sentralisering og standardisering er kjerneelementer i reformen (Christensen, Lægreid og Rykkja, 2017, s. 255). Dette har ført til sammenslåing av politienheter, og derav nedleggelsen av flere lokale tjenestesteder til fordel for større, kunnskapsbaserte avdelinger. Begrunnelsen for dette er blant annet å kunne minske det administrative arbeidet, spisse kompetanse og frigjøre midler til økende tilstedeværelse og kartlegging av kriminalitet (Gundhus og Larsson, 2014, s. 276).

En annen bakenforliggende årsak til behovet for denne strukturreformen var påvirkningen digital teknologi har hatt for samfunnet (Justis- og Beredskapsdepartementet, 2015, s. 20). Digital teknologi kan gi et grunnlag for bedre arbeidsprosesser for politiet og god kontakt med innbyggerne, samtidig som det har skapt helt nye måter å gjennomføre kriminelle handlinger på (Justis- og Beredskapsdepartementet, 2015, s. 20). Større og mer robuste fagmiljøer er nødvendig for å møte den digitale kriminaliteten, da den krever utvikling av politiets arbeidsmetoder og kunnskap på området. I tillegg bringer den digitale utviklingen av samfunnet med et nytt område politiet må kontrollere; internett. En større tilstedeværelse og et mer synlig politi på nett, skal bidra til å sikre innbyggernes trygghet (Gundhus, Talberg og Wathne, 2018, s. 209).

Opprettelsen av et nytt, effektivt og kunnskapsbasert politi har konsekvenser. Nærpolitireformen har vært svært omdiskutert, og politiets avtagende nærhet til befolkningen har vært et av hovedpunktene i kritikken (Christensen, Lægreid og Rykkja, 2017; Gundhus, Talberg og Wathne, 2018; Larsson, 2017; Gundhus, Larsson, Sørli, Talberg, Wathne, 2018). Når politiet blir flyttet fra lokalmiljøene kan det være vanskelig å opprettholde relasjonen mellom publikum og politi. Terpstra, Fyfe og Salet (2019, s. 2) hevder at politireformer som skaper større fysisk avstand mellom politi og borger, bidrar til å utvikle et «abstrakt politi». De omtaler det abstrakte politiet som mer formelt, og mindre direkte (Terpstra, Fyfe og Salet, 2019, s. 2). Finstad (2018, s. 136) omtaler politireformens politi som et utrykningspoliti som er løsrevet fra de stabile og langvarige båndene et lokalintegrert politi har til samfunnet. Det nye politiet blir frontet som kunnskapsbasert, men gjennom politireformen går også verdifull kunnskap tapt. Politiets tette kontakt med publikum har tradisjonelt gitt politiet en innsikt i problemer i lokalmiljøet, og når politiet mister denne tette kontakten vil de følgende miste verdifull kunnskap og informasjon (Gundhus, Talberg og Wathne, 2018, s. 216). Ved å sentralisere polititjenester øker den fysiske avstanden mellom politiet og publikum, noe som også kan føre til lengre utrykningstid (Gundhus og Larsson, 2014, s. 276). Navnet nærpoliti kan være misvisende, fordi mange opplever at politiet er fjernere etter reformen enn de var før. Leder for Politidirektoratet Benedicte Bjørnland ønsker å gå bort fra navnet nærpolitireformen til å heller kalle det for en profesjonaliseringsreform (Schjetne, 2019). Det er ikke bare den fysiske avstanden som har økt, også den sosiale avstanden mellom politi og publikum oppleves å øke. Denne opplevde avstanden kan påvirke publikums tillit til politiet, samt påvirke befolkningens opplevde trygghetsfølelse (Finstad, 2018, s. 136).

2.5 Oppsummering

I dette kapittelet har jeg beskrevet elementer som må legges til grunn for å se oppgavens bidrag i en bredere kontekst. Internett har skapt en helt ny plattform for kriminalitet, og gitt den nye egenskaper som ikke før har vært en del av kriminalitetsbildet. Kriminalitetens grenseløshet skaper utfordringer og krever endringer i etablerte organisatoriske aspekter. I de siste årene har politiet satt det digitale kriminalitetsbildet på agendaen, men kritiseres for manglende oppfølging og gjennomføring av dette. Politiorganisasjonen er i kjølvannet av en omstruktureringsreform som oppleves å stride imot historisk forankrede prinsipper for politiarbeid, som en fysisk tilstedeværelse i lokalsamfunn. Et formål med denne reformen er nettopp å bedre ruste politiet for å møte på utfordringene internett som kriminell mulighetsarena byr på. Oppgavens empiri må derfor ses i lys av hvilke endringer politiet har gjennomgått, hvilke virkemidler de må ta i bruk, og hva tankene bak disse er. I neste del vil oppgavens teoretiske rammeverk presenteres.

3. Teoretiske perspektiver

En stor motivasjon for å utarbeide og undersøke oppgavens problemstilling, var det delvis manglende teoretiske grunnlaget for forebygging av datakriminalitet og forebygging som finner sted i det digitale rom. For å kunne utforske min problemstilling må jeg derfor ta for meg flere, til dels store, teoretiske retninger innenfor kriminologien og samfunnsvitenskap. Oppgavens teoretiske rammeverk består i hovedsak av fire ulike perspektiver, og hensikten er at samspillet mellom disse skal kunne omfavne problemstillingen. Først vil jeg ta for meg sosiologiske tanker som sikter på å forklare det digitale skiftet i samfunnet og hvordan dette har omgjort vår tilhørighet til det lokale og fysiske. Disse vil videre bli knyttet til konsepter viktig for politiarbeid, som tillit og nærhet. Videre vil jeg presentere fenomenet datakriminalitet og hvordan dette forvandler de tradisjonelle rammene for sted og lovbryter. Deretter vil eksisterende litteratur og teori som omhandler forebygging og datakriminalitet bli presentert. Jeg vil deretter ta for meg tradisjonelle kriminalitetsforebyggende strategier, i hovedsak situasjonell og lokalorientert forebygging. Til slutt vil jeg ta for meg yrkeskultur innad i politiet som kan knyttes opp mot økt bruk av IKT og forebyggende arbeid. Dette for å kartlegge hvilket klima nye digitale polititjenester og større satsninger på forebygging av datakriminalitet vokser frem i, og hvilke mulige påvirkninger dette har hatt for utviklingen av arbeidet. Underveis i kapittelet vil også tidligere forskning bli presentert tematisk.

3.1 Modernitet og sosiale relasjoner

3.1.1 Reproduksjon av struktur

Anthony Giddens sin strukturasjonsteori forsøker å forklare samspillet mellom sosial struktur og aktørers handlinger i det moderne samfunn, og kan trekkes mot digitaliseringen av samfunnet. Strukturasjonsteori betegner sosial struktur som underliggende ressurser produsert av individer, som muliggjør sosial praksis (Pettersen, 2018). Giddens (1984, s. 17) tar for seg strukturen av sosiale relasjoner, som består av regler og ressurser reprodusert av handlede aktører. Strukturene legger regler for sosial praksis, og disse reglene representerer den allmenne godtatte måten å handle på. Struktur preges av en dualitet. Aktører og strukturer er ikke to selvstendige fenomen, de er avhengig av hverandre og burde ses på som en helhet (Giddens, 1984, s. 27). Strukturer kan ikke eksistere uten aktører som følger dem. Reproduksjonen av sosial struktur er både betingelser for og konsekvenser av folks samhandling (Pettersen, 2018). Reproduksjonen av struktur skjer i moderne samfunn på tvers av tid og sted (Giddens, 1984, s. 25). Giddens (1997, s. 22) viser til at med utviklingen av moderniteten har det parallelt skjedd

en utvikling av «et tomt rom». I det førmoderne samfunn faller rommet for sosial interaksjon og stedet denne interaksjonen skjer i sammen, men i moderne samfunn er rommet og stedet i større grad atskilt. Modernitetens betingelser løsriver sosial handling fra nærhet eller lokaliserte aktiviteter, og slik er ikke lenger rommet der reproduksjonen av sosial struktur skjer forankret i et geografisk eller fysisk sted (Giddens, 1997, s. 22). Giddens (1997, s. 24) omtaler modernitetens restrukturering av tid og sted for en utleiring av sosiale relasjoner – de løftes ut av lokale sammenhenger og restruktureres ut i uendelige rom. Denne utleiringen har ført til at deler av samfunnet som før var forankret i fysiske steder har blitt overført til tidløse, nettbaserte og globale rom.

Giddens sine perspektiver har blitt videreført og utviklet i senere tid, særlig knyttet opp mot utviklingen av digitale kommunikasjonsmidler. Abeele, de Wolf og Ling, (2018, s. 5) bruker strukturasjonsteori for å undersøke hvordan mobil kommunikasjon former det hverdagslig liv, og omformer maktdynamikker som underligger sosial handling. Pettersen (2018) bruker Giddens sine tanker om reproduksjon av struktur i moderne samfunn for å undersøke hvilke forhold som risikerer å gå tapt som en følge av teknologiske konteksforflytninger. Hun viser til at disse forflytningene blant annet bidrar til at vi har færre sosiale interaksjoner med tilfeldige, fremmede mennesker, og hvilke konsekvenser dette kan ha (Pettersen, 2018). Disse funnene knyttes blant annet opp til forskning som understreker at nærhet og tilkobling til andre mennesker, samt bruk av skjermkommunikasjon, påvirker individers livskvalitet og velvære (Sandstrom og Dunn, 2014; Shakya og Christakis, 2017; Turkle, 2015). Forskningsområder som tar for seg forflytninger av sosiale relasjoner i moderne samfunn er stort, og det er verken mulig eller hensiktsmessig for oppgavens omfang å gi en fullstendig oversikt over dette. Videre vil jeg presentere noen aspekter som er relevante for oppgavens problemstilling og empiri.

3.1.2 Tillit, ekspertsystemer og symbolske tegn

Tillit er en essensiell del av samfunnet, og Giddens mener det moderne samfunnet har påvirket hvordan tillit skapes. Utleiring av sosiale systemer består av mekanismer, mekanismer som adskiller tid og rom. Giddens deler disse mekanismene i to; symbolske tegn og ekspertsystemer. Symbolske tegn er utvekslingsmedier som kan sendes rundt på tvers av tid og sted, som ikke mister sin betydning (Giddens, 1997, s. 24). Et eksempel på symbolske tegn er internett: gjennom internett har aktiviteter blitt flyttet til nettbaserte og globale rom, og har vært en grunnleggende del av utleiring av kriminelle muligheter, prosesser og systemer som er avhengig av internett. Ekspertsystemer er teknisk eller faglig ekspertise som organiserer store områder

av livene våre (Giddens, 1997, s. 27). Vi er alle en del av ekspertsystemer som vi må ha tiltro til, selv om vi ikke nødvendigvis vet hvordan de fungerer. Eksempelvis har vi tiltro til arkitekten og byggearbeidet gjort i huset vi bor i, vi stoler på at veggene holder taket oppe og at vi er trygge der vi bor. Det er uvitenheten som gjør oss avhengig av å ha tiltro til ekspertsystemer (Giddens, 1997, s. 68). Ekspertsystemer kan også være ulike systemer knyttet til data og internett (Jones og Karsten. 2008, s. 134). Vi har tiltro til operativsystemet til vår datamaskin, anti-virusprogrammet vi har installert og at vårt personvern blir tatt vare på, selv om vi ikke har god kunnskap om hvordan dette fungerer.

Noen vil være enig i at vi i det moderne samfunn må ha tiltro til systemene rundt oss fordi vi ikke har noe annet valg – symbolske tegn og ekspertsystemer omringer alle aspekter av livene våre. Tillit var tidligere forankret i en personifisering, og relasjoner ble skapt ansikt til ansikt (Pettersen, 2018). I moderne samfunn derimot er tilliten mer anonymisert og vi er ikke lenger kun avhengig av tillit til andre personer. Vi er i dag like avhengig av tillit til symbolske tegn, eksperter og teknologi som vi før var avhengig av lokalsamfunnet (Pettersen, 2018). I moderne samfunn blir også kriminalitetsforebyggende tiltak preget av en anonymisering, politiet driver ikke lenger kun forebygging ansikt til ansikt. Er dette en god utvikling for kriminalitetsforebygging, eller svekker den mer anonyme karakteren arbeidet har kvaliteten på forebyggingen?

Det norske velferdssamfunnet er sterkt preget av tillit, og politiet innehar typisk høy tillit blant befolkningen. Resultatene fra en undersøkelse gjennomført av NorSIS (2019) tyder derimot på at den karakteristiske høye tilliten til politiet ikke består i sammenheng med datakriminalitet. I denne undersøkelsen kommer det frem at kun 44 % tror at politiet kan hjelpe dem dersom de blir utsatt for datakriminalitet (NorSIS, 2019). Over halvparten av de som ble spurt tror altså ikke at politiet kan hjelpe dem med dette. Også Giddens (1997, s. 69) innrømmer at det kan forekomme skepsis om ekspertsystemer, og at dette er en naturlig del av uvitenhet. Men uansett hvor hardt man prøver, vil man aldri klare å helt unnslippe å ha tiltro til ekspertsystemene – fordi de omfatter alle aspekter ved det moderne liv (Giddens, 1997, s. 69). Giddens tar utgangspunkt i at vi i moderne samfunn må ha mer tillit til flere og andre aktører enn vi hadde før. Men er tilliten som bygges gjennom ansiktsløse relasjoner like sterk som den som oppstår gjennom ansiktsforankrede relasjoner? Vil ansiktsløse interaksjoner kunne erstatte samhandling ansikt til ansikt eller vil dette nødvendigvis gå på bekostning av tillit?

3.1.3 Tid-rom komprimering

Et annet synspunkt på modernitetens påvirkning på sosial struktur ble presentert av David Harvey i hans «The condition of postmodernity: an enquiry into the origins of social change» i 1989, hvor han diskuterer globaliseringens påvirkning på tid og rom. Tid og rom er grunnleggende kategorier av menneskelig eksistens, men likevel blir konseptenes betydning sjeldent diskutert ifølge Harvey (1989, s. 201). Rom og tid er naturlige og hverdagslige begrep som vi alle vet betydningen av, men betyr konseptene det samme i dag som de gjorde før? Tid blir målt i sekunder, minutter, dager, år, som om alle konsepter av tid passer inn på én og samme ensidige skala (Harvey, 1989, s. 201). Konseptet rom blir rammet inn av fysiske betingelser, et sted har en retning, det omfatter et område, følger et mønster eller består av et volum (Harvey, 1989, s. 203). Harvey (1989, s. 204) hevder at tid og rom ikke lenger kan bli rammet inn av disse historiske konseptene. Nye teknologiske endringer har vært en nødvendig forutsetning for denne forandringen (Eriksen, 2014, s. 35). Innføringen av teknologier har ført til at forholdet mellom tid og rom har blitt komprimert, vår opplevelse av rom avhenger av tiden det tar å reise gjennom det. For å forklare hvordan konseptene tid og rom har blitt forvandlet i det postmoderne samfunn, lanserte Harvey begrepet «Time and space compression» (Tid-rom komprimering). Tid-rom komprimering er en prosess som endrer forholdet mellom tid og rom; opplevelsen av tid øker og betydningen av rom reduseres (Franko, 2020, s. 261).

Harvey sitt perspektiv om tid-rom komprimering har blitt videreutviklet i nyere forskning om globalisering. Tid-rom komprimeringen blir drevet av nettopp globaliseringen (Santos og Azevedo, 2019, s. 262). En viktig del av globaliseringsprosessen er bevegelsen av kulturelle bilder, informasjon og idéer, som gjør det mulig å besøke og kommunisere, både fysisk og virtuelt, med mennesker og steder omkring i hele verden (Franko, 2020, s. 7). I den globale verden kan vi reise på tvers av kloden ved hjelp av et tastetrykk, og fjernt blir til nært. Dagens kommunikasjons- og interaksjonsløsninger øker i en enorm fart, og Appadurai (1996, s. 33) hevder at det moderne liv utfolder seg i helt nye transnasjonale omgivelser, som landskaper bestående av etnografi, teknologi, media, finans eller idéer. Konsepter vi tidligere har opplevd som stabile, som geografiske grenser, blir visket ut som en følge av globale strømmer som driver på tvers av disse (Franko, 2020, s. 7). Komprimeringen av tid og rom kan sies å forvandle det historiske forholdet vi har til nærhet, vi er ikke lenger avhengig av fysisk avstand for å nå hverandre. Oppgaven vil fokusere på hvordan temaer knyttet til tid-rom komprimering utspiller seg særlig på feltet datakriminalitet og i sammenheng med bruk av sosiale kommunikasjonsmidler.

3.2 Data og kriminalitet

3.2.1 Data, kriminalitet og sted

Et av de største skillene mellom tradisjonell kriminalitet og datakriminalitet er stedet kriminaliteten utvikler seg. Internett bryter seg ut av begrensninger knyttet til tid og sted som påvirker interaksjon i den fysiske verden (Yar og Steinmetz, 2019, s. 14). Normale barrierer skapt av fysisk avstand finnes ikke på internett. Internett muliggjør øyeblikkelige møter og interaksjoner mellom mennesker med stor fysisk avstand (Shields, 1996, s. 7). I følge Yar og Steinmetz (2019, s.169) er datakriminalitet et fullstendig de-territorialisert fenomen på grunn av sin globale egenskap, en enkelt lovbryter kan gjennom internett ramme tusenvis av mennesker på en og samme tid. McGuire (2007, s. 8) hevder at kriminalitet som skjer i den virtuelle verden har gjennomgått en en hyperutstrekningsprosess, og slik strekker seg utover en rekke tradisjonelle grenser. Tid og sted er ikke lenger en utfordring for kriminelle, det er en mulighet. Selv om konseptet «sted» betyr ikke det samme på nett som i den fysiske verden, finner man fremdeles mye forskning på datakriminalitet å baserer seg på geografiske variabler, som for eksempel fra hvilke land de fleste data-angrep kommer fra (Miró-Llinares og Moneva, 2020, s. 4).

Den nye betydningen av fysisk tid og sted skaper utfordringer for håndteringen av datakriminalitet. Tradisjonelt er politiarbeid basert på områder, og datakriminalitet skaper på grunn av sin globale struktur utfordringer for lovgivning og utøvelse av denne. Forholdet mellom politi og lovbryter på nett er asymmetrisk; politiets virksomhet er knyttet til nasjonalt territorium, men lovbryterens virksomhet er ikke lenger geografisk forankret (Sunde, 2019a, s. 134). Datakriminalitet skaper utfordringer for både nasjonale og internasjonale rettslige jurisdiksjoner (Blakemore, 2012, s. 12). Grenseløsheten utfordrer territorialprinsippet, et folkerettslig prinsipp som fastslår en stats rådvelde over eget territorium (Snl, 2020). Skal en stat utøve tvangsmyndighet utenfor sitt territorium kreves det særskilt hjemmel (Snl, 2020). Det norske politi sitt handlingsrom er begrenset til Norge, og ettersom kriminalitet på nett ikke er bundet av de klare geografiske skillene som tradisjonelt preger rettsforfølgelse, byr dette på problemer for håndtering av visse straffbare tilfeller på nett. En innbygger i Norge kan bli utsatt for et lovbrudd utført av en lovbryter som sitter på andre siden av jorden. Hvilket lands lovgivning gjelder for lovbruddet, og hvilket rettssystem er det som skal etterforske saken? Det digitale rom er i sin globale natur internasjonalt, og omfattende transnasjonalt samarbeid er derfor viktig (Politidirektoratet, 2015, s. 14). Det digitale rom skaper slik et behov for en felles,

internasjonal lovgivning og strategi for å bekjempe datakriminalitet. Glick (2001, i Blakemore, 2012, s. 13) mener at de jurisdiksjonære grensene ideelt må fjernes helt for at stater skal skulle samarbeide godt nok om datakriminalitet, men han innrømmer også at dette vil være vanskelig i praksis. Hvordan skal politiet håndtere datakriminalitet uten at det er etablert en fullstendig internasjonal strategi?

Selv om datakriminalitet preges av muligheten til å krysse landegrenser, er ikke all kriminalitet som skjer ved hjelp av internett de-territorial. I 2013 gjennomførte Redd barna, Feltteamet Alna og Salto et prosjekt om digitale arenaer med Oslo-ungdom (Nettgruppen, 2013, s. 3). Her fant de at de fleste norm- og lovbruddene som skjer på nett, skjer mellom bekjente (Nettgruppen, 2013, s. 19). Selv om datakriminalitet kan skje over store geografiske områder, er det ikke alltid den gjør det. Et eksempel på datanorm- og lovbrudd som ofte er nærmere lokalt forankret er cyber-bullying (mobbing på nett). Mobbing på nett mellom jevnaldrende anses som en av handlingene unge på internett risikerer å utføre og bli utsatt for (Menesini, Nocentini og Palladino, 2016, s. 15). Datakriminalitet i mindre alvorlig grad som utarter seg mellom mennesker i samme lokalsamfunn får ikke den samme oppmerksomheten innenfor teori og forskning som. I følge Wall (2008, s. 871) er eksempelvis mobbing på nett et fenomen som på grunn av sin dagligdagse karakter blir oversett eller regnet som uviktig i sammenligning med datainnbrudd eller angrep utført av sofistikerte hackere.

3.2.2 Data, kriminalitet og anonymitet

På internett får man mulighet til å gjenoppfinne seg selv, det virtuelle selvet kan være hvem som helst (Yar og Steinmetz, 2020, s. 14). Internett gjør det enkelt å skape sin egen identitet, og byr på mange teknikker som kan hjelpe med å skjule hvem du faktisk er. Anonymitet er et mektig verktøy som kan blir utnyttet av datakriminelle (Snyder, 2001, s. 252). De får muligheten til å begå lovbrudd i en digital forkledning, ukjent for både offer og politi. Denne anonymiteten bidrar til at den opplevde oppdagelsesfaren er lav blant lovbryterne. Anonymitet gir ikke bare en mulighet for kriminalitet, det byr også på utfordringer for politiet (Sunde, 2019a, s. 134). Å spore opp lovbrytere i den digitale verden kan være vanskeligere enn i den fysiske verden, fordi muligheten til å forbli anonym finnes. En nøkkelegenskap for datakriminalitet er utnyttelsen av digitale spor (Wall, 2007, s. 36). Det er imidlertid ikke bare potensielle ofre som legger igjen spor på nett, dette gjelder for alle internettbrukere. Selv om lovbrytere opplever seg trygge fra politiets søkelys, har politiet en mulighet til å følge spor fra

kriminelle aktiviteter. Men jo mer sofistikerte datakriminelle blir, jo mer teknisk kompetanse krever det av politiet for å effektivt kunne avsløre dem.

En gjenganger i kriminologiske teorier er fokuset på lovbrytere; hvem blir lovbrytere, hvor er lovbrytere fra, hvorfor ender de opp med å begå lovbrudd? Selv om datamaskin og teknisk utstyr i dag er en vanlig gjenstand å eie, har det ikke alltid vært sånn. Datamaskiner var lenge kostbare maskiner kun store selskaper hadde råd til å eie. Datakriminalitet kunne slik også kun bli begått av foretaket eller foretakets ansatte (Sunde, 2019a, s. 130-131). Kriminalitet utført med hjelp av data ble derfor lenge kategorisert som hvitsnippkriminalitet, og eksempelvis var det Økokrim som først fikk ansvar for å bekjempe datakriminalitet i Norge (Sunde, 2019a, s. 130). Datakriminalitet består i dag av mange ulike kriminelle aktiviteter og er praktisk mulig å utføre av en større gruppe mennesker, men den tekniske kompetansen som ofte kreves kan fremdeles skille datalovbryterne fra tradisjonelle lovbrytere.

Datakriminelle kan ha typisk andre karakteristikker enn tradisjonelle kriminelle (Gill, 2019, s. v). Undersøkelser viser at det finnes en sammenheng mellom lovbrytere og dårlige sosioøkonomiske forhold som familieforhold, lav utdanning og svak tilknytning til arbeidslivet (Thorsen, Lid og Stene, 2009, s. 128-129). Sosial eksklusjon, marginalisering og deprivasjon er også nøkkelord knyttet til mange kriminologiske teorier som undersøker hvorfor mennesker begår lovbrudd (Yar og Steinmetz, 2020, s. 16). Karakteristikkene nødvendig for å begå datakriminalitet bryter derimot med denne tradisjonelle tankegangen om hvem lovbrytere er. For å utføre datakriminalitet kreves det høy teknisk kompetanse, kompetanse som kan oppnås gjennom utdannelse eller arbeidsliv, og dyrt utstyr (Yar og Steinmetz, 2020, s. 16). Det er derfor ikke usannsynlig at lovbrytere som utfører data-avhengig kriminalitet typisk hører til en mer privilegert klasse enn tradisjonelle lovbrytere, fordi det krever flere ressurser og kunnskap for å utføre datakriminalitet. Tanken om at kriminalitet er sosialt plassert trenges ikke nødvendigvis å forkastes i sammenheng med datakriminalitet, men de sosiale mønstre for datalovbrytere skiller seg slik fra typiske sosiale mønstre for andre typer kriminalitet.

3.3 Kriminalitetsforebygging og datakriminalitet

Politiet er samfunnets utøvende makt, en sterk institusjon som skal bekjempe kriminalitet og beskytte befolkningen ved å patruljere gater, etterforske saker og bekjempe lovbrudd med sitt voldsmonopol. Samtidig stadfester Politilovens § 1 at politiet har flere roller enn kriminalitetsbekjempelse; de er en hjelpende, håndhevende og forebyggende virksomhet. Forebygging av kriminalitet er et vidt og vagt begrep, og består av et bredt spekter av metoder

og strategier (Lie, 2011, s. 21). Det finnes mange lærebøker, definisjoner og teorier knyttet til forebygging av kriminalitet. I følge Bjørgo (2015, s. 16) omfatter begrepet kriminalitetsforebygging handlinger som reduserer fremkomsten av fremtidige lovbrudd eller eventuelt skadevirkningene av disse. Gundhus (2014, s. 179) viser til at kriminalitetsforebygging kan sies å forebygges gjennom alle tiltak som virker positive på samfunnet og rettshåndhevelse av loven kan virke allmennpreventivt (Gundhus, 2014, s. 179). Videre presenterer Lab (2020, s. 34) en snevrere definisjon på begrepet:

> «Forebygging av kriminalitet omfatter enhver handling som er skapt med et mål om å redusere den faktiske kriminaliteten og frykten for denne» (Lab, 2020, s. 34).

Oppgaven tar sikte på å undersøke hvordan politiet driver digitalt forebyggende politiarbeid, det vil si hvilke tiltak og metoder de tar i bruk med hensikt om å forebygge kriminalitet. Med bakgrunn i oppgavens problemstilling, ser jeg det derfor som hensiktsmessig å benytte meg av Lab sin definisjon av forebygging av kriminalitet videre i oppgaven.

Kriminalitetsforebygging må skilles fra kriminalitetskontroll, som innebærer håndtering av allerede eksisterende tilfeller av lovbrudd (Lab, 2020, s. 34). Samme aktiviteter kan resultere i både kontroll av og forebygging av kriminalitet, eksempelvis kan politi på patrulje oppdage og håndtere kriminalitet, men tilstedeværelsen kan også ha en avvergende og preventiv effekt. Skillet mellom disse begrepene går hvor i den kriminelle handlingsprosessen politiaktiviteten slår inn. Kriminalitetsforebyggende strategier har fokuspunkt forut for kriminaliteten, de skal forhindre at lovbrudd i det hele tatt finner sted (Lie, 2011, s. 21). Forebygging av kriminalitet kan også sies å være trygghetsskapende arbeid. Dette er en viktig presisering, da denne oppgaven ikke bare handler om forebygging av datakriminalitet, men også å vise hvordan politiet ønsker å øke sin tilstedeværelse på internett og drive med trygghetsskapende arbeid på digitale plattformer. Politiet ønsker ikke bare å forebygge fremtidige lovbrytere og lovbrudd, men også fremtidige ofre. For å gjøre dette må de oppmuntre det sivile samfunn å ta større ansvar for sin egen sikkerhet (Gundhus, 2014, s. 179). Å informere samfunnet om hvordan de selv skal håndtere kriminalitet, og hvordan de best mulig kan sikre seg mot det er også kriminalitetsforebyggende tiltak.

Politiet er på ingen måte den eneste aktøren som utfører tiltak og påvirker forebygging av kriminalitet. Mange forebyggende verktøy er fordelt i andre offentlige etater, og i både offentlige og frivillige organisasjoner (Bjørgo, 2015, s. 13). Skoler og ungdomsklubber er eksempler på viktige forebyggende arenaer for unge. Privat kriminalitetskontroll og sikkerhet

har de siste årene utviklet seg til å bli en kommersiell industri, trygghet er ikke lenger bare et offentlig gode (Loader og Walker, 2007, s. 22). Kriminalitetsforebygging i Norge har også i en viss grad blitt utsatt for privatisering, eksempelvis samarbeider den frivillige organisasjonen Natteravnene, som er til stede for barn og unge ute på gata på nattestid, med forsikringsselskapet Tryg (Egge og Gundhus, 2012, s. 267). Involveringen av ikke-statlige aktører i politivirksomhet kalles «plural policing» (pluralt politiarbeid). Politiet er ikke den eneste aktøren som utøver polisiært arbeid, og de siste tiårene har vi vært vitne til en stor økning i det private sikkerhetsmarkedet (Newburn, 2013, s. 643). Jones og Newburn (1998, s. 116) viser til at en årsak til denne veksten kan være at kriminalitetsnivået og den generelle usikkerheten blant folket har økt de siste tiårene, og slikt skapt et behov for sikkerhet som politiet alene ikke klarer å imøtekomme. Det er heller ikke bare organisasjoner og bedrifter som i tillegg til politiet er forebyggende aktører i det norske samfunn; nærmiljø og foreldre er også viktige i det forebyggende bildet. Alle aktører virker sammen mot et helhetlig forebyggingsbilde, og det er viktig at de samspiller.

Hvordan kan de ulike forebyggende tiltakene forstås? Brantington og Faust (1976 i Gilling, 1997, s. 4) tok i bruk uttrykk som stammet fra medisinsk litteratur om forebyggende helsetiltak for å kategorisere kriminalitetsforebyggende arbeid. Disse begrepene er primær-, sekundær- og tertiærforebygging, og fungerer som ulike nivåer basert på hvem de forebyggende strategiene er rettet mot. Primærforebygging forstås som forebyggende strategier med en universell karakter, som er rettet mot store grupper eller befolkningen generelt (Bjørgo, 2015, s. 22). Primærstrategier for forebygging forsøker å eliminere generelle fysiske og sosiale faktorer som gir kriminalitet en mulighet til å blomstre (Lab, 2020, s. 57). Det er en systemrettet tilnærming til forebygging; fokuset ligger på hvordan kriminalitet kan forhindres gjennom endringer i samfunnet. Strafferettssystemet er kanskje det mest omfattende forebyggende strukturen som kan knyttes til primærstrategier. Konsekvensene av et lovbrudd er i seg selv avskrekkende; frykten for å bli i lagt negative og ubehagelige sanksjoner fra samfunnet i form av formell straff kan føre til forebygging av kriminalitet. Å ilegge et individ straff kan altså medføre avverging av framtidig kriminalitet, straff kan bli en forebyggende trussel for resten av samfunnet (Lab, 2020, s. 36). Straffesystemet har slik en generell avskrekkende effekt som kan påvirke befolkningen til å forbli lovlydige. Sekundærforebygging omfatter forebygging rettet mot dem som anses å være i en risikosone for å bli lovbrytere eller ofre for lovbrudd (Gilling, 1997, s. 4). For å kunne vurdere hvem som burde kategoriseres som risikogrupper og de forebyggende tiltakene derav burde bli rettet mot, må man forsøke å forutse framtiden av kriminell aktivitet

(Lab, 2020, s. 172). Tertiære forebyggingsstrategier retter seg mot de som allerede har begått kriminalitet eller blitt utsatt for kriminalitet (Gilling, 1997, s. 4). Forebyggingen forsøker å forhindre tilbakevendende kriminell oppførsel og skåne samfunnet for videre kriminell utsettelse (Lab, 2020, s. 37). Strafferettsystemet innebærer blant annet tertiær forebygging gjennom spesifikk avskrekking. Individet som har begått kriminalitet og blitt ilagt en straff kan oppleve dette som så ubehagelig eller uønsket at det påvirker valget deres om å begå flere lovbrudd i framtiden.

3.3.1 Forebygging av datakriminalitet

Politiet skal være en forebyggende enhet, også når det kommer til datakriminalitet. I datakrimstrategien kom det derimot frem at norsk politi i liten grad utfører forebyggende arbeid knyttet til datakriminalitet (Politidirektoratet, 2015, s. 12). Det har blitt over tid rettet lite oppmerksomhet mot forebygging av datakriminalitet, både innenfor politiet men også innenfor forskning (Brewer, de Vel-Palumbo, Hutchings, Holt, Goldsmith og Maimon, 2019, s. 2). Selv om interessen rundt forebyggende tiltak som kan utføres på nett lenge har vært lav, ser man en økende interesse (Sunde, 2019a, s. 134). I Norge er mye av forskningen på forebygging av kriminalitet på internett knyttet mot seksuallovbrudd og ungdommer. Inger Marie Sunde undersøkte hvordan politiet bruker chat for å etterforske og forebygge seksuelle overgrep som skjer over nett (Sunde, 2019b, s. 177). Arbeidet bygger på erfaring fra ”The Sweetie Project”, et prosjekt som utvikler teknologier for å avdekke seksuelle overgrep. Politiet tar i bruk en chatbot eller manuell chatting, som vil si at en politibetjent utgir seg for å være et barn, i åpne eller lukkede forum på internett (Sunde, 2019b, s. 178). Som tidligere nevnt, gjennomførte Redd barna, Feltteamet Alna og Salto et prosjekt i 2013 med Oslo-ungdom for å undersøke norm- og lovbrudd blant ungdom på digitale arenaer. De var opptatt av å finne ut hva ungdom selv, politiet og fagfolk som arbeider med ungdom, kan gjøre for å forebygge kriminalitet på nettet (Nettgruppen, 2013, s. 3). Gjennom kafé-prater med ungdom fant de blant annet at ungdommer flest har liten kunnskap om lover og regler på internett og at det finnes store gråsoner mellom det som er vanlig tull og lovbrudd (Nettgruppen, 2013, s. 19).

Mye av fokuset viet til forebygging av datakriminalitet er knyttet opp mot potensielle ofre, ikke lovbrytere. Å informere individer om hvilke grep de kan ta for å beskytte seg selv og gjøre seg selv mindre sårbare på nett, kan forebygge en stor del av kriminaliteten (Staniforth, 2017, s. 123). At staten overlater ansvaret for beskyttelse over til private aktører eller innbyggerne selv, er ikke et nytt fenomen. Garland (1996, s. 452) beskriver en strategi statlige aktører tar i bruk i møte med blant annet forebygging av kriminalitet, som i større grad består av å fordele ansvaret

til andre, ikke-statlige aktører. I det senmoderne samfunnet er beskyttelse mot kriminalitet overført til markedet, lokalsamfunnet og enkeltindividet (Aas, 2006, s. 75). Garland kaller dette for en «responsibilization strategy» (ansvarliggjøringsstrategi). Staten står fremdeles med hovedansvaret for beskyttelse mot kriminalitet, men strategien går ut på at blant annet innbyggerne selv også må delta aktivt for å bevare sin egen sikkerhet (Garland, 1996, s. 452). Politiets rolle blir å styre på avstand og styrke kriminalitetsforebyggende tiltak lokalsamfunnet og kommersielle aktører setter i gang (Aas, 2006, s. 75). Braithwaite (2000, s. 223) forklarer forholdet mellom den nye regulerende stat og det private sikkerhetsmarkedet som roing og styring. Private aktører tilbyr trygghet og sikkerhet, de «ror» markedet, og statens rolle blir å regulere, de styrer markedet (Braithwaithe, 2000, s. 226). Crawford (2006, s. 471) hevder at til tross for at staten har inntatt en mer passiv rolle innenfor polisiær virksomhet, står staten fremdeles sterkt. Dette nye bildet av staten, som overlater mye av «roingen» til private aktører, er godt egnet til å beskrive internett, for som Bygrave og Michaelsen (2009, s. 92) viser til har styringen av internett i stor grad har blitt gjennomført av og overlatt til private aktører.

Ifølge Williams og Levi (2017, s. 454) kan en mulig årsak til hvorfor fokuset for kriminalitetsforebyggingen er skiftet fra lovbryteren og til mulige ofre og spesifikke lovbrudd er at vi ikke har nok tilgang til datakriminelle og deres motivasjoner. Williams og Levi (2017, s. 459) beskriver at individer kan foreta seg tre former for primærforebygging for å beskytte seg selv mot datakriminalitet; aktiv, unnvikende og passiv. Aktiv forebygging går ut på å jevnlig endre utsatte sikkerhetsrisikoer, som å endre på sikkerhetsinnstillinger og passord ofte, mens unnvikende forebygging går ut på å utføre mindre aktiviteter på nett (Williams og Levi, 2020, s. 459-460). Passiv primærforebygging er den enkleste formen for beskyttelse, som å installere anti-virusprogram og aktivere et spamfilter for sin e-postinnboks (Williams og Levi, 2020, s. 459-460). Private leverandører av teknologi har fått en voksende rolle og gjennomgripende innflytelse i kontrollen av det digitale, som bidrar til å omforme konturene av politiarbeid (Bowling, Reiner og Sheptycki, 2019, s. 158). Begreper som pluralt politiarbeid og ansvarliggjøring er sentrale begreper for forebygging av datakriminalitet.

Forebyggende tiltak mot datakriminalitet møter på flere særegne utfordringer knyttet til dens digitale karakter. Forebyggende tiltak på nett som overvåker eller hindrer oppførsel på nett kan stride i mot personvern og ytringsfrihet (Sunde, 2019a, s. 134). Grensen mellom beskyttelse av individer og samfunn, og inngripende sensur, kontroll og overvåkning av befolkningen blir stadig mer visket ut (Politidirektoratet, 2015, s. 113). Datakriminalitet sin globale egenskap skaper utfordringer når det kommer til etterforskning og rettsforfølgelse, og det samme skjer i

forbindelse med forebygging av den (Yar og Steinmetz, 2019, s.169). Hvor på nett er det norsk politi skal ha mulighet til å drive forebyggende arbeid? Til og med internettsider basert i Norge, som for eksempel norske profiler på sosiale medier, er ikke nødvendigvis norsk territorium. Eksempelvis driver norsk politi forebygging på sosiale medier, men selve plattformene er utenlandske; Facebook er amerikansk og videodelingsappen TikTok er kinesisk. I tillegg er det ikke slik at alle nordmenn holder seg til norskbaserte profiler eller nettsider. Hvilke områdeprinsipper som gjelder for datakriminalitet må også avklares når det kommer til forebygging av datakriminalitet (Sunde, 2019a, s. 147). Forebyggende tiltak på nett kan også vanskeliggjøre etterforskning av datakriminalitet. Integrerte sikkerhetsfunksjoner som skal ha en forebyggende effekt, kan hindre tilgangen på digitale bevis (Politidirektoratet, 2015, s. 113). Det oppstår slik en konflikt, skal politiet satse på å forhindre at kriminalitet finner sted eller forsikre seg om at de vil ha den beste muligheten til å etterforske de lovbruddene som finner sted?

3.3.2 Situasjonell kriminalitetsforebygging

Situasjonell forebygging vokste frem i Norge på 1980-tallet, hvor en ny giv for kriminalitetsforebyggende arbeid vokste frem i nordisk sammenheng (Gundhus, 2014, s. 184). Tanken om situasjonell forebygging bygger videre på et fokus på hvilken rolle naturlige og sosiale miljøer spiller for kriminalitet (Lab, 2020, s. 32). Det er en handlingsorientert tilnærming til forebygging, hvor fokuset flyttes fra individet og til den kriminelle handlingen. Situasjonell kriminalitetsforebygging baserer seg på at kriminalitet er styrt av rasjonelle valg og vektlegger selve områdene og omgivelser kriminalitet finner sted i (Lie, 2011, s. 253). Situasjonell kriminalitetsforebygging forsøker ikke å endre på de fjerne årsakene til kriminalitet, som en mulig lovbryters motivasjon til å begå kriminalitet, men tar heller sikte på de nære årsakene (Smith og Clarke, 2012, s. 292). Nære årsaker til kriminalitet kan være at det oppleves som attraktivt å begå kriminalitet fordi området man befinner seg i har gode muligheter for enkelte kriminelle handlinger eller at oppdagelsesfaren i situasjonen man befinner seg i er lav, som i en dårlig belyst gate eller i et nabolag med gamle dørlåser som er enkle å bryte opp. Kriminalitet blir et rasjonelt kost-nytte regnestykke, og ved å bidra til at kostnaden ved å begå kriminalitet oppleves som høyere enn nytten vil man kunne avverge kriminelle handlinger (Lie, 2011, s. 254). De nære årsakene til kriminalitet tenkes å være mer mottagelige for endring enn de fjerne, eksempelvis er det å installere gatelys er betydelig enklere enn å kontrollere en persons temperament (Smith og Clarke, 2012, s. 292).

Situasjonell forebygging baseres også på rutineaktivitetsteori, som tar utgangspunkt i at mennesker vil begå lovbrudd så lenge forholdene ligger til rette for det (Lie, 2011, s. 259). Knutsson og Søvik (2005, s. 14) viser til lovbruddstriangelen som fastlegger tre grunnleggende elementer som må være tilstede for at et lovbrudd skal finne sted; en motivert gjerningsmann, et passende offer eller subjekt, og fraværet av beskyttere. Situasjonell forebygging forsøker på bakgrunn av denne tankegangen å identifisere muligheter for å begå bestemte typer kriminalitet, for å videre forsøkte å eliminere disse (Bjørgo, 2015, s. 36). Dette gjøres for å oppnå to ønskede resultater; å redusere de faktiske muligheter for å begå kriminalitet og øke sjansene for å bli oppdaget (Clarke, 1980, s. 139). Tanken er at ved å endre situasjoner der kriminalitet kan finne sted, vil man kunne påvirke individers beslutninger om å utføre kriminalitet (Gundhus, 2014, s. 185). Manipulasjon av situasjoner kan for eksempel oppnås ved å endre et fysisk område, som å lage flere fartshumper i veien, eller øke kontroll, for eksempel ved å sette opp flere overvåkningskameraer eller øke patruljering i visse områder.

Det er ikke bare fysiske rom som kan manipuleres for å avverge mulige lovbrudd, dette kan også skje i den virtuelle verden. Naturen av de teknologiske omgivelsene gjør at situasjonell kriminalitetsforebygging kan virke svært effektivt, ettersom datasystemer og internett er godt tilrettelagt for manipulering (Lessig, 1999, s. 6). Situasjonelle teknikker for kriminalitet som skjer på nett fokuserer på selve grunnlaget av internett: nemlig koder (Williams og Levi, 2017, s. 454). Mye av den grunnleggende sikkerheten vi benytter oss av på internett hver dag er også situasjonelle forebyggingsmekanismer. Innstallering av antivirus-program, brannmurer, bruk av passord og aktivering av spamfiltre er eksempler på dagligdagse sikkerhetsmekanismer som vanskeliggjør kriminelle aktiviteter (Brewer m.fl., 2019, s. 20). Det forsket på situasjonelle tiltak man selv kan gjøre for beskyttelse mot datakriminalitet, og effekten av disse. Surisetty og Kumar (2010) undersøkte effektiviteten av brannmurer for å kontrollere og filtrere utgående og inngående aktivitet, og Algaith, Gashi, Sobesto, Cukier, Haxhijaha, og Bajrami (2016) utførte en empirisk undersøkelse av ni ulike antivirus-programmer og blant annet kvaliteten mellom gratis versjoner versus fullstendige versjoner. Bonneau (2012) undersøkte forholdet mellom antall mulige gjetninger på et passord, variasjoner i passordbruk og hacking ved hjelp av passordgjetning. Han konkluderte blant annet med at individer ofte bruker for lite varierende passord og at strengere regler for valg av passord kan gi en betydelig høyere motstand mot hacking via passordgjetting (Bonneau, 2012, s. 550).

Det er også forsket på situasjonelle kriminalitetsforebyggende tiltak som politiet velger å ta i bruk. Hutchings, Clayton og Anderson (2016) undersøkte effekten av fjerning av nettsider hvor

det antas å foregå kriminell aktivitet. Dette kan blant annet være nettsider som forsøker å lure individer til å legge igjen kortinformasjon, sider som brukes for å distribuere overgrepsmateriale eller sider med skadelig datavare (Hutchings, Clayton og Anderson, 2016). Ved å fjerne slike nettsider, fjerner man også plattformen til og anledningen for kriminelle handlinger. Hutchings, Clayton og Anderson (2016) viser til at det kan være et ueffektivt tiltak for politiet, fordi de må kontakte en tredjepart for å få gjennomført fjerningen. Dette kan både ta lang tid, og det er ikke en selvfølge at politiet eller andre møter velvilje hos vertene. Maimon, Alper, Sobesto og Cukier (2014) forsøkte å undersøke hvilken effekt advarende meldinger hadde på datainnbrudd ved å lokke til seg innbrudd i systemer både med og uten advarende meldinger. Slike meldinger har som formål å modifisere menneskers oppførsel ved å for eksempel advare om at en handling er ulovlig, og kan for eksempel plasseres på automatisk sikkerhetsprogramvare (Brewer m.fl., 2019, s. 23). Maimon m.fl. (2014, s. 33) fant ingenting som tydet på at tilgjengelige advarende meldinger førte til at datainnbrudd umiddelbart ble avsluttet eller førte til en nedgang i frekvensen av datainnbrudd, men at lengden på datainnbruddene der det var en synlig advarende melding var kortere enn uten en slik melding.

3.3.3 Lokalorientert kriminalitetsforebygging

Lokalorientert kriminalitetsforebygging er et vidt begrep, og referer til forebyggende strategier som bygger på idéen om at det er mer enn individene som skaper kriminalitet (Gundhus, 2014, s. 187). Lokalorientert forebygging baserer seg på en politimodell med fokus i lokal forankring og samarbeid med publikum (Lie, 2011, s. 183). Fokuset i denne tilnærmingen til kriminalitet og forebygging ligger på et høyere nivå enn situasjonell forebygging, nemlig lokalmiljøet (Gundhus, 2014, s. 187). Sammenlignet med situasjonell forebygging er ikke lokalorienterte forebyggingsstrategier veldig teoretisk forankret eller nøye definert. Det er omstridt om det i det hele tatt kan kalles for en forebyggende metode, og blir ofte omtalt mer som en filosofi for politiarbeid (Lab, 2020, s. 244). Men denne filosofien har gitt inspirasjon til forebyggingsstrategier som baserer seg rundt relasjoner, engasjement og arbeid knyttet til lokalmiljø, og nærhet mellom politi og publikum. På grunn av det manglende teoretiske grunnlaget er resultatene av lokalorientert grunnlagte strategier ulike, men har som fellesfaktor at de fokuserer på sosiale nettverk og hverdagskriminalitet (Gundhus, 2014, s. 187).

En bred strategi innenfor lokalorientert forebygging er lokalorientert politiarbeid, også kalt «Community Policing». Skogan (2006 i Gundhus, 2014, s. 187-188) identifiserer tre kjennetegn ved lokalorientert politiarbeid; Sivilt engasjement, problemløsning og desentralisering. Sivilt engasjement går ut på at lokalmiljøet skal involveres i å identifisere kriminalitetsproblemer og

trender, og hvilke tiltak som skal settes inn for å forebygge disse (Lab, 2020, s. 245). Dette krever at det etableres plattformer hvor politiet kan samhandle med publikum (Gundhus, 2014, s. 187). Ulike lokalmiljøer møter ulike problemer, og lokalorientert politiarbeid skal tilpasse seg til hvert enkelt miljøs største utfordringer. Politiet forsøker å knytte sterke bånd med lokalmiljøet, og dette gjøres ofte ved å plassere de samme politibetjentene i samme miljø over en lengre tidsperiode (Bullock og Fielding, 2017, s. 94). Lokalorientert politiarbeid er problemorientert, og forsøker å se på de underliggende årsakene til problemene og kriminaliteten som preger lokalmiljøet (Lab, 2020, s. 245). Desentralisering er en viktig del av lokalorientert politiarbeid for å gjøre politiet mer tilgjengelig for befolkningen (Gundhus, 2014, s. 188).

Lokalorientert politiarbeid er videre bygget mye videre, blant annet til strategien beroligende politiarbeid (Gundhus, 2014, s. 191). Beroligende politiarbeid ligner svært på sin forkommer, men de to strategiene skilles på et punkt; hovedmålet med arbeidet. I beroligende politiarbeid er det nemlig publikums trygghetsfølelse og tillit til politiet som står i fokus (Gundhus, 2014, s. 191). Det er altså ikke bare kriminalitetsreduksjon som er viktig for politiet, men å fremtre i lokalsamfunnet på en måte som betrygger publikum (Lie, 2011, s. 191). For å oppnå dette blir fokuset rettet mot signal-kriminalitet, kriminelle hendelser som blir opplevd som nærliggende problemer i lokalmiljø (Aas, 2006, s. 78). Slik sender politiet signaler til befolkningen om at de tar deres sikkerhet på alvor og at de er til å stole på. For å kunne fokusere på de viktigste hendelsene, er det avgjørende at politiet har tette bånd med befolkningen. Fokuset innenfor en beroligende strategi er ikke kriminalitet i seg selv, men hvordan befolkningen opplever kriminalitet og uønskede hendelser (Weston, 2010, s. 758). Som jeg kommer til å vise i analysedelen er politiets strategier når det gjelder datakriminalitet ofte rettet nettopp mot å vise sin tilstedeværelse på internett, og betrygge befolkningen om at dette ikke er et lovløst rom.

3.4 Politikultur

En yrkeskultur kan beskrives som et nettverk av mentale prosesser som veileder hvordan tilværelsen organiseres og forstås (Gundhus, 2006, s. 44). Alle yrker har typiske kulturer, men spesielt politikulturen har fått mye oppmerksomhet i både i forskning og media. Politikultur referer til hvordan politiet ser verden og sin egen rolle i den (Finstad, 2018, s. 98). Politikultur består av et sett av normer, tro og verdier som påvirker politiets oppførsel både operasjonelt og mellom hverandre (Loftus, 2009, s. 4). Politiet er en del av den demokratiske stats utøvende

makt, et symbol på lov og rett og har beskyttelse av samfunnet som hovedoppgave. De spiller en fundamental rolle i samfunnet med sitt voldsmonopol og døråpner til straffesystemet (Loftus, 2009, s. 4). For å bevare demokratiets rettssikkerhet er det viktig å reflektere over makten politiet har og hvilke mekanismer som kan være med på å påvirke måten politiet utøver denne på. Gundhus (2006, s. 42) påpeker at det ikke bare finnes én homogen politikultur, men at politikulturer består av et mangfold og variasjoner.

En mye omdiskutert yrkeskultur i politiet karakteriseres blant annet av maskuline normer, et mulig resultat av at politi lenge ble oppfattet som et mannsyrke (Petersson, 2014, s.122). Selv om kjønnsfordelingen av ansatte i politiet ikke lenger er så store som de var før lever enda assosiasjonen mellom politiyrket og menn i samfunnet, eksempelvis gjennom at ansatte i politiet i dagligtale fremdeles ofte blir omtalt som politimenn. Det har vært vanskelig for kvinner å bli akseptert inn i politiet og bli politibetjenter på lik linje som menn (Lofthus, 2009, s. 10). I lang tid ble menn tildelt arbeidsoppgaver knyttet til fysisk makt, mens de mindre fysiske arbeidsoppgavene som kontorarbeid ble delegert til kvinnene (Petersson, 2014, s. 122). Kvinner har i senere tid fått slippe til i større deler av politiet, eksempelvis er opptaket på Politihøgskolen i dag ganske likt mellom kvinner og menn, men arbeidsfordelingen innad i institusjonen preges fremdeles av kjønn (Ellingsen og Lilleaas, 2020). Wathne (2016) finner i sin forskning om kvinners plass i politiet at kun 16, 5 % av kvinner jobber med orden, mens andelen kvinner som jobber som etterforskere er dobbelt så høy som menn. Det er altså fremdeles en skjevdeling av arbeidsoppgaver innad i politiet som kan tenkes å bidra til reproduksjon av den tradisjonelle tøffe, sterke og macho politikulturen. Også yrkets karakter bidrar til denne reproduksjonen. Politiet må oppsøke risikofylte situasjoner, det er alltid mulige farer (Bowling, Reiner og Sheptycki, 2019, s. 172). «Ordentlig politiarbeid» består av adrenalin, tøffe konfrontasjoner på gata og fysisk krevende arbeid.

I realiteten består politiyrket i dag av mye mer enn en spenningsfylt jakt etter de hardbarka kriminelle. Normene som reproduseres om at politiyrket skal bestå av fart og adrenalin krasjer med politiets administrative og forebyggende oppgaver. Arbeidsoppgaver knyttet til kriminalitetsforebygging er oppgaver for kvinner og bamsepoliti, ikke for «ordentlige» politimenn. Tidligere forskning viser at den tradisjonelle forebyggende politirollen ses på som en underordnet form for maskulinitet, og blir omtalt som å utføre politiarbeid i kvinneklær (Ericsson, 2000, s. 30). Kriminaliteten har flyttet seg fra gata til data, og politiet må følge etter. Det økende fokuset på datakriminalitet og digitalt forebyggende politiarbeid strider mot den tradisjonelle politirollen som har formet organisasjonen og prioriteringer (Wall, 2007, s. 161).

Jensen og Stubberud (2011, s. 5) hevder at politiarbeid burde bestå av god gammeldags dialog, ikke av datamaskiner, analyser og avstand fra folket som teknologibasert politiarbeid tenkes å presentere. Motsetningen det digitale skiftet representerer kan støte mot allerede etablerte yrkeskulturer og forsterke gamle eksisterende kulturelle skiller (Gundhus, 2006, s. 448).

4. Metode

Dataene som har blitt hentet ut er gjort med hensikten å svare på oppgavens problemstilling. Datamaterialet består av intervjuer med ansatte i ulike deler av politiet og sier noe om hvordan de utfører arbeid med og hvordan de opplever arbeidet med digital kriminalitetsforebygging. Først vil kapittelet ta for seg intervju som metode og beskrive prosessen bak innhenting av datamaterialet. Videre vil planleggingen og gjennomførelsen av intervjustudien presenteres, før oppgaven forklarer hvordan dataene har blitt behandlet og analysert blir. Til slutt vil kapittelet presentere hvilke hensyn som er tatt til datamaterialets kvalitet og etiske problemstillinger.

4.1 Intervju som metode

Da jeg skulle velge hvilken metode jeg skulle ta for meg falt valget raskt på en kvalitativ tilnærming. I kvantitativ metode legges det vekt på å forklare et fenomen, mens kvalitativ metode søker etter å få en forståelse av et fenomen (Tjora, 2012, s. 18). I denne oppgaven søker jeg etter å få en forståelse for hvordan politiet arbeider og hva som blir lagt vekt på i arbeidet med digitalt forebyggende politiarbeid. Jeg ønsker å blant annet trekke dette opp mot teorier om tradisjonelt forebyggende arbeid, og dette er ikke et spørsmål som nødvendigvis har et svar man kan sette to streker under. Selvsagt kunne jeg lest arbeidsbeskrivelsene til de ulike stillinger i politiet som arbeider med digitalt forebyggende politiarbeid, men dette hadde skapt en svært lite nyansert oppgave, og heller ikke vært en god fremstilling av hvordan politiet faktisk arbeider. Politiyrket består av svært komplekst, dynamisk og ikke minst reaktivt arbeid. Hvilke innsatser som skal settes inn for forebygging og hvor disse skal settes inn endres fra år til år, uke til uke og dag til dag. For å få tak i et datamateriale som kan hjelpe med å belyse dette valgte jeg å ta i bruk intervjuer for innsamling av data. Kvalitative intervjuer kan gi forskeren et unikt innsyn i en persons tanker og opplevelser av et fenomen. Gjennom å intervjue kan forskeren få tilgang til detaljerte beskrivelser og god kunnskap som ellers hadde vært utilgjengelig (Weiss, 1994, s. 1). For å få best mulig informasjon om politiets forebyggende arbeid på nett og med datakriminalitet var det viktig at jeg fikk intervjue ansatte i politiet som jobber med dette på daglig basis. De er de mest pålitelige kildene, og vil kunne gi meg de beste skildringene av hvordan de utfører sitt arbeid.

4.2 Utvalg og rekruttering

Intervjuer er også en god metode for å innhente ulike synsvinkler på samme fenomen ved å intervjue personer som kan ha ulike fortolkninger og innfallsvinkler (Skilbrei, 2019, s. 66). Fordi jeg ønsker å få et helhetlig bilde av politiets arbeid med digitalt forebyggende politiarbeid

var det viktig å få informanter fra flere steder og med ulike arbeidsoppgaver innenfor politiet. Thagaard (2018, s. 54) forteller at et strategisk utvalg baseres på å systematisk utvelge personer eller enheter som har kvalifikasjoner som vil være strategiske i forhold til problemstillingen. Jeg ønsket å intervjue personer med spesiell kompetanse og erfaringer om digitalt forebyggende politiarbeid og datakriminalitet, og gjennomførte derfor et strategisk utvalg. Dette gjorde jeg i håp om at datamaterialet vil gi meg nok bredde til å kunne utforme en større forståelse av politiets arbeid med digitalt forebyggende politiarbeid. Jeg sendte derfor en søknad til et politidistrikt, Vest politidistrikt, og en søknad til et særorgan i politiet, Kripos. Jeg rettet disse søknadene mot avdelinger som har digital kriminalitetsforebygging i fokus, som resulterte i at jeg kontaktet nettpatruljen i Vest politidistrikt og NC3 i Kripos. Etter jeg sendte søknaden fikk jeg etter hvert en kontaktperson i hver avdeling. Vi snakket litt sammen om hva jeg ønsket å utforske og oppnå med oppgaven, før de anbefalte passende informanter.

Å bruke et mellomledd for å rekruttere informanter kan være problematisk. Ved at et mellomledd hadde ansvaret for å anbefale informanter mistet jeg noe kontroll over rekrutteringen (Skilbrei, 2019, s. 113). På forhånd snakket jeg og mine mellomledd om hva slags informanter jeg ville ha til mitt prosjekt, men man kan ikke alltid vite om de legger samme kriterier som meg i bunn av rekrutteringen. For å ha best mulig kontroll over utvelgelse av informanter er det hensiktsmessig at forskeren gjennomfører denne prosessen på egenhånd, slik at man i større grad kan unngå misforståelser og sikre at informantene man får er riktige for prosjektet. I min rekrutteringsprosess hadde jeg derimot ikke et annet valg enn å få informanter anbefalt gjennom et mellomledd, fordi jeg skulle intervjue ansatte i politiet. Det hadde vært vanskelig for meg å komme i kontakt med ansatte i politiet som jobber akkurat med digital forebygging på egenhånd, og de ansattes deltagelse i prosjektet må bli godkjent av deres arbeidsplass. Etter at jeg fikk anbefalt informanter fra mine mellomledd henvendte jeg meg direkte til personer jeg følte passet til mitt prosjekt. Slik sikret jeg at mellomleddet ikke fikk informasjon om selve utvelgelsen av informanter og deres samtykke til å delta i prosjektet. Jeg fikk også slik tatt tilbake litt av kontrollen for mitt eget prosjekt, ved at jeg selv fikk vurdere hvilke informanter som var passende. All informasjon om prosjektet utover den innledende søknaden gikk direkte fra meg til mine informanter.

I min rekrutteringsprosess møtte jeg på få utfordringer. Søknadene jeg sendte ut om deltagelse ble møtt med positive tilbakemeldinger fra de ulike avdelingene, og jeg fikk alle mine informanter på plass som et resultat fra disse søknadene. Jeg hadde sett for meg at denne prosessen skulle være mer utfordrende, at det var mange hindringer som kunne føre til at de

aktuelle avdelingene ikke ønsket å delta i prosjektet. Ved å si ja til å delta i mitt prosjekt ga de meg tillatelse til å bruke deres tid og ressurser, en tillitserklæring jeg setter stor pris på. Det å ønske å forske på politiet som kriminologistudent er i seg selv ikke særlig nyskapende, så den gode responsen jeg fikk kan tyde på at prosjektet mitt treffer et område innenfor politiet de ser et behov for å forske på. I 2017 ble virksomhetsrapporten «Politiet mot 2025» publisert, og denne fastslo at forebygging skulle være politiets primærstrategi i møte med kriminalitet (Politidirektoratet, 2017, s. 6). På samme måte som i resten av samfunnet blir også politiet påvirket av digitaliseringen, og digitale forebyggingsenheter som nettpatruljer er et relativt nytt fenomen innenfor politiet. Det økende fokuset på forebygging innenfor institusjonen og at satsningen på digitale forebyggingsarenaer har økt de siste årene kan være årsaken til hvorfor ønsket om å delta i mitt prosjekt var stor.

Jeg intervjuet 8 personer med ulike stillinger innenfor politiet. Gruppen av informanter består av en blanding av politi som arbeider lokalt med forebygging i Vest politidistrikt og politi som arbeider nasjonalt og internasjonalt med spisskompetanse innenfor spesifikke felt i Kripos og Interpol. De dekker store områder av politiets forebyggende arbeid, fra forebygging rettet mot lokal befolkning og lokale problemer til forebygging av nasjonale og internasjonale områder som datakriminalitet, ekstremisme og radikalisering, og overgrep mot barn. Informantene består av to kvinner og seks menn i aldersspennet 27 til 52 år. Som spennet i alder tilsier er det stor variasjon mellom informantene når det kommer til hvor lang erfaring de har innenfor politiet. Halvparten av informantene gikk ut av Politihøgskolen i løpet av de siste 5 årene, mens den andre halvparten har betydelig lengre erfaring fra institusjonen. Det er også skiller mellom informantenes erfaring med forebygging og datakriminalitet. Fire av informantene har tidligere jobbet på lensmannskontor, hvor forebygging er en av mange oppgaver. To informanter har jobbet spesifikt med forebygging over lengre tid, det vil si i flere stillinger enn den de er i nå, og tre har gjort det samme innenfor datakriminalitet.

4.3 Planlegging og gjennomføring

4.3.1 Intervjuguide

Et viktig ledd i planleggingen av et studie er å utforme gode spørsmål for å forsøke å få et så godt datamateriale som mulig (Skilbrei, 2019, s. 154). Jeg la mye vekt på å forsøke å utarbeide gode spørsmål i forkant av intervjuene. Ettersom intervjuene ble gjennomført ganske tidlig i prosjektet, var det vanskelig å forutse hvilken data jeg ønsker eller burde tilegne meg. Thagaard (2018, s. 95) skriver at det er viktig å utforme en intervjuguide som gir mulighet til å være

fleksibel overfor intervjupersonenes utsagn. Intervjuguiden besto derfor både av overordnende spørsmål og noen underspørsmål. Da jeg fikk prosjektet godkjent av NSD, ble jeg tipset om å legge ved intervjuguide før intervjuene for å sikre meg at informantene ikke opplyste meg om taushetsbelagt informasjon. Derfor opplyste jeg informantene da vi avtalte tidspunkt for intervju, om at jeg også ville sende dem litt nærmere informasjon om hva samtalen vår kom til å handle om på forhånd. Det negative med å sende intervjuguide på forhånd er at informantene kan føle seg tvunget til å bruke tid på forberedelser, eller at de forbereder seg så mye at samtalen ikke blir organisk. For å forsøke å unngå dette, men fremdeles være i samråd med tipset jeg fikk fra NSD, valgte jeg å ikke sende hele intervjuguiden men heller skrive et lite sammendrag av hva den bestod av. I tillegg sendte jeg denne informasjonen en eller to dager før intervjuene med hver informant. Jeg følte at dette ville oppleves mindre formelt enn å få tilsendt en lang liste med spørsmål, men at det samtidig ga informantene mine mulighet til å reflektere over temaene og hvilke opplysninger de kunne gi til meg knyttet til disse.

I gjennomførelsen av intervjuene var noen av informantene veldig ivrige og gikk i dybden om ulike aspekter av jobben, mens andre holdt seg litt kortere og konsist til spørsmålene jeg stilte. Å oppleve forskjell i intervjuenes erfaringsdeling og svar på spørsmål mener Kvale og Brinkmann (2017, s. 194) er vanlig å oppleve i intervjustudier. Ulikheter både i svar, men også i kompetanse og erfaring, førte til at intervjuguiden ble fulgt semi-strukturert, i noen intervjuer mer strukturert enn andre. Tematikken og spørsmål var bestemt i forkant, men jeg var samtidig åpen for variasjon i rekkefølgen og for at innspill fra informantene kunne endre den videre gangen i intervjuet. Ved å gjøre dette fulgte alle intervjuene den samme røde tråden, men jeg hadde også mulighet til å gå mer i dybden i enkelte temaer underveis. Dette er verdifullt, fordi informantenes svar kan lede opp til nye emner som en utenforstående ikke hadde kunnet forutsett. I tillegg opplevde jeg at noen av informantene svarte på flere spørsmål på en gang og jeg prøvde derfor å unngå å stille spørsmål jeg allerede hadde fått svar på. Etter hvert som jeg hadde intervjuer la jeg også til noen spørsmål, basert på hvilke oppfølgingsspørsmål jeg hadde stilt tidligere informanter. Allikevel forble intervjuguidens struktur og innhold nesten likt i alle intervjuene.

4.3.2 Digitale og fysiske intervjuer

På grunn av covid-19 ble de fleste intervjuene gjennomført digitalt. Digitale intervjuer kan både ha fordeler og ulemper. De kan påvirke forholdet mellom intervjuer og informant ved at det ikke oppnås en like god kontakt mellom dem (Skilbrei, 2019, s. 158). Intervjuer som foregår

gjennom en videotjeneste kan fremstå noe mer upersonlig og slik føre til at informanten ikke bygger samme tillit til intervjueren. Hvis en informant føler seg ukomfortabel med intervjusituasjonen, kan det påvirke hvor åpen hen er villig til å være og derav utgjøre et mindre godt datamateriale. Samtidig gir digitale intervjuer informantene mulighet til å gjennomføre intervjuene på et sted der de selv føler seg komfortable. Hvor et intervju foregår setter rammen for hvordan samtalen blir (Skilbrei, 2019, s. 130). Selv om selve intervjuet foregår over nett, får informantene mulighet til å selv skape seg en bekvem situasjon. Jeg håper derfor at det personlige aspektet intervjuene mister ved å ikke bli gjennomført ansikt til ansikt, kan intervjusituasjonen vinne på at intervjuet blir gjennomført i kjente omgivelser på hjemmekontoret til mine informanter

To av intervjuene ble gjennomført på arbeidsplassen til informantene. Disse intervjuene opplevde jeg at intervjuguiden ble fulgt mindre enn i de digitale intervjuene, fordi informantene var veldig engasjerte og snakket lenge uoppfordret. Jeg valgte å la de gjøre dette istedenfor å bryte inn, fordi jeg tenkte at det kunne være en ulempe å avbryte dem. De fikk snakket en del fritt først, før jeg stilte spørsmål om det jeg følte manglet knyttet til de spørsmålene jeg hadde tenkt å stille. At informantene i de fysiske intervjuene pratet mer fritt kan tyde på at disse kanskje ble opplevd som mindre formelle enn de digitale. Vi fikk en større mulighet til å småprate litt både før og etter de fysiske intervjuene som jeg tror kan ha fått informantene til å føle seg komfortable. Samtidig oppdaget jeg at omstendighetene rundt covid-19 hadde resultert i at alle jeg gjennomførte digitale intervjuer var vant med å ha samtaler over videotjeneste, ettersom de selv satt på hjemmekontor og ofte gjennomførte møter over nett. Samtlige informanter virket bekvemme med å bruke videotjeneste, og det opplever jeg som å ha spilt til min fordel. Jeg opplevde også lite tekniske problemer med intervjuene, som trolig også skyldes at både jeg og informantene hadde blitt såpass vant til digitale løsninger de siste månedene. Informantene mine hadde allerede brutt barrieren med å føre samtaler gjennom kamera og mikrofon, så de digitale intervjuene ble tilsynelatende så normalisert som mulig.

4.3.3 Opptak

Jeg gjennomførte 8 intervjuer med en varighet på mellom 40 minutter til en time. Jeg valgte å ta opp mine intervjuer. Selv om opptak av intervjuer fører til en stor jobb med transkribering, gir det også mye positivt til prosjektet. Alternativet til å ta opp intervjuene hadde vært å notere underveis. Dette hadde gjort meg som intervjuer mer utilgjengelig da fokuset hadde vært på å

få skrevet ned det som ble sagt istedenfor å føre en god samtale med mine informanter. Ved å ta opptak får man også med seg alle detaljene fra intervjuene. Selv om noe informanten sier på intervjutidspunktet ikke oppfattes som viktig av meg som intervjuer kan det vise seg å være spennende på et senere tidspunkt.

Jeg brukte båndopptaker for å ta opp intervjuene. Jeg valgte dette over UiO sin tjeneste der man kan ta opp intervjuer med telefonen for å prøve å sikre at kvaliteten på opptaket ble så god som overhodet mulig. Ettersom jeg gjennomførte flesteparten av intervjuene digitalt var dette ekstra viktig, for dårlig forbindelse eller mikrofon kan føre til at kvaliteten blir dårligere enn ved fysiske intervjuer. Å ta opp intervjuer med båndopptaker minner informanten om at samtalen blir tatt opp og dens tilstedeværelse kan gjøre informanten ubekvem (Weiss, 1994, s. 53). I de digitale intervjuene kunne ikke informantene mine se båndopptakeren, men de fikk informasjon om at det var det jeg brukte for å ta opp intervjuene. Intervjusituasjonen kan virke skremmende for noen, og jeg merket at noen av mine informanter virket litt nervøse før vi begynte intervjuet. Men jeg opplevde ikke at båndopptakerens tilstedeværelse skapte noen større barriere mellom meg og informanten, snarere tvert imot. Båndopptakeren ble faktisk et samtaleemne før flere av intervjuene og den ble møtt av en nysgjerrighet og fascinasjon fordi noen av informantene enten aldri hadde sett en båndopptaker eller ikke hadde sett en på mange år.

4.3.4 Forberedelser og min egen rolle som intervjuer

Det første intervjuet jeg gjennomførte i prosjektet var også det første intervjuet jeg har gjennomført selv, sett bort ifra i forbindelse med øvingsoppgaver i metodefag. Hvilken rolle jeg hadde i intervjuene var en viktig del av gjennomføringen, for som Kvale og Brinkmann (2017, s. 195) hevder er intervjueren et forskningsinstrument. Jeg syntes derfor det også er viktig å fortelle om og reflektere over min rolle i intervjuene. Før mitt første intervju gjennomførte jeg et pilotintervju sammen med en venn. I et pilotintervju kan man få testet ut ulike aspekter ved intervjusituasjonen; teknologien som videotjeneste og båndopptaker, intervjuguiden og hvordan man opptrer i rollen som intervjuer (Weiss, 1994, s. 52). Jeg opplevde pilotintervju som veldig hjelpsomt når det kom til å få testet ut videotjenesten og at jeg fikk testet ut å stille spørsmål og lytte til svarene. Jeg opplevde derimot ikke at det hjalp mye med å ferdigstille intervjuguiden. Dette er heller ikke så veldig rart, ettersom prosjektet mitt er rettet mot en spesifikk gruppe utdannede og arbeidstakere.

I forkant av intervjuene merket jeg at jeg var litt nervøs. Dette var fordi intervjusituasjonen var ny for meg, samtidig som jeg har veldig stor respekt for mine informanter og jobben de gjør.

Det faktum at jeg var litt nervøs tror jeg også kan ha virket positivt på intervjuene. Å bli intervjuet kan oppleves som litt skremmende, og noen av informantene var sikkert også litt usikre før intervjuet. Jeg tror derfor at det hjalp at jeg var litt spent, for da ble jeg nok ikke oppfattet som en streng og skummel forsker i deres øyne, noe som kan ha gjort dem mer komfortable. Jeg opplevde at forskerrollen min endret seg fra intervju til intervju når det kom til hvor involvert jeg måtte være i samtalen. I noen intervjuer holdt det med å stille de spørsmålene jeg hadde utarbeidet på forhånd, mens andre intervjuer ble mer som en samtale som jeg i større del var en del av. Dette krevde at jeg som forsker var erindrende, en egenskap Kvale og Brinkmann (2017, s. 196) påpeker er viktig for å kunne oppfatte, bevare og be om å få utdypet informantenes uttalelser. Dette utfordret meg som intervjuer og bidro til at jeg allerede i intervjudelen av prosjektet begynte å reflektere over datamaterialet sammen med mine informanter.

4.4 Databehandling

4.4.1 Transkribering

Transkriberingsprosessen tok lenger tid enn jeg hadde antatt. En årsak til dette var at det var veldig varierende kvalitet på opptakene. Kvale og Brinkmann (2017, s. 207) påpeker at lydopptak av dårlig kvalitet kan gjøre transkriberingen mer anstrengende. En bakside ved å gjennomføre digitale intervjuer er at det er en større fare for at selve opptaket blir av dårlig kvalitet slik at det var vanskelig å høre hva som ble sagt. Jeg måtte derfor bruke mye tid på å høre deler av noen intervjuer om igjen. Jeg tok i bruk transkriberingsprogrammet F4 da jeg transkriberte. Det viste seg å være veldig verdifullt da jeg skulle transkribere deler av intervjuer med dårlig kvalitet fordi jeg blant annet kunne senke farten på opptaket. Jeg fikk til slutt transkribert alle intervjuene tilnærmet så nærme de faktiske samtalene som mulig, selv om det var en tidskrevende prosess. Men jeg angrer ikke på at jeg valgte å ta opptak av intervjuene for å så transkribere dem, fordi transkriberingen ga meg en mulighet til å komme tett på materialet. Jeg gjorde meg flere notater underveis, blant annet hvilke koder og hvilke teorier jeg kunne knytte opp mot datamaterialet Slik ga transkriberingsprosessen meg et dypdykk inn i intervjuene og jeg begynte tankene om videre koding og analyse allerede da.

Tjora (2012, s. 144) påpeker at et valg man må ta når det kommer til transkribering, er om man skal beholde dialekter eller skrive på en «normalisert» måte. Lode (2006, i Tjora, 2012, s. 144) mener at en normalisering av språk kan fungere som en anonymisering. Jeg valgte å fjerne mine informanters dialekter underveis i transkriberingen, da de ulike dialektene kunne være

identifiserbare. En nedside ved å transkribere normalisert språk, er at spesielle dialektord kan ha en særegen betydning, og ved å fjerne disse kan man miste verdifullt materiale (Tjora, 2012, s. 144). Dette var jeg oppmerksom på underveis i min transkribering, og opplevde ikke at det normaliserte språket mistet mye mening. Videre valgte jeg å beholde muntlige preg i samtalen, for som Kvale og Birkmann (2017, s. 210) hevder kan fjerning av muntlig språk føre til at utsagnets tolkningsalternativer går tapt. Jeg valgte derimot å fjerne lyder som «ehm» og «øø», da jeg ikke opplevde at disse hadde en viktig relevans til utsagnene.

Det finnes ingen standardsvar på hvilke transkripsjoner man skal ta i bruk underveis i en transkribering, men det er viktig å fastsette noen standardvalg på forhånd (Kvale og Brinkmann, 2017, s. 208). Jeg brukte en enkel venstre- og høyreklamme for å angi punktet der en overlapping mellom meg og informanten begynner og slutter, som for eksempel: «[1: ja]». I tillegg brukte jeg en enkel venstre- og høyreparentes og tidsstempel for å angi at jeg ikke hørte hva som ble sagt, eksempelvis: «(#01:26-6)». Jeg brukte doble parenteser for å skrive egne kommentarer, for eksempel i tilfeller hvor informantene brukte ord som «det» eller «de» om noe eller noen for å gi setningen kontekst, eksempelvis: «((TikTok))». Transkripsjon av en intervjusamtale til en skriftlig form medfører at man mister flere kontekstuelle trekk ved intervjuet (Kvale og Brinkmann, 2017, s. 205). Det vil være vanskelig å gjengi toneleie, ironi og andre muntlige preg som kan bidra til å gjengi intervjuet. Med dette i bakhodet valgte jeg å markere når det forekom latter i intervjuene med: «(h)». Latter er en indikator det er mulig å gjengi fra et lydopptak, og ved å transkribere inn dette fikk jeg dokumentert deler av humøret og stemningen i intervjuene.

4.4.2 Analytisk tilnærming

Jeg var interesserte i å få en forståelse av hvordan politiet driver digitalt forebyggende politiarbeid. Analysens hensikt var ikke å analysere selve innlegget politiet legger ut på sosiale medier, men å undersøke hvilken opplevelse informantene har av metodene og praksisene de tar i bruk i det digitale forebyggende arbeidet. For å gjøre dette har jeg benyttet meg av en induktiv forskningsstrategi, en analytisk metode som blir drevet av empiri (Tjora, 2012, s. 223). Data fra intervjuene har vært avgjørende for hvilke teorier, litteratur og temaer som har rammet den videre oppgaven. Ved å ta i bruk en induktiv tilnærming har jeg kunnet systematisk hente inn litteratur som kan belyse de viktigste temaene og funnene jeg oppdaget i empirien. Samtidig som oppgaven min bærer preg av en induktiv tilnærming, har jeg også tatt i bruk en deduktiv strategi som analytisk fremgangsmåte. Deduktiv forskning blir drevet av teori, og kan gjenkjennes blant annet av at begrepene som blir knyttet til forskningsdataene er avledet fra en

teori (Thagaard, 2018, s. 172). Begrepene jeg har knyttet til intervjudataene har bakgrunn i teoretiske perspektiver om forebygging og datakriminalitet, og derfor er min analytiske tilnærming både induktiv og deduktiv. Et slags skjæringspunkt mellom en induktiv og en deduktiv tilnærming kalles for abduksjon. I en abduktiv tilnærming bidrar analysen til videreutvikling av teoretiske perspektiver, samtidig som teorier kan utvikle vår forståelse av empirien (Thagaard, 2018, s. 184). Mason (2018, s. 228) beskriver den abduktive strategien for en kontinuerlig prosess, hvor overganger mellom analyse av dataene, inspirasjon fra teoretiske rammeverk og utviklingen av nye perspektiver bidrar til å styrke analysen. Dette er beskrivende for min analysestrategi i denne studien, teoretiske perspektiver utvikler min empiri samtidig som datamaterialet bidrar til sammensetningen av teoretiske retninger jeg anvender for å svare på problemstillingen.

4.4.4 Analyseprosessen

Første ledd i behandlingen av datamaterialet var for meg å sette i gang med å kode intervjuene. Formålet med å kode datamateriale er å knytte datamaterialet opp mot ulike kategorier eller begrep som vil være relevante for å kunne svare på problemstillingen (Weiss, 1994, s. 154). Utfordringen er å utvikle koder presise nok for at det skal være mulig å foreta en god analyse, men samtidig brede nok for at de samme skal kunne anvendes for flere deler av datamaterialet. Koding er en slags systematisering av datamaterialet som viser hvilke mønstre som går igjen (Skilbrei, 2019, s. 183). Jeg var usikker på hvordan jeg skulle gå frem for å kode datamaterialet, fordi jeg følte et slags press på at det måtte være perfekt for å gi meg nytte videre i oppgaven. Underveis i transkriberingen noterte jeg ned overordnende temaer jeg oppdaget gikk igjen i flere intervjuer, men slet med å anvende de i kodingsprosessen. Problemet var at disse temaene var for brede og generelle, noe som Skilbrei (2019, s. 186) hevder er et vanlig problem i kodingsprosessen. Dette løste seg for meg da jeg begynte å tenke på kodene som knagger. Kodene til datamaterialet er rett og slett knagger hvor du får kategorisert og hengt opp de ulike delene av dataene for hjelp til videre fortolkning av materialet. De store temaene jeg skrev ned underveis i transkriberingen ble stort sett kategorier, eller knaggrekker, og mindre underkategorier er enkelte knagger på disse rekkene. Eksempelvis var koden «effektivitet» en knaggrekke, med «samarbeid» og «rekkevidde» som underordnede knagger.

Da jeg videre skulle bestemme meg for hvordan jeg skulle analysere datamaterialet hadde jeg flere muligheter. Et av alternativene som ble vurdert var meningsfortetting, hvor man forkorter setningene informantene har sagt til å kun inneholde den faktiske meningen (Kvale og Brinkmann, 2017, s. 232). Essensen av dette er egentlig å komme frem til større temaer som

kan tolkes videre. Dette var interessant for oppgaven min, blant annet fordi jeg avdekket større temaer i kodingen som virket hensiktsmessig å utforske videre. Likevel valgte jeg en noe lignende analysemetode, nemlig temaanalyse. Dette valget ble tatt fordi jeg ønsket å gå i dybden på noen temaer og se på de i lys av hver av informantenes egne vurderinger og refleksjoner. Jeg fant at denne analysemetoden resonnerte godt med fremgangsmåten jeg valgte for kodingen av datamaterialet, samtidig som det gir meg som forsker noe fleksibilitet i analysearbeidet. Målet mitt med å velge denne analysemetoden var både å kunne gruppere dataen ut i fra viktige fellestrekk og finne noen konkrete «svar» i de generelle temaene jeg avdekket (Johannessen, Rafoss og Rasmussen, 2020, s. 279).

Det kan oppstå utfordringer med tematisk analyse, fordi det kan være vanskelig å «vurdere temaene løsrevet fra den konteksten utsnittene av data opprinnelig ble presentert i» (Thagaard, 2018, s. 172). Altså kan en sammenligning av to utsnitt fra forskjellige informanter være tatt ut av kontekst og egentlig ikke bli en korrekt sammenligning. Som i mye kvalitativ forskning kan det altså være vanskelig å sikre at den riktige konteksten figurerer i analysen, men det finnes metoder for å sikre mer reliable analyser. Man må vurdere enkelte utsagn fra informantene opp mot intervjuet som en helhet, og analysere sammenhengen mellom temaene for å få en helhetlig forståelse (Thagaard, 2018, s. 172). Dette stiller noen krav til at informasjonen vi har fått samlet inn fra informantene har gode beskrivelser, og det vurderer jeg at mitt datagrunnlag har.

4.5 Datakvalitet

Det er viktig å kvalitetssikre datamaterialet i enhver forskingsprosess. Informasjon er avhengig av kontekst, all informasjonen jeg tilegner meg vil bli formet av intervjusituasjonen (Weiss, 1994, s. 149). På forhånd og underveis i prosessen har jeg forsøkt å sikre kvaliteten ved å for eksempel bruke tid og teori for å utvikle intervjuguiden, være åpen og tydelig med mine informanter og være klar over rollen jeg har som forsker. Det finnes også kriterier for å undersøke kvaliteten i datamaterialet etter at det er samlet inn. Reliabilitet måler påliteligheten til materialet, er det en logisk sammenheng mellom det man ønsker å finne svar på og prosjektets utforming og funn? Tjora (2012, s. 204) hevder at mye kunnskap om temaet er en fordel for å stille presise spørsmål, men det kan også være en ulempe fordi man har med seg mange forutinntattheter. Forskerens forforståelse og kunnskap kan påvirke oppgavens pålitelighet. Det jeg tolker og oppfatter, som mangeårig kriminologistudent, kan være forskjellig fra hva noen med en annen akademisk bakgrunn oppfatter.

Validitet er et annet kriterium relevant for dette prosjektet. Validitet måler om materialet man har tilegnet seg kan svare på målsettingen for forskningen (Tjora, 2012, s. 206). Kvale (2007, s. 123) kaller validitet for kvaliteten av håndverk; det er kvaliteten av forskerens undersøkelser, evne til å stille spørsmål ved og teoretisk tolke materialet som er samlet inn. Validitet kan deles opp i to; intern og ekstern. Den interne validiteten omhandler forskerens troverdighet, om konklusjonene som trekkes er støttet av datamaterialet (Skilbrei, 2019, s. 88). Måler jeg det jeg ønsker å måle? En måte å sikre den interne validiteten er å revurdere og utvikle spørsmålene og temaene man tar opp i intervjuene underveis. Jeg gjennomførte alle intervjuene på to uker, og jeg hadde derfor ikke muligheten til å transkribere underveis. Jeg hadde hatt en større mulighet til å validere materialet hvis jeg kunne transkribert mye underveis i intervjuprosessen, for da hadde jeg hatt mulighet til å nøye kartlagt, vurdert og forbedret intervjuene mine. Jeg var derimot oppmerksom på å markere hvilke spørsmål som kunne skape misforståelse underveis, slik at jeg kunne ordlegge meg tydeligere i de følgende intervjuene. Slik fikk jeg til dels styrket den interne valideten underveis, ved å endre på det jeg umiddelbart opplevde som uklart for informantene mine.

Den eksterne validiteten omfatter prosjektets overførbarhet, om resultatene i studien og kunnskapen derfra også er gyldig sammenlignet med andre fenomener (Skilbrei, 2019, s. 88). Mitt mål har vært å samle inn informasjon om arbeid som kategoriseres som digitalt forebyggende politiarbeid for å svare på mitt forskningsspørsmål. Informantene jeg har intervjuet er kvalifiserte til å gi innsiktsrik og god informasjon til prosjektet, men de kan ikke fungere som representanter for hele fagfeltet. Som tidligere nevnt er ikke hensikten med oppgaven å forklare, men å få forståelse for forebyggingsarbeidet gjort på digitale plattformer og av digitale kriminalitetstyper. Dette undersøkes gjennom aktørenes øyne; hvilket formål har arbeidet de gjør, hvilke tanker ligger bak de forebyggende tiltak og hvordan suksessen av dette arbeidet blir opplevd av de som jobber tettest med det. Med dette fokuset tar jeg med oppgaven høyde for å skape en konseptuell generalisering framfor en generell generalisering. Med konseptuell generalisering menes det at anvendelsen av teorier og konsepter kan vise seg å være relevant for beslektede tilfeller enn akkurat det undersøkt i denne oppgaven (Tjora, 2012, s. 215). Dette kan være spesielt aktuelt fordi oppgaven undersøker et nytt fenomen, et spesifikt område det er forsket lite på tidligere i norsk sammenheng. Det vil nok ikke være mulig å overføre funnene i dette prosjektet til beslektede fenomener, men disse funnene kan dermed bidra til videre forskning på dette feltet, uten at selve resultatene overføres.

4.6 Etiske refleksjoner

På forhånd av intervjudeltagelsen, ble intervjudeltagerne informert om undersøkelsens formål og hovedtrekkene i studiens design, et såkalt informert samtykke (Kvale og Brinkmann 2017, s. 104). Et samtykke kan gjøres både skriftlig og muntlig, men er bare gyldig hvis det kan dokumenteres (NSD, 2021). Jeg mottok skriftlig samtykke i form av underskrift på en samtykkeerklæring fra de informantene jeg gjennomførte fysisk intervju med. I de digitale intervjuene fikk jeg muntlig samtykke fra hver informant, dokumentert i lydopptaket jeg tok av intervjuet. Det muntlige samtykket foregikk ved at jeg først leste opp samtykkeerklæringen og deretter spurte om informantene samtykket. Så mottok jeg et svar fra mine informanter, og følgende oppga de sitt fulle navn. Lydopptakene og samtykkeerklæringene med underskrift ble oppbevart i et låst skap på det juridiske fakultet, et område kontrollert med adgangskort. Lydfilene ble videre lagret på Universitetet i Oslo sitt hjemområde via min private pc. Etter prosjektets slutt vil lydopptakene slettes, og de skriftlige samtykkeerklæringene makuleres.

4.6.1 Anonymisering

Nettpatruljen representerer en helt ny form for politi, et politi som gir av seg selv og er tilgjengelige på nett. Følgertall og innhold fra den spesifikke avdelingen er viktige aspekter ved deres arbeid, og derav også viktige momenter for empirien. Dette reiser en problemstilling for oppgavens etiske hensyn, hvordan kan jeg analysere det digitalt forebyggende politiarbeidet men fremdeles beholde deres anonymitet? Konfidensialitet innebærer blant annet at dataene anonymiseres, som kan gjøres ved å bruke fiktive navn eller endre personenes kjennetegn (Kvale og Brinkmann, 2017, s. 106+300). Som tidligere nevnt har jeg valgt å anonymisere dialekter og talemåter som kan bidra til å identifisere hvem sitatet tilhører. I tillegg er alle navn brukt i oppgaven er anonymisert. Jeg har også valgt å ta et noe utradisjonelt valg ved å kun kalle opp informantene mine for mannlige anonymiserte navn, til tross for at datamaterialet består av begge kjønn. Dette er et ekstra grep jeg har tatt for å ytterligere sikre mine informanters anonymitet, og forsikre meg om at sitat ikke kan knyttes tilbake til den enkelte informant. Kvale og Brinkmann (2017, s. 300) hevder at det er viktig å ikke endre informasjon om informantene som også endrer betydningen for datamaterialet. Jeg vurderer det derimot slik at hvilket kjønn de ulike sitatene tilhører ikke er avgjørende for forståelsen av empirien. Informasjonen om informantene som jeg vurderer kan være avgjørende for forståelsen av empirien er om informantene er ansatt i nettpatruljen eller Kripos. Derfor har jeg valgt å legge til /K etter navnet til informantene som tilhører Kripos, og /N for de ansatte som hører til nettpatruljen.

5. Forebygging på nett

Dette kapittelet er den første delen av oppgavens analyse, og vil ta for seg de forebyggende praksisene informantene presenterer. Kapittelet vil først begynne med å presentere nettpatruljen og analysere de forebyggende praksisene med bakgrunn i teorikapittelet. Følgende vil også de forebyggende praksisene i Kripos bli presentert i lys av oppgavens teoretiske rammeverk. Til slutt vil kapittelet ta for seg informantenes skildringer av internett som en krimogen arena. Hensikten er å undersøke hvordan nettpatruljen og Kripos driver digitalt forebyggende politiarbeid, samt hvordan de forsøker å gjøre krav på internett og hvilke utfordringer de møter på som er særegne for de virtuelle omgivelsene.

5.1 Arbeid med internett

Hvordan jobber de ansatte i nettpatruljen og Kripos for å gjøre krav på internett? For å undersøke dette, vil jeg dele opp den videre analysen i to. Jeg vil først ta for meg hvordan nettpatruljen jobber for å kreve sin plass på internett, deretter vil jeg gjøre det samme med Kripos. Det er to forskjellige deler av politiorganisasjonen, som representerer to ulike ender av skalaen over arbeid med internett. Mens Kripos jobber med saker både nasjonalt og internasjonalt, er nettpatruljen et lokalt tilbud for Vest politidistrikt. De ulike tilnærmingene viser det store geografiske mangfoldet man møter på ved datakriminalitet, avstanden mellom offer og lovbryter kan være alt fra en pult i klasserommet til landegrenser. Kripos tar for seg mer alvorlig og fagfeltrettet data-aktivert og data-avhengig kriminalitet, mens i nettpatruljen står de mer hverdagslige utfordringene med kriminalitet og sikkerhet på nett mest i fokus. Dette viser hvor komplekst kriminalitet som skjer ved bruk av nett er, det kan være alt fra store dataangrep, massedistribuering av overgrepsmateriale og radikalisering til ekstreme miljøer, til svindel-e-poster, falske profiler og uønsket bildedeling. Hensikten med den videre diskusjonen er å identifisere hvilke kriminalitetsforebyggende tanker som ligger bak forebyggende tiltak i det digitale rom, basert på informantenes beskrivelser av tiltak og formål.

5.1.1 Nettpatruljen

Politiets nettpatruljer er en del av politiets satsing på å være til stede på nett. Formålet med tjenestene er å veilede om trygg og god nettbruk, og være et synlig politi som er tilgjengelig på internett (Politiet, 2020). Allerede i 2015 ble politiets første nettpatrulje etablert, i regi av Kripos. I dag har politiet til sammen 12 nettpatruljer – et for hvert politidistrikt. Nettpatruljen Vest ble opprettet i 2019, og skal fungere som et lokaltilbud for befolkningen der i Vest

politidistrikt. Nettpatruljen er tilstede på i hovedsak tre sosiale plattformer hvor de har opparbeidet seg en betydelig følgerskare. I august 2021 har nettpatruljen Vest rundt 10 000 følgere på Instagram, omtrent 15 000 følgere på Facebook og rett i underkant av svimlende 460 000 følgere på TikTok. Deres tilstedeværelse på internett deles altså med nesten en halv million nettprofiler.

Nettpatruljen hadde på tidspunktet intervjuene ble gjennomført 5 ansatte, og i etterkant av datainnsamlingen har dette antallet økt. Sindre/N forklarer at:

> *«Vi jobber jo på distriktsnivå, det vil si at vi dekker hele Vest politidistrikt og prøver da å, altså når vi jobber prøver vi å nå flest mulig i distriktet.»*

Arbeidet de driver med er altså områdebasert, de forsøker å være et tilbud for innbyggerne i Vest. Sindre/N beskriver videre arbeidet de driver med slik: *«Vi har på en måte to hovedoppgaver, det er kommunikasjon inn og informasjon ut»*. Kommunikasjon inn består av henvendelser fra publikum på diverse sosiale medier. Som nevnt er nettpatruljen til stede på flere sosiale medier; TikTok, Instagram, Facebook, og til tider Snapchat. De har en åpen toveis kommunikasjon med publikum på to av disse plattformene. Det vil si at publikum kan ta kontakt med politiet ved å sende en melding, og vil følgende få svar på denne fra en av de ansatte i nettpatruljen. Erik/N forklarer arbeidet med kommunikasjon inn som at:

> *«Det består veldig masse av, først og fremst å svare på spørsmål, ta imot tips og tilbakemelding fra innbyggerne, og følge opp det som kommer der.»*.

Stein/N forteller at: *«Vi har garantert at alle sammen skal få svar når de sender meldinger til oss, alle skal få svar uansett hva de skriver og spør om.»*. Arbeidet med å behandle kommunikasjonen som kommer inn er derfor et omfattende arbeid, alle skal få et skikkelig svar, uavhengig av hva de sender inn. Richard/N forklarer arbeidet med å håndtere meldingene inn slik:

> *«Så da er det jo å logge seg på, se på hvilke meldinger som har kommet inn siden sist arbeidsdag, prioritere deretter, er det noe som kan tas umiddelbart eller kan vi ta nederst til øverst.»*.

Selv om alle skal få svar, gjør de altså alltid en vurdering på om noen meldinger haster mer med svar enn andre.

Erik/N opplyser at oppgaven de har knyttet til kommunikasjon inn, henger tett sammen med oppgaven om å få informasjon ut: *«Det danner jo mye utgangspunktet for ulike tiltak og ting vi*

gjør da, hvis man får et tips for eksempel så må man ofte gjøre noen tiltak ut fra det». Behovene og spørsmålene som kommer inn fra publikum er altså med på å fastsette hvilken informasjon innbyggerne i distriktet har nytte av. Å skape trygghet og forebygge kriminalitet gjennom å styrke samarbeidet mellom publikum og politi er et viktig trekk innenfor lokalorientert politiarbeid (Lie, 2011, s. 183). Å legge publikums behov og observasjoner av lokalsamfunnet til grunn for forebyggende tiltak er altså en del av nettpatruljens trygghetsskapende arbeid. Det er ikke bare det befolkningen kommuniserer direkte til nettpatruljen som legger grunnlaget for informasjonsarbeidet. Theodor/N forteller at *«det kan være nasjonale føringer»* som fastsetter noen temaer nettpatruljen skal gå ut med informasjon om. Nettpatruljen samarbeider også med andre seksjoner i politidistriktet, som seksjon for etterforskning, og tredjeparter, som barnevernet, for å kartlegge hva som rører på seg. Stein/N forteller prosessen slik:

> *«For eksempel, hvis vi ser at det er mange meldinger om GPS tyveri, bilratt, og vi ser at det er et fenomen som beveger seg på en måte i hele Vest politidistrikt, så skal jeg prøve å fange opp den informasjonen og ta den videre med meg da til nettpatruljen og se om vi kan bruke den informasjonen til å formidle et budskap til publikum sånn at de kan sette i verk tiltak selv for å, ja avverge eller hindre at de blir utsatt for kriminalitet.»*

Formålet med å komme ut med informasjon er, som Stein/N sier, er å gi publikum informasjon de kan bruke til å beskytte seg selv. Nettpatruljen legger mye vekt på å opplyse om ulike problemer, og Erik/N oppfatter faktisk akkurat den delen som den mest essensielle rollen til nettpatruljen:

> *«Den viktigste oppgaven vil jeg jo si er å få informasjon ut, altså hjelp til selvhjelp, økt kunnskap til folk gir jo dem et bedre grunnlag for å beskytte seg selv.»*

Nettpatruljen har flere sosiale medier-plattformer de kan ta i bruk for å komme i kontakt med befolkningen. Hvilke digitale plattformer nettpatruljen velger å bruke for å komme ut med spesifikk informasjon er ikke tilfeldig. Stein/N forteller:

> *«Det er jo alt etter hvilken målgruppe vi ønsker å nå. Facebook er de eldste, Instagram er unge voksne og voksne, og TikTok er mest, eller først og fremst barn.»*

Også innholdet de går ut med, og måten informasjonen blir formatert er tilrettelagt for de ulike målgruppene. Erik/N forteller:

> *«Skal vi nå rett ut til barn og unge, så bruker vi for eksempel TikTok og vi snakker et eget språk der. Vi jobber på en helt annen måte, der lager vi ikke et innlegg med tekst*

og sånt nødvendigvis, der lager vi videoer som er interaktive og som vi mener treffer målgruppen. (...) Får vi spørsmål fra en voksen om et tema så vil jo tilnærmingen være på en viss måte, og får vi spørsmål fra et barn så vil vi kanskje snakke mer som et barn gjør da om det temaet, og bruke andre begreper da.»

5.1.1.1 Profiler på sosiale medier

Arbeidet nettpatruljen driver med å være tilstede og tilgjengelig for publikum på nett, er i seg selv et forebyggende tiltak. Richard/N reflekterer rundt hva denne muligheten gir:

«For det i seg selv skaper trygghet og tillit, bare det å vite at politiet er der når du trenger de. Om det er lite eller stort så er de der.».

Tanker om et politi som skal være til stede, ha åpen kommunikasjon med befolkningen og et fokus på å skape tillit kan trekkes opp mot strategier om lokalorientert forebygging. En strategi innenfor denne tankegangen er lokalorientert politiarbeid, som karakteriseres blant annet av et fokus på sivilt engasjement (Gundhus, 2014, s. 187). Nettpatruljen opplever sivilt engasjement ved å være tilgjengelig for befolkningen og gi publikum en mulighet til å involvere seg ved å alltid ha åpne to-veis kommunikasjonskanaler. Etableringen av sosiale medie-profiler for politiet har gitt publikum en større mulighet til å kontakte dem om mer enn nødsituasjoner og lovbrudd som allerede har funnet sted. Dette kan bidra til å bryte barrierer mellom politi og publikum. Richard/N forklarer kommunikasjonen med publikum, og spesielt unge slik:

«Og så tenker jeg når vi snakker om et barn om en konkret ting så er det også viktig for oss at de får en god opplevelse når de snakker med politiet, for det er kanskje første gangen deres. Kanskje de syntes det var litt skummelt, men samtidig - sosiale medier gjør det mer tilgjengelig, det er et lavterskeltilbud. Man kan sitte hjemme under dyna og sende en melding til politiet plutselig, det føles tryggere det enn å skulle møte dem på gata eller ringe. Så vi er opptatt av at de skal få en god opplevelse av det, og det i seg selv kan være forebyggende tenker vi da. Det skaper trygghet og tillit.»

Nettpatruljen representerer en ny form for tilgjengelighet, og kan bli kontaktet uansett hvor publikum befinner seg. Politiets tilgjengelighet blir slik løftet til et helt nytt nivå. Samtidig vil det at politiet kan komme i kontakt med publikum også når det ikke har skjedd noe spesielt på forhånd være viktig for tillitsbygningen (Lie, 2011, s. 191). Den åpne to-veis kommunikasjonen på sosiale medier gjør slik politi og publikum mer tilgjengelig for hverandre, et verktøy som kan spille en viktig rolle i tillitsbygningen.

Å oppnå tillit i befolkningen er noe nettpatruljen har et fokus på, og Theodor/N sier at: *«Tillitsbyggingen føler jeg at vi jobber med hver eneste dag, ved at vi svarer ordentlig og gir råd som publikum føler er nyttig.»*. De ansatte i nettpatruljen ser at det trygghetsskapende arbeidet gir resultater. Sindre/N forklarer at: «*Vi har jo hatt økende antall henvendelser nesten hver måned siden vi begynte. Så vi føler at tilliten øker ved at vi er til stede på nett*.». Å arbeide for å skape trygghet og oppnå befolkningens tillit, kan trekkes til tanken om beroligende politiarbeid. Strategien har sprunget ut av den lokalorienterte tankegangen, og her er det publikums trygghetsfølelse og tillit til politiet som står i fokus (Gundhus, 2014, s. 191). Ved å være i tett kontakt med befolkningen får informasjon om hva som rører seg i miljøet, og særlig den uformelle kontakten skaper trygghet mellom publikum og politi (Lie, 2011, s. 193). Slik får også politiet vite hva som er signal-kriminaliteten i samfunnet, hvilke kriminelle handlinger lokalmiljøet opplever som mest truende. Om datakriminalitet for eksempel, forteller Richard/N at:

> *«Samtidig har det vært lav tillit på digital kriminalitet, men det blir bedre og bedre med nettpatruljen tilstede. Da ser de at vi er jo her, vi driver med det og vi følger med rett og slett da. Det er min opplevelse av det i hvert fall.»*

Selv om nettpatruljens arbeid ser ut til å være forankret i tradisjonelle tilnærminger til kriminalitetsforebygging som lokalorientert og beroligende politiarbeid, skiller det seg ut på et punkt – fysisk tilstedeværelse i lokalmiljøet. Man kan spørre om lokalorientert politiarbeid i det hele tatt kan fungere i det virtuelle rom. Bakgrunnen for retningen lokalorientert forebygging er nettopp det at politiet skal være til stede i lokalmiljøet og jobbe for samhandling mellom politiet og lokalsamfunnet. At politiet flyttes fra gata og til data fører til at den fysiske avstanden mellom politi og publikum blir større. Men verden er ikke den samme i dag som den var på 1980-tallet da lokalorienterte strategier fikk sitt oppsving (Kelling og Wilson, 1982; Goldstein, 1979). Sosial handling er i det moderne samfunn løsrevet fra fysisk nærhet, og mye av denne foregår på akkurat de samme sosiale medieplattformene som nettpatruljen befinner seg på. Politiet er ikke i like stor grad plassert fysisk i hvert eneste lokalmiljø som de var før, men gjennom nettpatruljen kan politiets tilstedeværelse og budskap nå ut til publikum hvor som helst og når som helst. Sindre/N forteller: *«Jeg føler det er stort sett veldig positivt, at folk er fornøyde med at politiet har kommet litt nærmere, man har dem liksom i hånda.»*. Nettpatruljen befinner seg i et ikke-fysisk miljø, men samtidig har de en klar geografisk identitet. Som tidligere vist baserer nettpatruljen Vest seg på hvilke utfordringer som er synlige i Vest politidistrikt, og jobber for å forbedre kriminalitetsbildet innenfor dette området. Samtidig når den forebyggende

tilstedeværelsen på nett langt utenfor deres geografiske identitet. Representerer nettpatruljen ikke bare en ny måte å drive politiarbeid på, men også et nytt lokalmiljø som ikke har de samme geografiske begrensinger som før?

5.1.1.2 Informasjon om lovbrudd og konsekvenser

En stor del av nettpatruljens arbeid går ut på å få ut informasjon. Ved å gi informasjon om lovbrudd, hva man skal gjøre hvis man blir utsatt for det og hvilke konsekvenser det vil ha, jobber nettpatruljen forebyggende gjennom å gjøre publikum mer bevisste. Erik/N forteller om en video de la ut på TikTok:

> *«Jeg kan for så vidt bruke et eksempel fra TikTok der vi lagde en video om "nudes" og "dickpics", uønsket bildedeling mot barn og unge, som det etter lovverket ikke er lov å sende til personer under 16 år, eller til personer som ikke har samtykket til det. Da lagde vi en TikTok der vi beskrev lovverket som sier at det ikke er lov til å sende nudes eller dickpics til andre. Og hvis du opplever det, så gjør det her.»*

For å kunne gå ut med et effektivt forebyggende budskap, er det viktig at den forebyggende aktøren forstår seg på målgruppen de ønsker å nå (Brewer m.fl., 2019, s. 42). Som tidligere forklart, forsøker nettpatruljen å tilpasse seg blant annet ved bruk av sosiale medier etter hvilken målgruppe de vil nå. Budskapet Erik/N forteller om er rettet mot barn under 16 som kan bli utsatt for å motta uønskede bilder, men gir også informasjon om hvorfor det er et lovbrudd og konsekvensene det å sende uønskede bilder kan få. Nettpatruljen har derfor valgt å bruke plattformen TikTok. I tillegg inneholder ikke videoen eller teksten under videoen vanskelige begreper, slik at den lett kan forstås av barn og ungdom.

Arbeidet med å gå ut med informasjon oppleves å ha en positiv virkning på befolkningen av samtlige ansatte i nettpatruljen. Stein/N forteller:

> *«Det vi veldig ofte ser når vi går ut med noe, er at det resulterer i mer meldinger inn på det temaet. Så det avdekker jo også mer mørketall ved at vi går ut med informasjon.»*

Det fremkommer fra Stein/Vest sitt utsagn at ved å gå ut med informasjon om lovbrudd, kan de også få avdekket flere straffbare handlinger. Det er flere ledd i prosessen fra en kriminell handling begås til straff blir ilagt som gjør at lovbrudd faller utenfor kriminalstatistikken. For det første må et lovbrudd oppdages, og for at dette skal skje må blant annet den som ble utsatt

for lovbruddet kunne definere handlingen som straffbar (Lomell, 2017, s. 34). Mange mørketall kan altså oppstå av uvitenhet, at offeret for et lovbrudd ikke var klar over at det hen ble utsatt for var kriminalitet. Etter identifiseringen av lovbruddet må det således anmeldes til politiet. Ikke alle som er klar over at de er utsatt for et straffbare forhold velger å faktisk anmelde det, og årsakene til dette kan være mange. Eksempelvis kan offerets tvil om hvordan politi og domstol vil kunne håndtere lovbruddet og kriminalitetens alvorlighetsgrad spille inn på valget om å anmelde (Lomell, 2017, s. 34-35). Ved å gå ut med informasjon om et tema, åpner politiet også for å innlede en trygg samtale om det. Det kan spille positivt inn på anmeldelsestilbøyeligheten og fjerne barrierer som hindrer ofre i å anmelde kriminaliteten. I Riksrevisjonens vurdering av politiets innsats mot datakriminalitet, slår de fast at kunnskapen om forekomsten av IKT-kriminalitet er svak ettersom tilbøyeligheten for å anmelde lovbrudd er lavere for IKT-kriminalitet enn tradisjonell kriminalitet (Riksrevisjonen, 2021, s. 95). Man kan anta at å dele informasjon om akkurat datakriminalitet vil derfor kunne ha størst effekt på avdekking av nettopp denne typen lovbrudd.

Grunnleggende beskyttelse for tradisjonell kriminalitet er i stor grad en integrert del av våre liv, de fleste trenger ingen påminnelse om å låse ytterdøren og passe på sine verdisaker. Datakriminalitet er derimot et nyere fenomen og følgelig er tiltak for beskyttelse i større grad ukjent og uvant, og de ulike datalovbruddene man kan bli utsatt for er ikke like kjente som tradisjonell kriminalitet (Renaud, Orgeron, Warkentin og French, 2020, s. 585). Det samme gjelder for det å begå datakriminalitet, hvilke handlinger som er lovbrudd og hvilke konsekvenser som medfølger er muligens mindre kjent for datakriminalitet. Bevisstgjøring har vist seg å være effektivt innenfor forebygging av diverse tradisjonell kriminalitet, det har blant annet vært et stort fokus innenfor forebygging av voldtekt (Justis- og beredskapsdepartementet, 2019, s. 7). De fleste barn lærer gjennom oppveksten at det ikke er lov å stjele, men blir de lært at det ikke er lov å skrive hatkommentarer, sende uoppfordrede nakenbilder og å bryte seg inn i andres datamaskiner? Ifølge Renaud m.fl. (2020, s. 585) burde myndighetene ta på seg et større ansvar for å informere innbyggerne sine om datakriminalitet og hvordan beskytte seg mot det, fordi det enda ikke er en like inkorporert del av livene våre. Ved å gå ut med informasjon om ulike lovbrudd på sosiale medier, bidrar nettpatruljen til å gjøre befolkningen mer opplyste om datakriminalitet og hvordan de skal reagere hvis de blir utsatt for det.

Å gå ut med informasjon kan være et viktig tiltak for å forebygge og avdekke datakriminalitet, men informantene opplyser at politiet må samtidig være varsom med hvilken informasjon de

går ut med. Stein/N forteller om hvorfor det er noe politiet ikke informerer om: *«For vi er redd for at det skal skje en smitteeffekt eller at barn og unge blir så nysgjerrig på hva det er».* Å gå ut med informasjon om lovbrudd kan ha en uønsket effekt ved at det istedenfor å avskrekke potensielle lovbrytere, kan pirre nysgjerrigheten til flere (Brewer m.fl., 2019, s. 43). Stadig informasjon om måter å begå kriminalitet på nett, selv om det kommer i et advarende format fra politiet, kan skape en nysgjerrighet og være vanskelig å motstå. Det er en utfordrende vurdering å ta, hvilken informasjon kan gjøre mer skade enn nytte?

5.1.1.3 Hjelp til selvhjelp

Nettpatruljen har et stort fokus på hvordan publikum kan gjøre seg selv mindre sårbare på nett, og Sindre/N sier: «*Den viktigste oppgaven vil jeg jo si er å få informasjon ut, altså hjelp til selvhjelp, økt kunnskap til folk gir jo dem et bedre grunnlag for å beskytte seg selv*.». Han forteller videre:

> *«Vi fokuserer mye på det (forebyggende tiltak), folk tar kontakt og sier at de er utsatt for ting og det er jo typisk nettkriminalitet. Det var en typisk svindel-mail i en periode, vi fikk masse meldinger inn at de hadde mottatt det. Spesielt nå i korona er jo det veldig utbredt. Og da gikk vi ut med informasjon for å advare folk mot at det skjer og hva man bør gjøre.»*

Nettpatruljen går altså ut med informasjon om forsøk på datakriminalitet som for eksempel svindel-e-poster, og forteller hvordan publikum kan beskytte seg selv hvis de skulle bli utsatt for dette. Slik forebygger politiet gjennom å gi informasjon om hvordan man kan ta grep om sin egen beskyttelse. Dette støtter oppfatningen av at en stor del av forebyggende tiltak mot datakriminalitet foregår nettopp rettet mot hva man selv kan gjøre for å unngå å bli et offer (Brewer m.fl., 2019, s. 2). Det kan argumenteres for at lovbryteren i datakriminalitet er enda mer ukjent, og dermed vanskeligere å nå for politiet. Potensielle ofre derimot, er ikke vanskelige å få tak i. Alle som bruker internett er mulige ofre for datakriminalitet, og det er ofte enkle sikkerhetsgrep som drastisk kan redusere denne risikoen (Williams og Levi, 2017, s. 459). Noe så enkelt som å bruke samme passord på sin privat-pc som sin jobb-pc kan være en sikkerhetsbrist stor nok til at noen får tilgang inn i selskapet du jobber i. Politiet kan ikke sørge for at absolutt alle bruker sikre passord, tar i bruk to-trinns verifisering eller kun kobler seg til sikre nettverk – men de kan råde innbyggerne til å gjøre dette selv som et risikoreduserende tiltak. Politiet kan ikke fjerne alle svindel-e-poster før de når en mottaker, men de kan gi innbyggerne verktøy til å avdekke og skille legitime e-poster fra svindel-e-poster. Gjennom å

legge ansvaret for å beskytte seg selv over på borgerne, kan politiet bidra til at flere av innbyggerne tar sin egen internettsikkerhet på alvor.

Å flytte fokuset bort fra lovbryter og til potensielle ofre kan virke positivt og forhindre lovbrudd, men det kan også ha flere utilsiktede konsekvenser. Ved å overlate ansvaret for datasikkerhet over til befolkningen, kan det skape et stigma rundt det å bli utsatt for datakriminalitet. Karaian (2014, s. 283) undersøkte de ansvarliggjørende konsekvensene av en kanadisk kampanje rettet mot å fraråde jenter og unge kvinner mot å sende og legge ut lettkledde, eller nakne bilder av seg selv. Hun viser til at fokuset i denne, og lignende kampanjer, ansvarliggjør unge jenter gjennom å legge skam over bildene de har valgt å ta av seg selv (Karaian, 2014, s. 283). Karaian (2014, s. 284) reagerer på at fokuset i slike kampanjer er å få jenter til å avstå fra å ta bilder av seg selv, en lovlig handling, istedenfor å fokusere på selve lovbruddet som skjer når bilder blir delt videre uten samtykke.

I et forsøk på å forebygge kriminalitet, kan ansvarliggjøring av ofre skambelegge det å bli utsatt for kriminalitet. På den ene siden vil det å informere og ansvarliggjøre befolkningen gi dem kunnskap og verktøy til å beskytte seg selv. På den andre siden derimot, kan det å legge ansvaret for egen beskyttelse over på enkeltindivider føre til at de som blir utsatt for datakriminalitet blir antatt å ikke ta godt nok vare på sin egen sikkerhet, og derfor fortjener å bli et offer (Ekendahl, Mansson, og Karlsson, 2018 i Renaud m.fl., 2020, s. 580). Selv om det er vanskelig å kartlegge, antas det å være veldig store mørketall knyttet til datakriminalitet (Riksrevisjonen, 2021, s. 30). Hvis offeret for datakriminalitet føler på en skam eller et ansvar rundt hvordan de ble et offer, kan det bidra til å øke den allerede høye terskelen for å anmelde datalovbrudd. Samtidig kan en ansvarliggjøring av egen beskyttelse påvirke hvordan politiets håndtering av datakriminalitet oppleves. Legger politiet ansvaret på innbyggerne fordi de selv ikke kan beskytte dem mot datakriminalitet?

5.1.2 Kripos

Nettpatruljen jobber på distriktsnivå, mens Kripos jobber på et nasjonalt nivå. Det vil si at der nettpatruljen jobber generelt med digitalt forebyggende politiarbeid rettet mot utfordringene som identifiseres i hele distriktet, jobber informantene mine med tilknytning til Kripos mot spesifikke fagfelt. Kripos fungerer også som Norges kontaktpunkt mellom internasjonale politisamarbeid som Interpol og Europol (Politiet, 2021a). Mine tre informanter fra Kripos er alle ansatt i NC3, men i forskjellige avdelinger. Deres stillinger innenfor NC3 angriper fagfeltet på svært ulike måter, og representerer slik godt det mangfoldige forholdet mellom internett og

kriminalitet. Det er ikke bare data-aktivert og data-avhengig kriminalitet som står i fokus, men også internett som en rekrutteringsplattform for fremtidig kriminalitet.

Pål/K jobber på seksjon for datakrimetterforskning, og beskriver sine arbeidsoppgaver slik:

> *«Jeg jobber mye med informasjonskoordinering, som vil si å motta informasjon særlig fra utlandet. Vi samarbeider mye med politienheter i andre land, og formidler den videre i egen organisasjon og agere på den ofte litt sånn med etterforskningstiltak, søke opp, finne knytninger og sånt. Og ta den informasjonen tilbake. Og i det blir det også koordinering av saker og av forebyggende aksjoner. (...) På min seksjon og på NC3 er det foreløpig ikke så mange som jobber eksklusivt med forebygging, det er mer et overordnet prinsipp på et av de overordnende målene for mye av den aktiviteten vi gjør.»*

Pål/K jobber i en avdeling for etterforskning, men er innom forebygging av datakriminalitet i arbeidshverdagen på flere måter. Han sier:

> *«I etterforskning, når vi jobber med sak så tenker vi hele tiden forebygging. Hvis det kommer en mulighet til forebygging så gjør det at man retter fokuset dit.»*

Det er ingen på avdelingen til Pål/K som kun jobber med forebygging, men det er en tanke som skal gjennomsyre alt arbeidet de gjør. Seksjonen til Pål/K tar også del i forebyggende initiativ satt i gang: «*Når de (Europol) kjører forebyggende kampanjer "timer" vi det sånn at vi er med samtidig, så det blir et europeisk fokus*.». Datakriminalitet har en grenseløs karakter, og således er det viktig at forebyggingen også skjer på tvers av landegrenser. Gjennom internasjonalt samarbeid kan transnasjonal kriminalitet bli møtt av en transnasjonal forebyggende innsats. Dette er en stor kontrast til nettpatruljens tankegang bak forebyggende innsatser som ble presentert tidligere i kapittelet. Nettpatruljens forebyggende tiltak blir i stor grad påvirket av kriminalitetsbildet i det enkelte politidistriktet, mens Kripos har et nasjonalt og internasjonalt fokus.

Herman/K jobber med tipsmottak for radikalisering og voldelig ekstremisme på internett, og hatkriminalitet. Her tar de imot tips fra befolkningen om enkeltpersoner som antas å være i en radikaliseringsprosess eller ytringer som antas å være hatkriminalitet. Det trenger ikke å foreligge et lovbrudd for å sende inn et tips, ei for at politiet skal agere. Arbeidet Herman/K driver med, kan ses i lys av en preventiv endring identifisert innenfor rettssystemet i de senere år særlig knyttet til fagfeltet radikalisering og terrorisme (McCulloch og Pickering, 2009;

Zedner, 2009). Blant annet McCulloch og Pickering (2009, s. 629) viser til denne prosessen innenfor kriminalitetskontroll, som hadde et kraftig oppsving etter 9/11. Dette preventive skiftet er karakterisert av å komme kriminaliteten i forkant gjennom kalkulering, vurdering og identifisering av mulige fremtidige farer (McCulloch og Pickering, 2009, s. 631). Herman/K jobber med forebygging av mennesker som allerede antas å være i en radikaliseringsprosess og slik altså anses som å være i en risikogruppe for å begå kriminalitet. Han forklarer tips-prosessen slik:

> *«Så når vi får inn saker, altså en typisk case er på en måte at vi får inn en bekymringsmelding om noen, en person, et miljø eller noe sånt, og så sier de at de er redd for at han eller hun er på vei til å bli en del av et ekstremt miljø eller ja virker radikalisert da. Og så gjør vi en innledende undersøkelse av det og en vurdering, og så shipper vi det videre til lokalt politi.»*

Herman/K har altså på mange måter en ren forebyggende stilling – formålet med arbeidet er å kunne oppdage og avverge individer som oppleves å være i en prosess. I følge PST (2014, s. 4) er internett det viktigste verktøyet i radikalisering. Det er altså ikke spesifikke straffbare handlinger som står i fokus, men risikoen for at et individ blir en del av et radikalisert miljø og internett som en plattform for radikalisering. Dette forebyggende arbeidet er altså personorientert. Politiets personorienterte forebyggende arbeid handler om å avdekke personer og miljøer hvor risikoen for at det vil begås kriminalitet regnes være stor (Lie, 2011, s. 60). Herman/K får inn tips om og vurdere symptomer på kriminalitet som gjør seg synlig på internett.

Jonas/K er ansatt i Kripos, men jobber for tiden i Interpol. Fagområdet han har jobbet med lenge i både Kripos og Interpol, er seksuelle overgrep mot barn på internett. Dette fagfeltet kan knyttes opp mot data-aktivert kriminalitet, for som Jonas/K viser til: *«Misbruk av barn er jo ikke et internettproblem, misbruk av barn er et menneskeproblem.».* Overgrep og overgrepsmateriale er ikke noe særeget for internett, det er en form for kriminalitet som også eksisterer utenfor internetts rammer. Internett gir derimot misbruk av barn en grenseløs karakter, overgrepsmateriale kan deles uendelig av ganger og overgripere kan nå barn fra over hele verden. Han forteller videre at: «*Håpet er jo at internett ikke lenger skal være en god plattform for å misbruke barn*.». For å jobbe mot at internett ikke forblir en plattform hvor det er enkelt å misbruke barn, forteller han at han i Interpol har hovedansvar for å drifte en samleliste over nettadresser som inneholder overgrepsmateriale. Den videre analysen vil begynne med å ta for seg arbeidet med denne listen.

5.1.2.1 IWOL

Fjerning av internettsider hvor det foregår kriminalitet er også et situasjonelt forebyggende tiltak som blir foretatt av både private og offentlige aktører for å forebygge datakriminalitet. Jonas/K forteller om Interpol sitt initiativ for å ta ned nettsider der det forekommer distribusjon av overgrepsmateriale:

> *«For meg når jeg kommer på jobb, det jeg alltid må sørge for at er i orden er at denne IWOL som vi lager, altså disse domenene som inneholder overgrepsmateriale, alltid er oppdatert. Vi deler den med alle 194 medlemsland. (...) Og målet er jo å ta bort eller fjerne adresseringer som peker til dette innholdet. Og det er en ganske betydelig jobb, å alltid være på hugget der for de endringene som vi gjør her får betydning for alle.»*

IWOL står for Interpol Worst Of List, en liste hvor Interpol samler domener som er bekreftet å inneholde overgrepsmateriale. Ved å arbeide med å opprettholde standarden og vedlikeholde denne siden, bidrar Interpol til å fjerne plattformer der det er kjent at distribusjon av overgrepsmateriale finner sted. Tanken bak situasjonell forebygging er at ved å endre situasjoner der kriminalitet kan finne sted, vil man kunne påvirke individers beslutninger om utføre kriminalitet (Gundhus, 2014, s. 185). Fjerning av nettsider bidrar til å fjerne potensielle muligheter for å tilegne seg kriminelt innhold, og slik sette kjepper i hjulene for de som ønsker å dele eller få tak i overgrepsmateriale.

Fjerning av internettsider skjer derimot ikke uten problemer, og Hutchings, Clayton og Anderson (2016) legger frem flere utfordringer ved å fjerne nettsider hvor det foregår kriminell aktivitet. De viser til utfordringer for aktører i begge ender av prosessen; både for politi som skal sette i gang nedtakelser og for tjenestetilbyderne og nettsidevertene som skal ta ned sidene. I kampen for å forhindre datakriminalitet er altså ikke politiet kun avhengig av at samfunnets individer tar grep for sin egen sikkerhet, de trenger også hjelp fra kommersielle aktører. Kripos oppfordret blant annet i 2019 at norske tjenesteleverandører til å bidra i arbeidet med å avdekke nettovergrep (Riksrevisjonen, 2021, s. 111). I dagens samfunn er en stor del av beskyttelse mot og forebygging av kriminalitet flyttet til det private markedet, det har foregått en ansvarliggjøring av trygghet (Aas, 2006, s. 75; Jones og Newburn, 1998; Loader og Walker, 2007). Eksempelvis blir ansvaret for å fjerne nettsider som inneholder kriminell aktivitet overlatt til private tjenestetilbydere, og dette kan by på utfordringer. På den ene siden står tjenestetilbyderne overfor en utfordring for å skille ut de legitime forespørslene om nedtakelser av nettsider (Hutchings, Clayton og Anderson, 2016). Samtidig kan tjenestetilbydere vegre seg

fra å hurtig ta ned nettsteder uten å selv være sikker på at det foregår kriminell aktivitet, da det kan påvirke brukerviljen av deres tjeneste. På den andre siden møter politiet på byråkratiske og jurisdiksjonære prosesser som kan gjøre det tidskrevende og vanskelig å få gjennomført nedtakelsen (Hutchings, Clayton og Anderson, 2016).

Også Moore og Clayton (2008, s. 220) identifiserer at jurisdiksjonære prosesser vanskeliggjør særlig nedtakelsen av nettsider som inneholder overgrepsmateriale av barn. Myndigheter i ett land har ikke gode muligheter til å fjerne nettsider hvor domenet er plassert i et annet land. Dette fører videre til at nettsider som inneholder overgrepsmateriale i større grad ligger på nettsider knyttet til land uten fullstendig lovverk til å effektivt forhindre den ulovlige distribusjonen (Moore og Clayton, 2008, s. 220). IWOL er derimot internasjonalt, et møtepunkt mellom offentlige og private aktører. Jonas/K forklarer det ikke kun er offentlige myndigheter i medlemslandene som har tilgang på denne listen:

> *«I tillegg blir den delt med mange store søkemotorer, store sosiale nettverk, de største "hostene" av webmateriale i verden, adresseringsselskaper og den slags.».*

På denne måten fungerer IWOL som en verifiserende enhet, dersom nettsideverter usikre på om forespørslene de mottar er legitime, har de muligheten til å få dette bekreftet gjennom IWOL.

5.1.2.2 Police2Peer

Situasjonelle forebyggingstiltak baserer seg ofte på manipulasjon av fysiske omgivelser, men som presentert i oppgavens teorikapittel kan også internett kan være en plattform åpent for manipulering. Politiet kan utnytte det faktum at internett er en arena hvor alle brukere har mulighet til å laste opp filer, for å få spredt forebyggende innhold. Et situasjonelt forebyggende grep for å øke den følte oppdagelsesfaren er advarende meldinger, beskjeder som forsøker å modifisere oppførsel gjennom å informere om konsekvensene de kriminelle handlingene som blir utført har. Jonas/K forteller om Police2Peer, et forebyggende tiltak i regi av Europol:

> *«Det vi har gjort med Police2Peer er å lage masse filmer med politifolk i uniform med bruk av politiets logoer, som alle har den samme beskjeden: denne filen har du fått fra politiets datamaskiner, når du bruker dette nettverket gir du fra deg informasjon og ip-adresse, søkehistorikk, filer du deler og en del sånne ting - og den informasjonene kan vi bruke til å finne deg, lage straffesak og komme og ta deg rett og slett. Pluss at vi peker til dette helpfiles hvis du har seksuelle interesser for barn. Også har vi tatt alle disse*

filene, da snakker vi om ti tusener av filer med politifolk og så har vi gitt de passende navn. Sånn at når du søker på det, får du opp en fil som heter akkurat det du er ute etter og velger å laste ned den. Og når du dobbeltklikker den og starter filen lokalt hos deg så er det jo ikke barn, men det er en grinete politimann som forteller deg at du kan bli tatt.»

Bakgrunnen for situasjonelle forebyggende tiltak er tanken om at kriminalitet er en rasjonell handling, og kriminalitet vil dermed være lavere i områder med tilstedeværelse av mulige vitner (Lie, 2011, s. 259). Internett kan virke som en tryggere plattform å begå kriminell aktivitet, fordi oppdagelsesfaren oppleves lavere (Blakemore, 2012, s. 14). Ved å plassere falske filer som inneholder advarende beskjeder fra politiet rundt om i fildelingsnettverk, kan politiet øke den opplevde oppdagelsesfaren. Ved å forstyrre den kriminelle atferden og minne om de alvorlige konsekvensene slike lovbrudd kan ha, ønsker politiet å avverget videre kriminell handling.

Maimon m.fl. (2014, s. 33) så i sin studie en sammenheng mellom advarende meldinger og varigheten på datainnbrudd; i tilfeller hvor lovbryteren ble eksponert for en advarende melding varte innbruddene kortere enn innbruddene uten denne meldingen. Handlinger knyttet til seksuelle overgrep mot barn, som å besitte overgrepsmateriale av barn, assosieres i samfunnet med å være pedofil (Bakketeig, 2001, s. 337). Å være pedofil blir moralsk fordømt i samfunnet og det finnes derav en enorm sosial stigma rundt handlinger knyttet til pedofili. Kan det dermed tenkes at advarende meldinger vil ha en større forebyggende virkning på denne typen kriminelle handlinger, fordi både de moralske og rettslige konsekvensene av slike lovbrudd er større? Kriminalitet blir i tankegangen om at kriminalitet et rasjonelt valg som knyttes til situasjonell forebygging et kost-nytte regnestykke, vil nytten av kriminaliteten være høyere enn kostnaden av å bli tatt? (Lie, 2011, s. 254). Kostnaden av å bli tatt for et seksuallovbrudd kan veie tyngre i kost-nytte regnestykket, på grunn av samfunnets holdninger til akkurat denne typen kriminalitet.

5.1.2.3 «Hei det er politiet, du har fått et datavirus»

Pål/K forteller om en forebyggende aksjon de satte i gang på hans seksjon, med grunnlag i informasjon de mottok fra utlandet. Han forklarer bakgrunnen for aksjonen slik:

«Det gikk ut på at denne informasjonen vi mottok fra utlandet inneholdt en del informasjon om norske personer som har blitt utsatt for datakriminalitet da. Spesifikt at noen hadde kommet seg inn på deres datamaskiner og installert skadevare, altså kall

det virus eller sånn da. Og det var en type som stjal innloggingsinformasjon, som vil si at alle disse personene hadde noe på pc-en som hele tiden sendte innloggings-informasjon, brukernavn og passord til datakriminelle.».

Eksempelet viser at datakriminalitet ikke bare har en evne å bli utført av anonyme gjerningsmenn, men selve kriminaliteten kan også være usynlig (Brewer m.fl., 2019, s. 44). Hvis noen har brutt seg inn i huset ditt vil du mest sannsynlig merke det, men det er ikke en selvfølge at man oppdager at noen har tatt seg inn i datamaskinen din. Det kan derfor være vanskelig for politiet å nå ofrene, fordi de selv ikke engang er klar over at de har blitt utsatt for kriminalitet. Gjennom internasjonalt samarbeid fikk Kripos informasjon om norske brukere som hadde blitt utsatt for en slik «usynlig» kriminalitet, og det er ikke sikkert at dette hadde blitt oppdaget uten informasjonen Kripos mottok. Pål/K forteller videre:

«Denne informasjonen, som var ganske omfattende, det var noen hundretalls norske personer, den måtte vi da agere på. Måten vi gjorde det på var at vi satt opp en egen aksjon hvor målet ved aksjonen var å varsle alle disse personene om at de hadde blitt utsatt for datakriminalitet og at passord og brukernavn var på avveie, og anbefale aktuelle tiltak som de måtte gjøre for å sikre seg selv og sin enhet. Og det ble aldri satt en formell etterforskning, det var en ren forebyggende aksjon, altså den eneste agendaen der var å forebygge. (...) Og det er jo problematisk av flere grunner, rent privat kan disse individene bli utsatt for ID-tyveri eller så kan noen hacke seg inn i nettbanken deres».

En utfordring med denne forebyggende aksjonen som Pål/K bet seg ekstra merke i, var å få eierne av den komprimenterte innloggingsinformasjonen å ha tillit til at det de ble fortalt var sant:

«Litt sånn bakenforliggende i aksjonen var jo utfordringen med å skape eller få troverdighet og tillit fra de vi kontaktet. For det som skjedde var at vi ringte og sa «hei det er politiet, du har fått et datavirus». Det høres jo veldig suspekt ut.»

Han forteller videre at det var mange som hadde svært vanskelig for å tro på dem, og at det til og med var et par de etter gjentatte forsøk ikke kom gjennom med budskapet til. Hadde mistroen vært like stor hvis de fikk en telefon om at bilen deres var stjålet eller huset deres var brutt inn i? Undersøkelser viser at befolkningen og næringslivet har lavere tillit til politiet når det gjelder datakriminalitet (Riksrevisjonen, 2021, s. 6). Hvorfor politiet opplever usikkerhet og tvil når de forsøker å informere offer for datakriminalitet, kan ha flere årsaker. Svindel er en svært utbredt

form for datakriminalitet, og finner sted for eksempel gjennom telefonsamtaler. Et eksempel på dette er den kjente «microsoft-svindelen», hvor svindlere tar på seg rollen som en Microsoft-ansatt som kontakter deg for å hjelpe deg med din datamaskin[1]. Pål/Kripos sine utsagn viser at det for publikum kan være vanskelig å skille det ekte fra det falske.

I tillegg kan mistilliten komme av at politiets håndtering av datakriminalitet ikke er like kjent for publikum som annen kriminalitetshåndtering. Befolkningen er ikke like klar over hvilke datalovbrudd de kan bli utsatt for, sammenlignet med bevisstheten rundt tradisjonelle lovbrudd (Renaud mfl., 2020, s. 585). Pål/Kripos sine opplevelser avdekker et behov for bevisstgjøring av datarelaterte lovbrudd. Datakriminalitet har ofte en «usynlige» karakter (Wills, 2017, s. 8), og dette kan påvirke denne mistilliten. De som blir utsatt kan få fortalt at det finnes et virus på deres datamaskin, men mindre datakyndige mennesker vil ikke kunne skille en data med virus fra en uten virus. Det kan tenkes at det vil være vanskeligere å stole på politiet, når de mener du er utsatt for en kriminalitet du ikke en gang kan se.

5.2 Internett som krimogen arena

Informantene har gjennomgående belyst hvilke særpreg kriminalitet på internett har, og hvordan dette påvirker deres arbeid. Internett kan hevdes å være «like mye en velsignelse, som en forferdelig forbannelse» (Jewkes, 2007, s. 5). Selv om internett har vært en viktig bidragsyter i den teknologiske revolusjon og digitale omveltning av det moderne samfunn, er det ikke en utelukkende positiv utvikling. Flere aspekter ved internett tilsier at det er et område som er bedre tilrettelagt for kriminalitet enn samfunnet for øvrig. Det videre delkapittelet vil undersøke internett, området mine informanter driver trygghetsskapende arbeid på, som en arena for kriminell aktivitet. Hvilke egenskaper er særegne for internett, og hvilke konsekvenser, sårbarheter og muligheter mine informanter opplever at disse skaper for det digitale politiarbeidet vil bli presentert.

5.2.1 Anonymitet

Internetts anonyme karakter er fremtredende i oppgavens datamateriale. Jonas/K forteller at det: «*Lenge har vært sånn at man har to måter å være på, du er en person i den reelle verden og en annen personlighet når du er i den virtuelle verden*». Internett åpner opp for at man kan re-identifisere seg selv, eller holde sin egentlige identitet skjult. Det kan skape en slags lovløshet. Hvorfor følge regler hvis ingen vet hvem du egentlig er? Theodor/N opplever at

[1] For mer informasjon om denne type svindel, se: Forbrukertilsynet (2021) *Microsoft-Svindel.* Tilgjengelig fra: https://www.forbrukertilsynet.no/microsoft-svindel

internett kan, spesielt for unge, virke som et sted hvor resten av samfunnets regler og normer ikke finnes:

> *«Vi ser en del barn og unge som tror at hvis det er et åpent kommentarfelt så kan du skrive hva du vil. De kjenner ikke til at de samme lover og regler gjelder på nett som i den fysiske verden.».*

Flere av informantene mente at samfunnets øvrige regler ikke virker like bindende på digitale plattformer. Jonas/K observerer at denne opplevelsen av at loven ikke gjelder på internett ikke bare gjelder for unge, og tenker at folk oppfører seg verre på internett enn de vanligvis ville gjort:

> *«Ikke sant vi ser det i kommentarfeltet og hvordan folk snakker med hverandre og hvor pyton man kan være, fordi de opplever at de er anonyme og det de gjør ikke får konsekvenser. Når vi tar bort muligheten for å være anonym så oppfører folk seg helt annerledes og mye bedre, og det er bra for alle i samfunnet.»*

I skildringene fra mine informanter, kan det virke som om det er muligheten for anonymitet som adskiller internett fra det fysiske sosiale rom. I den digitale verden får lovbrytere muligheten til å skjule sin egen identitet i mye større grad enn i den fysiske verden (Snyder, 2001, s. 252). Det finnes mange tilgjengelige verktøy som vanskeliggjør identifiseringen av lovbryterens faktiske identitet. Som skildret av Theodor/V og Jonas/K opplever de at anonymiteten senker terskelen for å begå norm- eller lovbrudd. Dette syntes støttes av blant annet Selzer og Oelrich (2021, s. 175), som hevder internetts anonyme karakter gjør at trusselen for å bli oppdaget og sanksjonert ikke oppleves like reell som i den fysiske verden.

5.2.2 Naturen av internett

Flere av informantene mente at internetts teknologiske egenskaper også gir større rom og nye muligheter for å begå lovbrudd. Stein/N mener at kriminaliteten ligger lett tilgjengelig for folk på internett:

> *«Og det er jo utrolig, blir dumt å si det kanskje, men det er ikke noe hemmelig at det er utrolig lett å være kriminell på nett og det er så lett å opprette fiktive profiler og brukere, og det er klipp og lim og du kan lage deg bilder.*

Han viser et ubehag ved å fortelle om hvor lett det kan være, hvor lite kontrollert internett er. På de samme plattformene mange tar i bruk hver dag, som sosiale medier, er det også mange muligheter å begå kriminalitet. Denne oppfatningen deler Pål/K, og han forteller at man heller ikke trenger å være en sofistikert aktør med lang utdannelse eller mange års erfaring innenfor IT for å kunne utnytte teknologien internett tilbyr:

> *«For de som virkelig vil så er jo ting tilgjengelig, og for de som bare har lyst til å begå litt digitalt hærverk eller har lyst til å prøve seg så er det såpass tilgjengelig til at veldig mange kan begynne med det.»*

Flere av informantene mente at hvis man går inn for å begå kriminalitet på internett, så er sannsynligheten stor for at man lykkes. Prosessene rundt etterforskning av datakriminalitet kan være svært komplekse og tidkrevende (Riksrevisjonen, 2021, s. 9). Mulige bevis og spor etter gjerningsmannen som har begått kriminalitet på internett kan forsvinne eller bli slettet, noe som kompliserer en eventuell etterforskning (Brenner, 2007, s. 17). Samtidig tilbyr den virtuelle verden nye verktøy til å begå tradisjonell kriminalitet mer effektivt, eller tilganger til å begå kriminalitet som er helt særegent for det virtuelle (Yar og Steinmetz, 2019, s. 14). Arenaen datakriminalitet gjennomføres på, kan også bidra til at det foregår så mye kriminalitet på nett. Pål/K tenker videre at det faktum at kriminaliteten foregår i en virtuell verden med et tastatur og en skjerm kan oppleves som mindre alvorlig enn å for eksempel begå hærverk i den fysiske verden:

> *«Helt klart, den (kriminaliteten) er veldig tilgjengelig og når du sitter bak en skjerm, kanskje litt det samme som med kommentartrådene, blir ting mer abstrakt, du føler deg ikke som en kriminell. Du slår ikke inn en rute, du trykker bare enter på tastaturet og ser egentlig aldri konsekvensene. Så i det er det nok lettere å bli kriminell.»*

For å avverge lovbrudd er man innenfor situasjonell forebygging opptatt av å øke risikoen for å bli tatt, fordi hvordan denne risikoen oppleves anses å være et viktig moment i vurderingen om man skal begå et lovbrudd (Lie, 2011, s. 261). Når man gjennomfører datakriminalitet har man ofte mulighet til å gjøre dette hvor som helst, uten å være fysisk omringet av andre mennesker som kan være vitne til lovbruddet. De datakriminelle kan slik oppleve et fravær av beskyttere, en av tre forutsetninger som i følge Knutsson og Søvik (2005, s. 14) skal til for at

mennesket velger å utføre et lovbrudd. Kriminaliteten blir slik mer tilgjengelig.

Internett består ikke bare av automatiske algoritmer og tekniske prosesser, mye av kriminaliteten som finnes på nett utføres av mennesker (Jewkes, 2007, s. 5). Menneskelig handling på internett kan forstyrres gjennom manipulasjon av omgivelsene. Jonas/K forteller om tiltak de gjør for å blant annet omadressere internett-trafikk bort fra sider som kjent inneholder overgrepsmateriale, og understreker at en viktig del av dette er å også gi informasjon til internettbrukeren at de har gjort dette:

> *«Når vi omorganiserer trafikk på nett så sier vi at vi har gjort det for at de skal nappes ut av den opplevelsen av at alt er ok og de bare kan klikke seg rundt og får det de ønsker.»*

Politiet kan altså utnytte internettets landskap ved å sende brukere bort fra nettsider de vet inneholder ulovlig aktivitet, samtidig som de forstyrrer den ulovlige nettsurfingen til potensielle lovbrytere. Dette momentet kan belyses blant annet av Lessig (1999, s. 6), som hevder at internett er et perfekt sted for kontroll, nettopp på grunn av de teknologiske omgivelsene. Han mener det er internetts arkitektur, landskapet skapt av koder, som gjør det til det perfekte sted for reguleringer. Internett er kanskje en del av samfunnet som er mer tilrettelagt for kriminalitet enn andre, men det kan også være bedre tilrettelagt for kontroll. Det vil også være mye mer effektivt å kontrollere internett, istedenfor å reagere i etterkant av hvert lovbrudd (Williams og Levi, 2017, s. 461). Alle internettbrukere legger igjen en form for dataspor, informasjon som kan brukes for å lage et bilde av hvem internettbrukeren er (Yar og Steinmetz, 2019, s. 237). Samtidig som man har muligheter til å holde seg anonym på internett, er det også en arena som lagrer mye informasjon om brukernes aktiviteter. I senere tid har begrepet «dataveillance» (dataovervåkning) satt sitt feste, og diskusjoner om hvilken og hvor mye informasjon ulike internettsider skal ha lov til å lagre om sine brukere har blitt utbredt (Lyon, 2014; Zuboff, 2015). Å utøve kontroll er derimot ikke uten utfordringer. Erik/N forteller at:*«Det kan være vanskelig å følge opp ting på internett.»* Han forlarer videre at det: « *Noen ganger kan det også være vanskelig å identifisere personer, og spor slettes og forsvinner fort på internett.»*. Denne uttalelsen trekker frem at politiet møter på flere utfordringer når de skal undersøke og etterforske hendelser på nett, og underbygger slik gunstigheten det å være i forkant av straffbare handlinger som skjer på internett har. Disse utfordringene med å identifisere gjerningspersoner og følge spor på internett synliggjør behovet for å drive forebygging i det digitale rom.

5.2.3 Geografisk omfang

På spørsmål om særlige utfordringer knyttet til arbeid med datakriminalitet, rettet informantene oppmerksomhet mot internetts globale struktur. Herman/K viser til at: «*Internett er jo grenseløst, det kjenner ikke fylkesgrensene eller grensene til politidistriktene*». Som nevnt i oppgavens teorikapittel skiller datakriminalitet seg fra tradisjonell kriminalitet på særlig et punkt; det finner ikke sted på et avgrenset fysisk område (Sunde, 2019a, s. 134). Selv om datakriminalitet ikke er bundet av tradisjonelle geografiske begrensninger, er fremdeles lovverk og politimyndighet avgrenset til en tradisjonell oppfatning av sted. Brenner (2007, s. 16) hevder at transnasjonaliteten som preger internett bidrar til å gjøre reguleringen av internett vanskelig. Theodor/N identifiserer også at grenseløsheten som preger datakriminalitet bidrar til at internett er et sted det er vanskelig å gjøre krav på. Han forteller at:

> *«Vi ser også at fordi det skjer på tvers av landegrenser så kan det også være krevende, fordi det å få ut brukerinformasjon og så videre er omstendelige og langvarige prosesser.»*

Theodor/N opplever det å få ut informasjon fra andre land som vanskelig og tidskrevende. Det er ikke bare det å motta informasjon for å oppdage og etterforske lovbrudd som landegrenser setter en stopper for. Jonas/K forteller at selv etter at de har oppdaget eksempelvis nettsider som inneholder kriminelt innhold, er det ikke sikkert at de får gjort noe med det*:*

> *«Noen ganger får vi ikke slettet det for det ligger i et land som gir faen rett og slett, der politiet ikke bryr seg eller de ikke har lovverk».*

Han skisserer et bilde av at store skiller mellom hva som er ulovlig, men også hvilke prioriteringer politi over hele verden har. Disse forskjellene gjør det utfordrende å kunne skape en global, universal strategi mot datalovbrudd (Blakemore, 2012, s. 12). Dette setter kjepper i hjulene for norsk politi og fører til at internett kan leve sitt eget liv uten å bli fullstendig kontrollert.

5.2.4 Tilstedeværelse og utsatthet

Fra intervjuene med noen informanter fremkommer det at en konsekvens ved at politiet tar i bruk digitale virkemidler som sosiale medier, kan være at politiets rolle i samfunnet mer utsatt. Stein/N har observert at ved å være tilstede på nett og dermed være veldig tilgjengelig for kontakt, har det også ført til en økning i useriøse henvendelser:

> *«Det er jo mye lettere å tulle med politiet nå enn hva det kanskje har vært tidligere. Vi har garantert at alle sammen skal få svar når de sender melding til oss, alle skal få svar uansett hva de skriver og spør om. Og det er jo selvfølgelig utfordrende å svare de som bare skriver "fuck politiet fuck politiet". Særlig når du sitter med andre meldinger som er reelle.»*

Han opplever denne økte muligheten for å tulle med og misbruke politiets tjenester som frustrerende, fordi det tar tid bort fra de seriøse henvendelsene. Ved å gi alle muligheten til å sende meldinger når som helst, gir man også de med onde og useriøse hensikter en større mulighet. Nettpatruljen blir nødt til å vie tid og ressurser også til dem med useriøse eller ondsinnede henvendelser. Pål/K forteller at selv henvendelser med redelige hensikter kan få uheldige konsekvenser for politiet:

> *«Det kommer til et punkt hvor man blir overlesset av informasjon, særlig kanskje irrelevant informasjon da. Når vi kan nås på mail og etterhvert også et tipsmottak for datakriminalitet, da blir terskelen så lav for å sende oss informasjon og folk forstår dessverre ikke helt hva som faller inn under definisjonen datakriminalitet. Vi får inn veldig mye og ja for det første, når man sender en mail til politiet må det trigge et svar. Og for det andre har vi en plikt til å følge opp straffbare forhold, så da generer det rett og slett masse merarbeid.»*

Pål/K viser til at økt tilgjengelighet og enklere kommunikasjon- og tipstjenester mellom politi og innbygger også kan skape unødvendig merarbeid for politiet. Å motta tips og henvendelser fra befolkningen kan være et viktig forebyggende tiltak (Politidirektoratet, 2012, s. 23), men det kan også generere mye tips og informasjon om kriminalitet politiet ikke vanligvis ville prioritert. Tilgjengeligheten økte digitale kommunikasjonskanaler inn til politiet skaper har altså en nedside, er det mulig at sosiale medier og digitale kommunikasjonskanaler gjør politiet *for* tilgjengelig? Riksrevisjonen (2021, s. 14) fastslår at politiet har en manglende oversikt over

den anmeldte IKT-kriminaliteten, samtidig som de legger frem at det er store mørketall knyttet til IKT-kriminalitet. Politiet ønsker at flere virksomheter anmelder datakriminalitet for å få en større oversikt over omfangene og metodene lovbryterne bruker (Politiet, 2021b). Samtidig vil dette føre til en enda større pågang til et allerede uoversiktlig og presset fagområde. Og som Pål/K reflekterer kan dette føre til at politiet også mottar økt informasjon om irrelevante lovbrudd som de dermed må bruke ressurser på. Den økte tilgjengeligheten politiet har fått presenterer et paradoks; politiet ønsker å motta flere anmeldelser, men samtidig er de frustrert over at folk ikke forstår hvilke lovbrudd som burde anmeldes. Politiet kan ikke fraråde befolkningen å melde fra om lovbrudd, selv om mindre anmeldte lovbrudd kunne ført til at ressursene i større grad kan brukes til de større sakene.

For å nå befolkningen på sosiale medier må politiet ta i bruk kommersielt eide medie-plattformer. Sindre/N reflekterer rundt dette:

> *«Ja nei jeg bare tenker i tillegg så er det jo en sårbarhet på en måte at det er tredjeparts applikasjoner som eier kommunikasjonsmediet vårt. Så vi må jo ha et veldig bevisst forhold til hva det er som blir delt der.»*

Han uttrykker at de må de være ekstra varsomme med hvilken informasjon de gir til befolkningen gjennom sosiale medier, fordi de bruker en plattform de selv ikke har fullstendig kontroll over. På sosiale medier har ikke politiets profiler en særegen rolle slik som ellers i samfunnet, på nett blir de én av mange. For å kunne være tilstede på samme digitale plattformer som befolkningen, har ikke politiet noe annet valg enn å gi fra seg denne kontrollen. Politiet blir slik sårbare, de må på lik linje med befolkningen stole på at tredjepartene behandler opplysningene og innholdet de legger ut på en redelig måte. Denne sårbarheten ved bruk av sosiale medier i politiarbeid trekker også Sunde (2019a, s. 147) frem, og hun viser til at bruk av slike medier til forebyggende arbeid utfordrer områdeprinsipper politiarbeid tradisjonelt er rammet inn av. Strukturen på sosiale medier er global; det finnes ingen skiller mellom nasjonalt og utenlandsk, alt innhold er åpent for alle. Dette reiser spørsmål om hvor norsk politi kan og burde drive forebyggende arbeid.

Pål/K forteller at en annen nedside med å drive kriminalitetsforebygging på digitale plattformer er at innholdet enkelt kan ødelegges, skades eller misbrukes av kriminelle aktører. Han forteller også at innholdet enklere kan misforstås enn budskap gjennom andre kanaler:

> *«Med en gang vi har lagt ut et budskap eller formidlet noe så er det ikke noen tvil at en del av det kan være litt statisk. Hvis vi legger ut et innlegg og det blir misforstått, så har man ikke samme muligheten som i et intervju med medier eller en telefonsamtale til å gjøre korrigeringer eller få oppfølgingsspørsmål.»*

Innholdet politiet produserer og legger ut på ulike plattformer havner i et hav av annet innhold og blir en del av borgernes daglige dose med sosiale medier. Dette fører derimot til at politiets innlegg blir en del av den forbipasserende «feeden» til befolkningen, og deres innlegg blir bladd forbi like fort som annet innhold. Det vil derfor være viktig for politiet å ikke bare legge ut innhold som fanger blikket til brukeren, men også innhold som er feilaktig eller kan oppleves negativt. Selvsagt har politiet mulighet til å korrigere innlegg eller slette innhold, men det er ingen garanti for at brukerne som så det uriktige innlegget i første omgang også får med seg denne endringen. Finstad (2018, s. 64) viser til at det ikke bare egne opplevelser med politiet som påvirker individers tillit, men også politiarbeidet de observerer. Dette kan knyttes opp mot hvordan politiet blir fremstilt i media, men også hvordan de fremstiller seg selv og driver forebyggende arbeid på sosiale medier. Pål/K viser til at innhold lagt ut på digitale plattformer er statisk, og slik er mer utsatt for feiltolkninger og misforståelser. Hvordan publikum oppfatter innholdet som blir lagt ut kan videre påvirke tilliten mellom politi og borger, på godt og vondt.

Det er ikke bare innhold som kan manipuleres på nett, det er også lett å holde sin egen identitet skjult. Samtidig er det også enkelt å utgi seg for å være noen andre. Richard/N forteller at de har opplevd en økende trend i kontoer som utgir seg for å være politiet:

> *«For det er jo også en sånn ting vi er opptatt av etter vi begynte på sosiale medier, nettpatruljen ble opprettet, så har vi merket også at det er falske politikontoer og det er jo en kjempeutfordring. Det er ikke så mange som har en politiuniform hjemme som ser ekte ut og som kan gå ut i gaten og late som de er på politi. Men nå som politiet er på internett og folk vet det, så er det også noen som utnytter dette og oppretter falske kontoer. For det har de jo muligheten til å gjøre, bare de har en mobil eller pc hjemme. Og ja, det ser vi er en utfordring og noe vi jobber med for å prøve å løse. Hvordan kan vi forhindre at det skjer?»*

Å utgi seg for å være politi gjennom å misbruke offentlig uniform, kjennetegn eller tittel er en straffbar handling (Straffeloven, § 165). Richard/N forteller at dette er et tradisjonelt lovbrudd som har fått større handlingsrom og muligheter ved hjelp av internett, et såkalt data-aktivert lovbrudd. Han understreker at dette er en utfordring de har møtt på, og sliter med å finne en løsning på. Dette er en problemstilling som kun er reell nettopp fordi politiet er tilstede på og har egne kontoer på sosiale medier. Tilstedeværelsen av politi på nett bidrar slik til å aktivere og muliggjøre flere datalovbrudd.

5.2.4 Publikum blir mer sårbare

Falske politikontoer kan også bidra til å sette befolkningen i sårbare og uheldige situasjoner. Hvis politikontoene virker legitime kan det føre til at personer som ønsker å kontakte politiet tar kontakt med disse falske, muligens ondsinnede falske profilene. I verste fall kan disse profilene virke så ekte at publikum tar kontakt med denne falske brukeren istedenfor den ekte. Informasjonen publikum sender til disse falske profilene kan videre potensielt bli misbrukt av de som styrer profilen. Sosiale medie-profilene til politiet bringer med en større risiko for misforståelse og feiltakelse, enn andre kommunikasjonstjenester som telefonlinjene 112 og 02800. Politidirektoratet (2015, s. 131) fastslår at det er avgjørende for politiet å styrke befolkningens tillit til deres håndtering av datakriminalitet. Negative opplevelser som assosieres med politiet på nett, som å komme i kontakt med en falsk politiprofil, kan motvirke det trygghetsskapende arbeidet politiet forsøker å drive i det digitale rom.

Theodor/N forteller at et tiltak de har gjort for å kunne veilede publikum til de ekte politiprofilene er å jobbe for å få verifiserte kontoer på Facebook, Instagram og Tiktok. Verifisering er en nettbasert legitimering, som går ut på at tjenestetilbyderen bekrefter at profilerte brukere er ekte og markerer dette med en blå «V»[2]. Dette er et verktøy publikum kan ta i bruk for å vite om politiprofilen de ønsker å kontakte er ekte. Det er derimot ikke en selvfølge at politiets profiler på sosiale medier blir verifisert, dette er en avgjørelse tjenestetilbyderne tar. Per juni 2021 er det flere nettpatrulje-profiler som ikke er verifisert, eksempelvis Instagramprofilene til nettpatruljen Agder, og Møre og Romsdal[3]. Verifisering av profiler er en mulig løsning på å skille falske politiprofiler fra de ekte, men det er problematisk

[2] For mer informasjon om verifisering av sosiale medie-profiler, se: Buisnessinsider (2014) *Instagram verifies badges*. Tilgjengelig fra: https://www.businessinsider.com/instagram-verified-badges-2014-12?r=US&IR=T

[3] Linker til omtalte instagram-profiler:
https://www.instagram.com/politietagder/
https://www.instagram.com/nettpatruljen_mrpd/

at dette er et aspekt ved profilene som er utenfor politiets kontroll og ikke felles for alle nettpatruljer.

Det er ikke bare muligheten for å bli lurt av kontoer som oppgir å være politiet som gjør at politiets tilstedeværelse på nett setter publikum i en sårbar situasjon. Theodor/N tar opp at de har opplevd at spesielt barn og unge ikke alltid klarer å kritisk skille mellom hvor de kan legge ut eller sende sensitiv informasjon. Han sier:

> *«Vi så at i kommentarfeltet på TikTok kunne det fort være at et barn eller ungdom fortalte at "Pappaen min slår meg" for eksempel. Det er jo ikke riktig forum i det hele tatt å dele den informasjonen på. For i kommentarfeltet er det synlig for alle og de gjorde seg egentlig bare sårbare. (...) Vi så at dette forumet (TikTok) ikke er modent nok eller egner seg for å ha kommentarfelt åpent, og vi derfor måtte stenge det.»*

Denne opplevelsen deler også Richard/N: «*Vi ser jo det at barn på sosiale medier er veldig sårbare. De legger ut mye informasjon, og gjerne litt ukritisk*.» Ved at politiet er til stede på sosiale medier og har åpne kommentarfelt, kan det føre til at publikum blir satt i sårbare situasjoner. Richard/N identifiserer at særlig barn ofte legger ut mye sensitiv informasjon om seg selv på nett. Åpne kommentarfelt på politikontoer kan derfor resultere i at barn og unge offentlig deler sensitiv informasjon om seg selv, og politiet blir en bidragsyter til denne delingen. Samtidig er det vanskelig å vite om unge på sosiale medier hadde delt sensitiv informasjon like ukritisk hvis politiet ikke var tilstede.

Sosiale medier er som Schneider (2016, s. 13) omtaler det, «a valuble tool with risks». Selv om politiet får flere muligheter til å nå, forebygge og være tilgjengelig for befolkningen, fører det også risikoer med arbeidet. Hvordan skal politiet vite om deres tilstedeværelse på nett gjør mer skade enn det gjør godt?

6. Organisatoriske aspekter: yrkeskultur, omorganisering og effektivitet

Dette kapittelet er den andre delen av oppgavens analyse, og vil ta for seg organisatoriske aspekter identifisert i informantenes fremstilling av deres arbeid. I denne delen av oppgaven vil jeg diskutere de strukturelle rammene som har skapt og påvirket utviklingen av digitalt forebyggende politiarbeid og datakriminalitet i norsk politi. Informantenes beskrivelser av arbeidet, dets utvikling og utfordringer vil fremlegges i lys av tre sider ved politiorganisasjonen; yrkeskultur, politireform som skaper omorganisering og fokuset på effektivitet. Hensikten er å undersøke hva som har formet håndteringen av digitale utfordringer og hvilke følger dette kan ha hatt for hvordan arbeidet med utføres i dag.

Som vi så i teoridelen er yrkeskulturer innad i politiet, særlig knyttet til endringer i den «tradisjonelle politirollen», et betydningsfullt perspektiv innenfor politivitenskapen. Hvordan mine informanter opplever yrkeskulturer i møte med det digitale forebyggende politiarbeidet og hvilken påvirkningskraft disse kan ha hatt, vil derfor bli analysert. I beskrivelsen av oppgavens bakgrunn ble politiets nylige omstruktureringsreform presentert. Denne har ført til nedleggelser av flere lokale polititjenester, i et forsøk på å skape mer sentraliserte og effektive tjenester som NC3 og nettpatruljer i hvert politidistrikt. Arbeidsstillingene til informantene i denne oppgaven kan slik omtales som et produkt av denne reformen, og vil derfor analyseres i lys av omstruktureringen.

6.1 Etablert yrkeskultur, teknologi og forebygging

Richard/N forteller om konteksten rundt nettpatruljer og utviklingen av digitalt politiarbeid, og hevder at: *«Vi henger jo langt etter, det kom ikke for tidlig akkurat»*. Det er en stor enighet rundt denne påstanden blant mine informanter, eksempelvis sier også Stein/N: *«Vi burde jo vært på banen for 10-15 år siden, vi kom veldig sent etter»*. Informantene mener at samfunnet har beveget seg raskere enn politiet, og at digitaliseringen av polititjenester ble satt i gang for sent.

At norsk politis utvikling for å opprette polititjenester på nett og håndtere datakriminalitet har gått sakte, er ikke bare mine informanters oppfatning. Dette synet støttes blant annet av Riksrevisjonen (2021, s. 14), som har gått hardt ut mot Norges håndtering av datakriminalitet og blant annet mener at Politidirektoratet og Justis- og beredskapsdepartementet ikke har prioritert IKT-kriminalitet i stor nok grad. Denne kritikken på manglende prioritering kan ses i lys av våre nabolands fremskritt innen det samme fagfeltet. Danmark opprettet sitt NC3 allerede i 2014 og like etter opprettet Sverige «Nationellt IT-brottscentrum» i 2015 (Trædal, 2017),

mens i Norge ble ikke et eget kompetansesenter for datakriminalitet opprettet før i 2019. Tidspunkt for opprettelsen av nettpatruljer kan også ses i lys av andre lands utvikling på dette punktet. Kripos opprettet Norges første nettpatrulje i 2015 og sakte, men sikkert, har dette utviklet seg til at hvert politidistrikt i Norge i dag har sin egen patrulje dedikert til nett. Schneider (2016, s. 15) viser til at Canadisk politi tok i bruk sosiale medier i sitt politiarbeid allerede i 2007, og innen 2010 ble det opprettet betjentstillinger kun viet til arbeid med sosiale medier.

6.1.1 En yrkeskultur motvillig for endring?

Hva er det som har ført til at utviklingen av kompetansesenter for datakriminalitet og digitalt politiarbeid begynte så sent i Norge? Herman/K presenterer en mulig årsak til dette. Han identifiserer at den digitale endringen i samfunnet har synliggjort et behov for et kulturskifte innad i politiet:

> *«Og det er et kulturskifte i politiet, fordi ja altså vi kommer jo fra en generasjon som er vokst opp med mobiltelefoner, datamaskiner, det er en del av vår hverdag, det er helt integrert, vi tenker ikke på det. Mens mange av de som bestemmer, mange av de som er voksne i dag de ser på det som noe fremmed ikke sant og da blir også policyen deretter.»*

Herman/K opplever at det er en etablert kultur, spesielt blant lederne i organisasjonen, som ikke ser verdien av politiarbeid som fokuserer på sosiale medier og datakriminalitet. Det er ikke bare Herman/K blant informantene som har ytret seg om at det finnes holdninger innad i politiorganisasjonen som ikke verdsetter det digitale kriminalitetsarbeidet, dette gjør også flere av de andre. Blant annet forteller Theodor/N om en opplevd skepsis rundt arbeidet med nettpatruljen:

> *«Vi så i begynnelsen at kanskje spesielt de voksne, erfarne politifolkene lurte på hva dette var for noe tull, sånn derre nettgreier. Kanskje de ikke har sosiale medier selv engang og ser verken nytten eller behovet for det.»*

Mine informanter trekker her linjer mellom kritikerne av satsningen på digitale aspekter ved kriminalitet og forebygging innad i politiet, sammen med politiansatte med lang erfaring i organisasjonen og manglende erfaring med sosiale medier. De tegner et bilde av en politiorganisasjon som blir styrt av «digitale immigranter», en gruppe som er fremmed for hvordan den virtuelle verden fungerer (Bennet, Maton og Kervin, 2008 s. 776-777). Mangel på integrering inn i den nye digitale verden kan hindre utviklingen av strategier for å ta over

kontrollen av samfunnsområdet internett. Hvorfor skal ledere satse på et område de ikke har tro på?

Om man regnes å være en digital immigrant eller ei, er det unektelig at den digitale politirollen skiller seg i stor grad fra den tradisjonelle politirollen. Historisk sett har politiyrket vært hendelsesstyrt og lokalt geografisk forankret (Gundhus, 2012, s. 178). Det nye kriminalitetsbildet krever derimot endringer i denne historiske og tradisjonsrike rollen, ettersom den ikke vil være tilstrekkelig for å møte dagens kriminalitetsutfordringer. Å innføre nye politiroller kan støte mot allerede etablerte yrkeskulturer (Gundhus, 2006, s. 54). At yrkeskulturer som omfavner den tradisjonelle politirollen kan skape barrierer for utvikling av politiet er et syn som blir støttet av flere. Jewkes og Andrews (2005, s. 55) omtaler en etablert kultur innad i politiorganisasjonen som vegrer seg for endring, og dette stanser utviklingen av en effektiv strategi for digitalt arbeid i politiet. Politiets trege utvikling på fagfeltet datakriminalitet og fraværende kontroll av arenaen internett blir ofte begrunnet med manglende ressurser og prioritering, men Yar og Steinmetz (2019, s. 219) hevder at den etablerte kulturen innad i politiet også er en bidragsyter til dette.

6.1.2 «Ordentlig politiarbeid»

Richard/N har opplevd at noe intern kritikk mot nettpatruljer grunnet i oppfatningen av hva politiet burde bruke ressurser på:

> *«Vi så at det internt var en del blandede reaksjoner. Noen sa "Så flott herregud, endelig skjer det". Mens andre er litt sånn "På nett? Ja hva skal dere på nett da?" og skjønner ikke helt grunnen til det, de mener vi må bruke mer tid på å ha folk ute i gata og drive med orden.»*

Denne uttalelsen underbygger at den digitale politirollen ikke bare strider med hva tradisjonelt politiarbeid består av, men også med en etablert oppfatning av hva politiarbeid burde bestå av. Richard/N skisserer en oppfatning innad i politiorganisasjonen som mener at digitalt politiarbeid tar ressurser bort fra andre, viktigere politioppgaver. Arbeid med datakriminalitet blir ikke omfattet av kategorien «ordentlig politiarbeid» (Yar og Steinmetz, 2019, s. 219). Gundhus fant i sin studie (2009, s. 107) at ordentlig politiarbeid ikke oppleves å bestå av teoretisk kunnskap, det skal bestå av gatekunnskap fra levende kilder. Ordentlig politiarbeid utføres blant de kriminelle på gata, ikke blant hackere og anonyme nettroll på data. Jewkes og Andrews (2005, s. 54) mener det ikke er overraskende at data-relaterte aspekter ved politiarbeid ikke blir prioritert i den grad de burde, grunnet i den macho og heltedådige kulturen som

eksisterer blant uniformert politi. Lofthus (2009, s. 199) trekker frem til at selv om politiet har gjennomgått store endringer og reformer de siste tiårene, er den fundamentale rollen politiet spiller i samfunnet fremdeles den samme. I følge Lofthus (2009, s. 199) vil tradisjonelle politikulturer fortsette å bli reprodusert og støte i mot nye endringer, på grunn av det faktum at autoriteten og makten politiet innehar, som politibetjenter former sin identitet etter, alltid vil forbli.

På spørsmål om hva han opplever som den største forskjellen mellom arbeid med tradisjonell kriminalitet og arbeid med datakriminalitet svarer Pål/K at: «*Du har liksom ikke den mistenkte i stolen som gjør det konkret da. Det gjør det mer komplekst og abstrakt*.». I arbeid med datakriminalitet og forebygging på digitale plattformer får man ikke den samme kontakten med lovbryter, og Pål/Kripos forklarer at dette gjør at arbeidet oppleves mindre konkret. Den abstrakte karakteren arbeid med datakriminalitet har, kan gjøre at arbeidet oppleves som mindre alvorlig. Å fange farlige, voldelige kriminelle kan deretter oppleves som viktigere enn å fange de ikke-voldelige datakriminelle (Jewkes og Andrews, 2005, s. 54-55). Sammenlignet med eksempelvis forebyggende arbeid oppleves ofte reaktivt politiarbeid som mer alvorlig (Gundhus og Larsson, 2014, s. 298). Når arbeidet, i tillegg til å ha en forebyggende karakter, dreier seg om en abstrakt, ukjent gjerningsmann som kan sitte bak en dataskjerm flere tidssoner unna, kan det føre til at arbeid med datakriminalitet og internett heller ikke oppleves som like alvorlig som tradisjonelt, reaktivt arbeid.

Det er ikke bare det digitale aspektet som kan diskuteres opp mot en etablert kultur innad i politiet, dette kan også gjøres med forebyggende oppgaver. Forebyggende politiarbeid representerer det såkalte «bamsepolitiet», en kontrast til det reaktive, uforutsigbare og spenningsfylte ordensarbeidet. Det er lite inngripende, smidig og mykt politiarbeid (Gundhus og Larsson, 2014, s. 298). Forebyggende arbeid er en kontrast mot den maskuline, uniformerte ordensbetjent. Miller (1998, i Gundhus, 2006, s. 54) mener at forebyggende arbeidsoppgaver blir assosiert med kvinnelighet, og for at denne rollen skal bli akseptert av tjenestemenn må de feminine trekkene omformes. Mine informanter har stillinger som innebærer forebyggende, men også noen etterforskende oppgaver. Andelen kvinner i disse områdene i politiet er typisk høyere enn andelen menn (Wathne, 2016). Dette til tross for at Politihøyskolen har oppnådd en kjønnsbalanse, de siste to årene har antall nye studenter bestått av mellom 51 og 53 prosent kvinner (Ellingsen og Lilleaas, 2020). Kjønnsbalansen blant mine informanter, hvor det er en overvekt av menn, er ikke ulikt balansen i resten av organisasjonen. At denne kjønnsbalansen finnes blant stillinger som jobber med forebygging og etterforskning som har et administrativt

preg, er derimot en observasjon som strider imot den historiske arbeidsfordelingen mellom kjønnene. Petterson (2014, s. 122) viser til at kvinner i politiet i lang tid ble tildelt kontorarbeidet, og kjønnsfordelingen mellom informantene kan være et bilde av hvordan dette har endret seg. Ut fra størrelsen på utvalget i dette prosjektet, er det ikke mulig å trekke noen konklusjoner om endringer i kjønnsforskjeller innad i politiet. Jeg syntes derimot at det uansett er et viktig moment å ta opp, fordi denne kjønnsfordelingen strider fra både mine egne og teoriens forventninger om hvem som jobber i forebyggende stillinger i politiet.

Samtidig har alle jeg intervjuet en ting til felles i stillingene de har; de jobber med teknologi. Tekniske profesjoner har lenge vært dominert av menn, og teknologier har symbolsk produsert bilder av maskulinitet (Gundhus, 2006, s. 51). I dag er det svært få kvinner i ingeniør og it-studier, til tross for et økt fokus for å rekruttere flere kvinner inn i disse yrkene (Foss, 2020). At det er en overvekt av menn som jobber med datakriminalitet og forebygging på nett er derfor muligens ikke så atypisk. Det finnes i tillegg store skiller blant spesialisering innad i politiet - av andelen spesialiserte er kun én av fem kvinner (Wathne, 2016). Miller (1998 i Gundhus, 2006, s. 54) hevder at for å oppnå en større aksept for forebyggende arbeid, må feminine trekk ved arbeidet fjernes. Fjerner forebygging med et teknologisk aspekt, som digital kriminalitetsforebygging og forebygging av datakriminalitet, de feminine trekkene med forebygging? Man kan således spørre om digitalt forebyggende politiarbeid hadde vært like attraktivt for menn uten det teknologiske aspektet.

6.1.3 En yrkeskultur i endring?

Richard/N forteller at de i nettpatruljen har jobbet for å gjøre tjenesten og dens formål kjent innad i politiet: «*I starten var det jo en jobb for å i det hele tatt gjøre oss kjent internt, folk skjønte ikke helt hva nettpatruljen var. Så det var jo en jobb vi la ned mye tid på i starten.»* Videre forklarer han at dette virker som å ha hatt en positiv innvirkning på hvordan kollegaer innad i politiet opplever viktigheten av deres tjeneste:

> *«Vi har sett at etter hvert som folk virkelig har fått innsyn i hva vi gjør og ser hva vi produserer og hva vi får til, så har vi fått snudd veldig mange av de.»*

Sindre/N forteller også om en opplevd holdningsendring, og spesielt ledelsen sine tanker om deres arbeid har snudd med tiden. Han håper at dette skal hjelpe med å utvikle deres tjeneste, Han forteller:

> *«Så jeg tror det blir mer og mer positivt, vi opplever at spesielt ledelsen i distriktet har blitt positiv og det er jo egentlig det viktigste, for det er jo de som på en måte bestemmer om vi skal satses på eller ikke.»*

Opplevelsene av oppgavens informanter om at de har oppnådd en større aksept med tiden kan tenkes å vise at det er satt i gang en integreringsprosess. Ved å få informasjon om nettpatruljen og hvilke resultater de oppnår kan de digitale immigrantene få en større forståelse for de positive effektene digitale tjenester kan ha for politiarbeid. Theodor/N forklarer at han tror at endringen i tanker om deres arbeid innad i politiorganisasjonen kan bidra til at arbeidet ikke blir bremset, og heller fortsetter å utvikle seg: *«Vi ser det at noen av de vi opplevde som både kritiske og bremsekloss i begynnelsen nå har endret holdning.».* Disse holdningsendringene kan bidra til å endre forståelsen av hva politiarbeid burde bestå av. Å produsere humoristiske og informative videoer på TikTok, eller kontakte hundrevis av innbyggere for å fortelle dem at de har et datavirus på sin maskin er politiarbeid av en helt annen karakter enn å patruljere gater og holde orden, men det betyr ikke at det ikke er like viktig for å bekjempe dagens kriminalitet. De digitale immigrantene i politiet kan tenkes å bli mer integrert i den digitale verden, som kan bedre utviklingen av håndteringen av datakriminalitet og internett som en kriminell arena.

I lys av Riksrevisjonens kritikk mot politiets håndtering av datakriminalitet ble justisminister Monica Mæland bedt om å redegjøre for hvordan departementet skal følge opp dette. Hun trekker blant annet frem at Riksrevisjonens undersøkelser ble gjort mellom årene 2016-2019, en periode der politiet gjennomgikk store organisatoriske forandringer som kan ha påvirket utviklingens fart (Riksrevisjonen, 2021, vedlegg 2). Hun hevder også det har blitt gjort flere framskritt i etterkant av Riksrevisjonens undersøkelser og at departementet og politidirektoratet er på god vei til å bedre politiets håndtering av datakriminalitet. At politiets utvikling innenfor fagfeltene datakriminalitet og digitalt politiarbeid står høyt på Politidirektoratet og Justis- og beredskapsdepartementet sin agenda er det ingen tvil om (Politidirektoratet, 2015; Politidirektoratet, 2017; Justis- og Beredskapsdepartementet, 2020). Samtidig som politiet som organisasjon retter et stort fokus mot å gjøre internett til et tryggere sted, observerer også flere av mine informanter endringer i hvilke holdninger politiansatte har til digitalt forebyggende arbeid. Dette kan tyde på at et større organisatorisk fokus kan gjøre flere innad i politiet klar over viktigheten og fordelene med å drive forebyggende politiarbeid på nett.

6.2 En politiorganisasjon i endring

I sin uttalelse ovenfor peker Mæland på at politiorganisasjonen har gjennomgått store strukturelle endringer særlig i de siste årene, og dette ble også tatt opp blant noen av mine informanter. Hovedlinjene til politireformen fra 2015 har blitt presentert i denne oppgavens bakgrunnskapittel. En begrunnelse for disse store strukturelle endringene innad i organisasjonen er blant annet å redusere det administrative arbeidet, for å frigjøre midler til økende tilstedeværelse og kartlegging av kriminalitet (Gundhus og Larsson, 2014, s. 276). Richard/N snakker om konsekvensene disse omstruktureringene har hatt for befolkningen, og sier: «*Nå er det jo flere og flere lensmannskontor som blir lagt ned, dessverre, og folk opplever en større fysisk avstand til politiet»*. Han viser en forståelse for at publikum kan oppleve sentraliseringen av tidligere lokale lensmannskontor som dumt, og er tydelig på at omstruktureringen etter reformen ikke bare har positive resultater. Flere argumenterer for at reformen som ble igangsatt i 2017 tar et steg bort fra nærkontakt med publikum (Christensen, Lægreid og Rykkja, 2017; Gundhus, Talberg og Wathne, 2018; Larsson, 2017; Gundhus m.fl., 2018). Nærpolitireformen kan være et misvisende navn fordi det ikke alltid skaper et nærere politi, i mange lokalmiljøer har avstanden til politiet økt med sentraliseringen av polititjenester.

På spørsmål om forskjeller mellom tradisjonelt forebyggende arbeid og digitalt forebyggende arbeid forteller Stein/N:

> *«Selvfølgelig kjenner jeg på at jeg savner den menneskelige kontakten, det kan ikke erstatte det. Det er noe med å kunne møte folk fysisk, kunne se dem i øynene når du prater med de, sjargongen blir jo deretter. Og det å kunne lese kroppsspråk og alt det her, ja da jeg savner det fysiske møtet.»*

Stein/Vest er tydelig på at få ting kan erstatte det fysiske møtet med publikum, og dette er et aspekt han savner i sin arbeidshverdag. I følge Justis- og beredskapsdepartementet (2020, s. 38) var et formål med nærpolitireformen å skape et mer tilgjengelig og tilstedeværende politi med god lokal forankring og samhandling. Stein/N påpeker at samhandlingen med befolkningen blir påvirket av en manglende fysisk tilstedeværelse, og han opplever det som utfordrende å kun møte ungdommen gjennom en skjerm. Richard/N forteller også om at det er forskjell mellom fysiske og digitale møter, og syntes dette er spesielt utfordrende når de er i kontakt med publikum som befinner seg i vanskelige situasjoner:

> *«Og så opplever jeg også at det er noe annet å møte folk på nettet enn i den virkelige verden, du ser ikke det samme, du får ikke kroppsspråk, du ser ikke hva slags situasjon de står i, du ser ikke hvem de eventuelt er med og så videre.»*

Mangelen på fysisk nærkontakt forklares av noen informanter å være et utfordrende aspekt ved det digitalt forebyggende politiarbeidet. Disse skildringene gjenspeiler noe av kritikken som blir rettet mot nærpolitireformen, større fysisk avstand kan påvirke kontakten mellom politi og borger (Gundhus, Wathne og Talberg, 2018, s. 210). Ved at den forebyggende arenaen er flyttet fra gata til data, opplever de ansatte at viktige komponenter ved forebyggingen kan falle bort. Det oppleves av noen informanter å være vanskeligere å samhandle med publikum i situasjoner hvor det hadde vært nyttig å forstå konteksten publikummet befinner seg i.

6.2.1 Digitale tjenester og politiets tilgjengelighet

I dag kan man nå politiet via en rekke digitale tjenester. Det er mulig å anmelde og sende inn tips om straffbare forhold, og med opprettelsen av nettpatruljer får også publikum mulighet til ha en to-veis kommunikasjon med politiet på nett. Richard/N forklarer at digitale tjenester ikke bare er noe befolkningen ønsker, men også forventer:

> *«Folk oppsøker ikke lenger kontorer, de vil ha det enklest mulig og gjøre det hjemme fra rommet sitt på nett eller telefon eller hva det skulle være».*

For mange er den foretrukne plattformen for kontakt med politiet i dag digital, og derfor skal politiet kunne tilby nye, digitale tjenester (Justis- og Beredskapsdepartementet, 2020, s. 36). Opprettelsen av nettpatruljer, og muligheten til å kontakte politiet på sosiale medier, kan bidra til å gjøre politiet mer tilgjengelig. Theodor/N er tydelig på at digitaliseringen av polititjenester kan fungere som en erstatning for noen polititjenester som har forsvunnet med reformen: *«Istedenfor at de (publikum) blir helt frustrert for at de aldri får tak i politiet, så kan de nå få tak i politiet på nye måter».*

Selv om politiets sosiale medier-profiler ikke er bemannet hele døgnet, er plattformenealltid åpne for publikum. De kan oppsøke innleggene politiet legger ut og sende dem meldinger til alle døgnets tider, og trenger ikke å forholde seg til stengte telefonlinjer eller politikontorets åpningstider for å ta den første kontakten med politiet. Som Sindre/N påpeker så «*virker det som det er lavere terskel for å ta kontakt med politiet når man blir utsatt for ting*». Det kan være

lettere å ta kontakt med politiet hvis man har mulighet til å sende en melding på Messenger eller Instagram mens man sitter hjemme på soverommet sitt. Justis- og Beredskapsdepartementet (2015, s. 75) understreker at et av formålene med den nye struktureformen er at organiseringen av politiet skal innrettes slik at publikum opplever at de har et tilgjengelig politi når de har et behov for deres tjenester. Definisjonen av et tilgjengelig politi består ikke lenger bare av geografiske avstander.

6.2.2 Rekruttering av sivile forebyggende agenter og prosesser

Politiets økte tilgjengelighet på nett via sosiale medier har hatt følger mine informanter ikke hadde sett for seg. Deres tilstedeværelse på nettet har vist seg å ikke bare ha virkninger for de som aktivt følger eller velger å oppsøke deres profiler på internett, det har også fått konsekvenser for andre brukere. Stein/N forteller:

> *«Og det samme i forhold til barn og unge som, og spesielt på TikTok, hvis de ser et eller annet som de reagerer på og de ønsker at politiet skal vite noe om så tagger de oss. Dette er jo noe ungdommen selv har funnet ut, at det er en ny måte å kontakte politiet eller gi beskjed til politiet, det er ikke noe vi har gått ut og bedt de om.»*

På de ulike sosiale medie-plattformene har brukere mulighet til å tagge nettpatruljene i kommentarfelt. Når nettpatruljen blir tagget, får de så et varsel om dette og link til kommentarfeltet de har blitt tagget i. Stein/N identifiserer at profiler på spesielt TikTok bruker denne funksjonen for å varsle politiet om ulovlig eller ugreit innhold som blir lagt ut på plattformen. Sindre/N forteller at:

> *«Vi blir tagget utrolig masse, vi ser også at mye blir fjernet fordi vi blir tagget. Og det vil jo si at når vi går hjem for dagen så fortsetter barn og unge å jobbe for oss.»*

Det å bli tagget kan altså øke den opplevde oppdagelsesfaren for når politiet blir tagget kan det jo hende at de ser innholdet som blir lagt ut. Sindre/N opplever at flere angrer seg på det de legger ut, og sletter videoen etter en nettpatrulje har blitt tagget i kommentarfeltet. Muligheten til å varsle politiet ved å tagge dem i et kommentarfelt, blir et lavterskel-tilbud. Taggingen kan gjøres ikke bare ved ulovlig innhold, men også videoer som inneholder mobbing, personangrep eller annet ugreit innhold. Det blir en enkel og ufarlig måte for brukere å varsle politiet, og skaper sivile forebyggende prosesser. Når de ansatte i nettpatruljen går hjem for dagen, bidrar brukerne på sosiale medier til å gjøre internett til et tryggere sted. Selv om nettpatruljen er et dagstilbud, foregår det forebyggende arbeidet på nett som nettpatruljen bidrar til, til alle døgnets tider. Sindre/N presiserer at: *«Vi har ikke sjans til å få med oss alt vi blir tagget i, for det blir vi*

flere hundre ganger i løpet av dagen.». Muligheten til å tagge politiet er noe som blir brukt så ofte, at nettpatruljen ikke engang klarer å få med seg alt innholdet de blir tagget i. Derimot kan bare det at de blir tagget være forebyggende, ettersom profilen som la ut innholdet ikke vet om politiet faktisk har tid til å se innholdet eller ikke.

Muligheten til å varsle politiet gjennom å bruke tagge-funksjonen kan også ha uheldige konsekvenser. Som Sindre/N nevner blir nettpatruljen tagget så mange ganger, at de ikke har mulighet til å undersøke absolutt alt. Hvis tagge-funksjonen blir brukt som en substitutt til, og ikke bare en tilleggstjeneste til å kontakte politiet direkte gjennom Messenger, 02800 eller 112, kan det ha uheldige konsekvenser. Det er viktig at informasjon om at man må sende en melding eller kontakte politiet på telefon for å få garantert et svar er tilgjengelig for befolkningen, og at tagge-funksjonen ikke blir brukt istedenfor de etablerte kontaktpunktene. Politiet har ikke mulighet til å se alt de blir tagget i, og hvis brukerne som bruker tagging forventer nettopp dette kan det skape utrygghet og svekke forholdet til politiet. En årsak til hvorfor nettpatruljen Vest opplever å bli tagget mye, kan tenkes å også kunne være fordi noen velger å misbruke tjenesten. Å tagge politiet i innhold kan også bli gjort med useriøse hensikter. Jo flere tagger politiet får, jo flere tagger vil de også ikke få med seg og slik kan de miste verdifulle varslinger fra befolkningen. Også når politiet får med seg tagger og velger å agere, kan det skape utfordringer. I mai 2021 ble nettpatruljen Vest ble kritisert av TikTok-profiler og beskyldt for å legge føringer på norske brukeres innholdsproduksjon (Arnø, 2021). Bakgrunnen for kritikken som oppsto var nettopp at politiet hadde oppsøkt et kommentarfelt de hadde blitt tagget i flere ganger, og de forsøkte å unngå en eskalering av konfliktnivået (Arnø, 2021). Når nettpatruljen mottar mange tagginger om samme innhold, forventes det kanskje også at de skal ta grep i situasjoner de vanligvis ikke ville blandet seg i. Det kan oppstå en konflikt mellom hvilket arbeid nettpatruljen skal fokusere på, og hvilke forventninger befolkningen har om politiet burde reagere i visse situasjoner.

6.3 Effektivitet

Et mål med nærpolitireformen var å skape et politi som arbeider mer effektivt ved å ta i bruk bedre metoder og ny teknologi (Justis- og beredskapsdepartementet, 2020, s. 38). Er digital kriminalitetsforebygging en mer effektiv form for kriminalitetsforebygging? For å undersøke dette vil jeg ta for meg ulike momenter informantene tok opp som gjenspeiler dette. Den videre analysen tar for seg tre synspunkt som påvirker arbeidets effektivitet og gjorde seg synlig i datamaterialet; rekkevidde, ressursbruk og samarbeid, både innad i politiorganisasjonen og med private tjenestetilbydere.

6.3.1 Digitalt forebyggende politiarbeid og rekkevidde

På spørsmål om hva den største forskjellen mellom tradisjonelt forebyggende arbeid og digitalt forebyggende arbeid, svarer Erik/N at han opplever at en av de mest merkbare forskjellene er rekkevidden det forebyggende budskapet får:

> *«Du kan tenke deg hvor mange du når i en klasse kontra hvor mange du når på TikTok, der vi har flere hundre tusen følgere.»*

Samtlige av mine informanter sier seg enig i dette, og Theodor/Vest poengterer at: «*En politipatrulje når mange hundre, en nettpatrulje når mange hundre tusen.*». Ved å ta i bruk digitale plattformer som sosiale medie-kanaler kan nettpatruljen nå alle internettbrukere. Selv om nettpatruljen Vest sitt hovedfokus er å skape innhold rettet mot Vest politidistrikt, har ikke digitalt forebyggende politiarbeid noen geografisk grense. Den mest sette videoen til nettpatruljen Vest sin TikTok-profil har i august 2021 9,8 millioner visninger[4], og det er helt klart at denne videoen har nådd forbi politidistrikt Vest sine grenser. Nettpatruljen Vest jobber derfor ikke bare forebyggende innenfor sitt eget distrikt, deres forebyggende innsats på nett kan også bidra med å pleie tillitsforholdet mellom politi og befolkningen over hele landet. Selv om nettpatruljene i Norge tilhører hvert sitt spesifikt politidistrikt, fastslår Justis- og Beredskapsdepartementet (2020, s. 36) at patruljene ikke trenger å følge de geografiske grensene og at et samarbeid på tvers av politidistrikter er viktig for utviklingen av nettpatruljene. Nettpatruljen Vest har helt klart den største følgerskaren på TikTok av de norske nettpatruljene, og vil derav ha mulighet til å nå flest mulig i Norge med sitt forebyggende budskap. Internett fjerner ikke bare geografiske begrensninger knyttet til kriminalitetsmuligheter, det fjerner også geografiske begrensinger for

[4] Link til omtalt video:
https://www.TikTok.com/@politivest/video/6849343583569448197?is_copy_url=1&is_from_webapp=v1

kriminalitetsforebyggende arbeid. Nettpatruljen representerer en ny politirolle som utnytter mulighetene internett gir og ikke er like geografisk forankret som før.

Richard/N opplever at den store rekkevidden de kan oppnå kan være svært verdifull hvis de ønsker å gå ut med et forebyggende budskap så raskt som mulig:

> *«Men det som, det jeg opplever annerledes med å forebygge kriminalitet på nett kontra tradisjonell forebygging er jo at vi har muligheten til å nå ut til sinnssykt mange på veldig kort tid. Sitter vi på informasjon som vi tenker "det her er tidskritisk, det her må vi få ut" så har vi muligheten til å gjøre det og nå ut til mange på kort tid.»*

De digitale plattformene nettpatruljen har etablert gjør at politiet kan nå befolkningen når som helst. Det fysiske rommet i det moderne samfunn har blitt invadert av det digitale, og skapt et digitalt rom som ikke er omfanget av de tradisjonelle begrensningene til tid og rom (Santos og Azevedo, 2019, s. 268). Som et resultat av denne komprimenteringen av tid og rom, kan politiet i større grad lykkes i å informere en stor del av befolkingen om aktuelle hendelser. Flere av informantene mine trekker frem at de setter pris på eksempelvis skolebesøk som et kriminalitetsforebyggende tiltak, men at det er uheldig at det går lang tid mellom hver gang elever får kontakt med politiet. Gjennom å drive forebyggende tiltak på digitale plattformer får barn og unge en mer konsekvent og jevn kontakt med politiet. Theodor/N forteller:

> *«Nå kan vi nå de (målgruppen) en gang i uken, vi kan nå dem hver dag hvis vi ønsker det. Vi kan nå dem på en jevn basis og la det bli en del av den inputen de får og legge til nye ting underveis, ikke om to-tre år.»*

Utsagnet viser at i tillegg til å øke den geografiske og demografiske rekkevidden, får også politiet mulighet til å øke hyppigheten de kan nå befolkningen med. Når de fysiske begrensningene for å nå ut til befolkningen med forebyggende budskap blir borte, får politiet også en økt mulighet til å nå befolkningen oftere. Theodor/N forklarer at de nå er mer tilgjengelig for befolkningen, hvor enn de befinner seg. Du trenger ikke å være tilstede på skolen eller se på nyhetene, det forebyggede budskapet når deg overalt hvis det kommer fra en digital plattform:

> *«Hvis barn og ung ligger syke hjemme så får de fortsatt TikTok-innholdet med seg. (...) Vi når dem også om de er på hytta eller i Spania, så lenge de følger Vest politidistrikt så får vi nådd dem der også. Og det har vi aldri kunne gjort før. Vi når folk på helt nye plasser og veldig samtidig.»*

6.3.2 Er digitalt forebyggende politiarbeid ressurseffektivt?

Sindre/N forklarer at en av de største fordelene han opplever i arbeid med digital kriminalitetsforebygging er at de får utnyttet ressurser på en god og effektiv måte. Han forklarer: «*Det er veldig ressurseffektivt, to-tre timers arbeid med en video kan være som et årsverk egentlig i sammenligning med eksponeringstid*.». Han viser til at den lille tiden de bruker på å produsere innhold til nettpatruljens profiler kan oppnå en eksponeringstid som sammenlignet med andre, tradisjonelle polititjenester er enorm. Flere av mine informanter trekker frem dette aspektet, og Theodor/N utdyper:

> *«Vi ser at enkelte av de budskapene vi har som vi bruker en eller to dag på, kan kanskje tilsvare arbeid for én person i politiet som måtte reist rundt i, ja vi snakker fort om et halvt år egentlig for å nå ut til like mange. Så jeg føler egentlig at den digitale kriminalitetsforebyggingen er effektiv bruk av ressurser.»*

Den enorme rekkevidden politiet kan oppnå ved bruk av digital kriminalitetsforebygging bidrar til at politiet får mye ut av få ressurser. Et av hovedformålene med nærpolitireformen var å utnytte de samlede ressursene bedre (Gundhus, Talberg og Wathne, 2018, s. 202). Et forsøk på å få mest mulig ut av ressursene og øke produktiviteten var gjennom digitalisering av polititjenester, som å opprette nettpatruljer (Justis- og beredskapsdepartementet, 2020, s. 36). Innhold produsert av nettpatruljen kan nå flere millioner, og i teorien er det forebyggende innholdet tilgjengelig for alle Norges internettbrukere.

Det er derimot en viktig forutsetning for at arbeidet nettpatruljen utfører skal være en effektiv bruk av ressurser. Erik/N forklarer:

> «*Men det er også veldig viktig at vi får mange nok som tar kontakt og bygger opp tjenesten, for å få det til å gå rundt er vi avhengig at vi får folk til å ta kontakt og at vi når til ut befolkningen med det forebyggende budskapet. For hvis vi bruker masse tid på å lage en post om ruskjøring, og så er det 100 personer som ser det så er det kanskje unødvendig arbeid.»*

Digital kriminalitetsforebygging reiser en problemstilling ukjent for tidligere politiarbeid. Politiet som statens voldsmonopol og en del av den utøvende makt har en naturlig autoritær rolle i samfunnet. Politipatruljens tilstedeværelse i samfunnet blir synliggjort ved bruk av uniformer og politibiler, og ved hjelp av dette kan de formidle budskap til befolkningen. For at

nettpatruljer skal få utført sitt arbeid og nå ut til befolkningen er de derimot avhengig av å opparbeide seg en følgerskare. Som Erik/N forklarer må innholdet de produserer faktisk nå ut til befolkningen for at det skal være en effektiv bruk av ressurser. I tillegg avgjør populariteten og engasjementet[5] innlegg skaper, hvor synlig innlegget blir på plattformen (Wood, 2020, s. 53). Denne forutsetningen, om at politiet må skaffe seg følgere og engasjement for å lykkes i arbeidet de driver med er sammenlignet med tradisjonelt politiarbeid svært annerledes. Det er derimot en viktig del av politiarbeid på sosiale medier, for å kunne få mest mulig ut av tjenesten må politiet opparbeide seg et interaktivt publikum (Schneider, 2016, s. 127). Det er en stor variasjon blant følgertallene til de ulike plattformene drevet av nettpatruljen Vest. Som tidligere vist har de en enorm følgerskare på TikTok, mens dette tallet er betydelig lavere for plattformene Facebook og Instagram. Vest politidistrikt omfatter mesteparten av Vestland fylke, et fylke med litt over 630 000 innbyggere (Snl, 2020). Sett i dette perspektivet er eksempelvis følgertallet nettpatruljen har på Facebook på litt over 10 000, ikke et veldig høyt tall. Når man ser på følgertallene må man legge til grunn at følgerkulturen er ulik fra plattform til plattform, det er kanskje mer normalt å trykke følg på en profil på TikTok enn det er på Facebook. I tillegg er alle nettpatruljens profiler offentlige, som vil si at man kan oppsøke innholdet de legger ut selv om man ikke er en følger. Det er likevel viktig å se deres rekkevidde og begrensningene digitalt forebyggende politiarbeid arbeid kan møte på. I tillegg kan man lure på om det å skaffe seg flere følgere og likes er noe politiet burde prioritere sine ressurser på.

6.3.3 Politisamarbeid på tvers

Datakriminalitet kan hevdes å være et de-territorialisert fenomen, det strekker seg forbi geografiske grenser som skiller bydeler, politidistrikter, land og verdensdeler (Yar og Steinmetz, 2019, s.16). Befolkningen er i dag teknologisk mer knyttet sammen enn noen gang før, og det samme må politiinstitusjoner være for å kunne møte og forebygge den grenseløse kriminaliteten. Samarbeid blir derfor en viktig del av politiets økende effektivisering av arbeidet med og forebygging av lovbrudd på nett. Stein/N forklarer at hans arbeidsoppgaver går mye ut på samarbeid med andre seksjoner i Vest politidistrikt:

[5] Engasjement i form av likes, kommentarer og delinger.

> *«Det jeg har hatt fokus på jobb er å få til et godt samarbeid internt der jeg ser at det er behov for dialog eller kunnskapsdeling for å skape en best mulig arena for forebygging.»*

Han forteller at internt samarbeider de mye med blant annet de som driver med etterretning for å kartlegge hvilke utfordringer som finnes i distriktet. For å kunne gå ut med nødvendig informasjon og forebyggende budskap er nettpatruljen nødt til å være klar over hvilket behov som finnes. Det vil derfor være viktig å samarbeide med de som jobber med etterretning i distriktet, for det er de som faktisk er ute i distriktene og opplever hva som rører seg. Ved å ha et fokus på dette samarbeidet kan nettpatruljen skape en helhetlig tjeneste for hele politidistriktet. Samtidig som å kunne styrke tjenestens kvalitet, vil det også kunne øke effektiviteten til tjenesten. For å kunne nå den ønskede målgruppen, må politiet også vite hvilke budskap de kan nå målgruppen med (Brewer m.fl., 2019, s. 42). Herman/K forteller at en stor del av hans arbeid også består av samarbeid innad i politiorganisasjonen: «*Vi har direkte kontakt med politidistriktene og de koordinatorene som er der, og det er ofte samarbeid på saksnivå.».*

Pål/K forteller at samarbeid med politienheter i utlandet er noe han jobber mye med. Han forklarer:

> *«Vi samarbeider mye med politienheter i andre land, og formidler informasjon videre i egen organisasjon.(...) Og så samarbeider vi med en del land gjennom Europol i noe som heter Empact, og der er forebygging formalisert gjennom flere punkter man skal jobbe med på en plan. Og gjennom det får vi informasjon fra utlandet og blir invitert til forebyggende aksjoner og tiltak hvor vi da deltar litt sånn innenfor det formaliserte ved forebygging.»*

Transnasjonale politisamarbeid, som Europol og Interpol, skal komplementere lokalt politi (Wall, 2007, s. 161). Justis- og Beredskapsdepartementet (2020, s. 44) hevder at forebygging, avdekking og håndtering av digital kriminalitet ikke kan rammes inn av nasjonale grenser. Det er ikke bare viktig, men også nødvendig å samarbeide på tvers av landegrenser for å kunne ha mulighet til å få kontroll på den kriminelle digitale sfære. Samarbeidsavtaler som Empact[6], hvor det blir satt felles mål om hvilke utfordringer medlemslandene skal sette inn ressurser for å

[6] For mer informasjon om Empact, se: Europol (2021) *Empact.* Tilgjengelig fra: https://www.europol.europa.eu/empact

bekjempe, er en felles innsats som kan øke effektiviteten i møte med digital kriminalitet. Når kriminalitetsformen er grenseløs, må responsen fra politimyndigheter være det samme.

Jonas/K forteller om et internasjonalt samarbeidsprosjekt kalt International Child Sexual Exploitation Database (ICSE). Bakgrunnen for denne databasen er å kunne unngå at politimyndigheter verden over etterforsker de samme overgrepssakene:

> *«Vi har hatt en del uheldige saker opp gjennom årene hvor man i et land har lagt ned masse tid, penger og tankevirksomhet for å prøve å oppklare en sak som allerede er oppklart i et annet land. Så for å unngå det har man opprettet en identifiseringsdatabase. (...) Hovedmålet med databasen er ut av det blå identifiseringer, at man kommer over materiale som har informasjon i seg som gjør at man tror man kan finne ut hvor det har foregått. Og så jobber man sammen for å finne ut at det er dette kontinentet, dette landet, dette området, så plasserer man etterforskningen nærmest mulig fornærmende eller gjerningsmannen, avhengig av hva man har av informasjon for å finne personer og stanse de overgrepene som fortsatt pågår.»*

Etterforskning og oppklaring av for eksempel grove overgrepssaker på internett kan ta utrolig mye tid og ressurser for å oppklare. Ved å forsøke å kartlegge alle saker som allerede er oppklart og hvilke ofre som allerede er identifisert, vil den samlede globale innsatsen mot overgrep på internett bli effektivisert. Kriminalitetsbildet tyder på at antall tradisjonelle kriminelle handlinger begått er nedadgående, mens data-avhengig og data-aktivert kriminalitet øker (Riksrevisjonen, 2021, s. 4). Hvis denne trenden øker, vil politiet trenge flere og flere ressurser for å kunne beskytte befolkningen for disse formene for kriminalitet. Tiltak for å effektivisere den internasjonale innsatsen, som å kartlegge hvilke lovbrudd som allerede er avdekket og slik frigjøre ressurser til andre lovbrudd, kan bli avgjørende for om politiet noen gang klarer å ta igjen de datakriminelle i det pågående kappløpet. Dette er en påstand Riksrevisjonen (2021, s. 9) er enig i, de fastslår at internasjonalt samarbeid i mange sammenhenger er avgjørende for oppklaring av datakriminalitet. De trekker derimot også frem at en utfordring norsk politi møter på er ulikheter i lovgivning i forskjellige land, som gjør det krevende å opprettholde en effektiv kriminalitetsbekjempelse (Riksrevisjonen, 2021, s. 9).

6.3.4 Samarbeid med tjenestetilbydere

Både det kriminalitetsforebyggende bildet og privat datasikkerhet er avhengig av flere aktører enn bare politiet. Når kriminaliteten blir flyttet til kommersielt eide digitale plattformer, blir også disse en aktør det plurale politiarbeidet. Særlig har private leverandører av teknologi fått en stor innflytelse i kontrollen av det digitale (Bowling, Reiner og Sheptycki, 2019, s. 158), for eksempel ved at tilbydere av tjenester som sosiale medier sitter på mye informasjon om sine brukere, som videre kan være verdifull for politiet. For å kunne innhente informasjon og drive det digitale forebyggede arbeidet mer effektivt må derfor politiet også samarbeide med tjenestetilbydere. Sindre/N forklarer at de samarbeider med sosiale medie-plattformer:

> *«Vi har kontakter i Facebook, Instagram så vi kan kontakte de direkte. Og det har vist seg spesielt verdifullt nå når det har vært sånn selvmordsvideoer og sånne ting. (...) Nå har vi fått det samme på TikTok og tror vi har en kontakt på Snapchat også. Som sagt så er det mer for å gjøre tiltak opp imot ting som skjer på de plattformene.»*

Sindre/N forteller at de har fått etablert egne kontaktpunkter hos de sosiale medie-plattformene de benytter seg av. Dette fører til at politiet for eksempel enklere får fjernet innhold som er med på å gjøre internett til et utrygt sted for barn og unge. Sindre/N viser til at denne muligheten har vært verdifull i tilfeller hvor videoer av selvmord[7] har spredd seg på internett. Kommer politiet over disse, eller får informasjon om det tilsendt fra befolkingen, kan de direkte kontakte plattformene innholdet befinner seg på.

Teknologiselskaper har blitt viktige aktører i den polisiære virksomheten for å skape et tryggere internett (Yar og Steinmetz, 202, s. 245). Politiet er blant annet avhengig av at tjenestetilbydere fjerner ulovlig materiale fra sine tjenester. Theodor/N legger til at en viktig årsak til hvorfor de fokuserer på å ha et godt samarbeid er fordi det vil effektivisere prosesser:

> *«Ja, vi har noen kontaktpunkt med de (Facebook og Instagram). Og det er rett og slett fordi det ikke alltid det er effektivt nok å bare rapportere i appen, men at vi må gå et hakk videre og kontakte de kontaktpersonene vi har.»*

[7] Et kjent tilfelle av massedeling av en selvmordsvideo skjedde høsten 2020. Nettpatruljen Vest lagde blant annet en TikTok-video som advarte barn mot denne, se:
https://www.TikTok.com/@politivest/video/6870942667417685250?is_copy_url=1&is_from_webapp=v1

Herman/K forteller om at han som i all hovedsak primært driver med personorientert forebygging ofte ikke har mulighet til å motta informasjon fra tjenestetilbydere:

> *«For å få informasjon fra Facebook må man vanligvis ha en straffesak i bunn da. Og det har vi jo sjeldent, så vi er nok stort sett overlatt til å finne informasjonen selv. Det er veldig få selskaper som bare gir oss informasjon. Det kan være at vi i en del tilfeller hvis det åpenbart er et nødstilfelle så får vi jo mye info fort. Men i vanlige saker så får vi ikke det.»*

Herman/K opplever at de ikke mottar noe informasjon hvis det ikke er knyttet opp mot en spesifikk straffesak. At tjenestetilbydere ikke er samarbeidsvillige før et lovbrudd har funnet sted, vanskeliggjør digitalt politiarbeid med forebyggende formål.

Samtidig er det ikke en selvfølge at politiet skal kunne motta all informasjon om sine innbyggere. På grunn av informasjonsegenskapene til data- og nettverksteknologier, blir det produsert massive mengder data når individer tar i bruk disse teknologiene (Yar og Steinmetz 2019 s. 238). Begrepet «Big Data» brukes om slike massive datamengder, denne datasamlingen gjør det mulig å søke, samle og kryssreferere informasjon om personer (Boyd and Crawford, 2012, s. 663). Denne egenskapen til å samle inn og lagre data har blitt utnyttet av myndigheter og private aktører for å overvåke befolkningen (Lyon, 2014, s. 5). Et av de største og mest kjente tilfellene av dette ble i 2013 avslørt av Edward Snowden, da han lekket dokumenter som viste hvordan den amerikanske sikkerhetsmyndighet masseovervåket både egne og utenlandske innbyggere (Lyon, 2014, s. 2). Denne avsløringssaken skapte storm i debatten om hvor mye myndigheter overvåker, og burde få lov til å overvåke befolkningen. Det er satt i gang mange prosesser for å kontrollere hvordan myndigheter og private aktører oppbevarer og behandler sensitiv personinformasjon om enkeltindivider, eksempelvis GDPR-lovverket innført av EU (Yar og Steinmetz, 2019, s. 240). Ønsket om å tilegne seg informasjon for å kunne avverge lovbrudd støter mot hensynet til befolkningens personvern. Burde politiet kunne motta informasjon om enkeltindivider lagret av tjenestetilbydere til forebyggende formål, selv om det er et inngripende tiltak i befolkningens personvern?

På spørsmål om hvordan han opplever samarbeidet med tjenestetilbydere svarer Richard/N:

> *«Det er utrolig varierende. I enkelte tilfeller så trengs det bare en mail og en halvtime etterpå så er det vi ønsker gjort. I andre tilfeller så er det veldig vanskelig for eksempel å få ut brukerinformasjon. For tjenestetilbyderen på sin side sitter jo og har ansvaret*

for folks opplysninger og personvern setter de høyt. Og så er det vi på den andre siden som trenger å vite hvem de er. Så det er jo ofte en utfordring og vanskelig, for det kan ta tid. Og så er det jo ofte i andre land da også.»

Bildet Richard/N skisserer av tjenestetilbyderens motvilje til å utgi informasjon om sine brukere, er ikke en særegen opplevelse for nettpatruljen. Yar og Steinmetz (2020, s. 245) identifiserer at politi ofte kan møte på tjenestetilbydere som ikke ønsker å utlevere informasjon om sine brukere. Dette kan blant annet være fordi det oppfattes negativt av tjenestens brukere at deres personlige opplysninger blir utlevert, og slik påvirke tjenestens omdømme (Yar og Steinmetz, 2020, s. 245). Hvis brukerne ikke føler at deres privatliv blir verdsatt, kan de kvie seg mot å bruke tjenesten og tilbyderne vil miste kunder. Det er ikke bare om tjenestetilbydere er villige til å utlevere informasjon som skaper problemer for samarbeidet, det gjør også deres muligheter for å oppbevare data. Erik/N hevder at: «*Spor slettes og forsvinner fort på internett*». Tjenestetilbyderenes lagringsmuligheter er omfattet av strenge tidsfrister, eksempelvis kan ikke en IP-adresse oppbevares i lenger enn 21 dager etter personopplysningsloven (2018). Dette krever at både politi og tjenestetilbydere må handle raskt. Regjeringen har i den siste tiden uttrykt et ønske om å forlenge muligheten for å oppbevare IP-adresser, det ligger i skrivende stund et lovforslag klart til høring i Stortinget (Regjeringen, 2020). Å forlenge tidsbegrensningen for lagring av IP-adresser vil kunne ha stor betydning for politiets håndtering av datakriminalitet og bedre samarbeidet mellom politi og tjenestetilbydere.

Bygrave og Michaelsen (2009, s. 92) understreker at det ikke finnes én enkelt aktør som styrer internett, internettkontrollen er fordelt mellom offentlige, private, gamle og nye aktører. Private aktører blir ikke bare ansvarliggjort til å gjennomføre tiltak for å gjøre internett til et tryggere sted, men politiet er også avhengig av dem for å kunne gjennomføre digitalt forebyggende politiarbeid. Et godt samarbeid mellom private aktører og politiet vil derfor være viktig i politiets forsøk for å gjøre krav på internett og effektivisere arbeidet med det.

7. Diskusjon

7.1 Oppsummering av oppgavens analyse

Oppgavens analysekapitler har sett på hvordan politiet gjennom nettpatruljen og Kripos driver digitalt forebyggende politiarbeid, samt undersøkt hvordan utviklingen av dette arbeidet blir påvirket av organisatoriske aspekter. Første analysekapittel tok sikte på å undersøke forebyggende tiltak i det digitale rom i konteksten av tradisjonelle forebyggende teorier. Oppgaven har vist at politiet er opptatt av å skape trygghet i det digitale rom gjennom å kommunisere og samhandle med publikum via sosiale medier, og trekker linjer til lokalorientert og beroligende politiarbeid. Det kommer frem at de ansatte opplever at tilstedeværelsen skaper tillit, som videre bidrar til å bryte ned barrierer. Nettpatruljens arbeid fremstår som svært publikumsrettet; mange av tiltakene nettpatruljen setter i gang er basert på informasjon de har mottatt direkte fra publikum, og de benytter seg strategisk av de ulike plattformene, ordlegging og innhold basert på hvilken målgruppe de ønsker å nå. Flere av de forebyggende tiltakene kan trekkes til strategien om ansvarliggjøring som Garland (1996, s. 452) presenterer. Oppgaven viser at nettpatruljen har et stort fokus på å skape bevissthet og gi potensielle ofre verktøy til å beskytte seg selv.

Følgende viser oppgaven hvordan Kripos tar i bruk situasjonelle kriminalitetstiltak for å drive digitalt politiarbeid, gjennom å blant annet administrere samlelister over domener som inneholder overgrepsmateriale. Også her kan strategier om ansvarliggjøring trekkes inn, politiet etablerer verktøy til private selskaper, og oppfordrer dem til å bidra til forebyggingen av datakriminalitet. Oppgaven har altså to ulike funn knyttet til ansvarliggjøring – det ene med formål om trygghet, det andre med formål om å redusere kriminalitet via situasjonelle tiltak. Den situasjonelle tankegangen kommer videre frem i tiltak hvor politiet retter advarende meldinger mot brukere som forsøker å laste ned overgrepsmateriale. Oppgaven viser også en opplevd mistro og mangel på tillit knyttet til datakriminalitet, i likhet med Riksrevisjonen (2021, s. 15) sine bemerkninger. I likhet med nettpatruljen jobber også Kripos med å skape en bevissthet rundt hvilke lovbrudd man kan bli utsatt for i det digitale rom. I tillegg til å undersøke de forebyggende tiltakene på nett opp mot tradisjonelle forebyggingsteorier, har oppgaven vist hvordan kriminalitet og forebygging som skjer på nett skiller seg ut fra mer tradisjonell kriminalitet og kontroll. Samtlige informanter tegnet et bilde av internett som en arena godt tilrettelagt for kriminalitet, og var åpne for at dette kunne skape utfordringer for det digitale forebyggende politiarbeidet. Informantene viser til en opplevelse om at det er lettere å begå

kriminalitet på nett, både fordi det er svært tilgjengelig og ikke tenkes å være like alvorlig som kriminalitet i den fysiske verden. Oppgaven viser til at muligheten til å holde seg anonym, det geografiske omfanget man kan nå og de tekniske omgivelsene ved internett skaper en sårbarhet både hos politi og borgere.

I andre analysekapittel ble politiets digitale forebyggende arbeid sett i lys av organisatoriske aspekter. Kapittelet åpnet med å se på utviklingen av digitalt politiarbeid i sammenheng med etablerte yrkeskulturer. Her kom det frem at de ansatte opplevde at politiet logget seg på nett for sent, og det ble vist til at utviklingen i Norge skjedde tregere enn andre sammenlignbare land både når det kom til opprettelsen av patruljer på nett og etableringen av et nasjonalt punkt for datakriminalitet. Eksisterende yrkeskulturer motvillige til endring innad i politiet blir tatt opp som en mulig årsak til tregheten i på denne utviklingen. Tanker om hva «ordentlig politiarbeid» skal bestå av strider tradisjonelt mot arbeidsoppgaver bestående av teknologiske eller forebyggende komponenter (Jewkes og Andrews, 2005; Lofthus, 2009; Gundhus, 2009). Videre kom det frem at informantene har observert en endring i kultur over tid, som trekker mot en større bevisstgjøring om hva digitalt politiarbeid består av innad i organisasjonen.

Følgende ble det trukket fram at omstruktureringer innad i organisasjonen fører til mindre fysisk interaksjon mellom politi og borger, og noen informanter innrømmer at det fysiske møtet er noe de savner i arbeidshverdagen. Samtidig kommer det frem at de ansatte opplever en forventing blant befolkningen om at politiet skal være tilgjengelige og tilstede på nett, og at de selv syntes det er viktig å møte befolkningen der de befinner seg. Oppgaven har vist at politiets tilstedeværelse på nett når lenger enn publikum som aktivt oppsøker politiets profiler på sosiale medier. Ved hjelp av tagge-funksjonen kan innbyggerne varsle politiet om støtende eller ulovlig innhold på sosiale medier, dette oppleves å virke avskrekkende. De ansatte opplever derimot at denne tilgjengeligheten kan medføre mye aktivitet, så mye at politiet ikke har ressurser til å behandle alle tips og henvendelser.

Analysen har vist at ved å bruke internett som kommunikasjonsplattform kan politiet nå ut til veldig mange på kort tid. Nettpatruljen Vest har en stor følgerskare, særlig på Tiktok, og denne går langt utover de geografiske grensene for politidistriktet. De kan nå store deler av befolkingen, alle med internettilgang, med jevne mellomrom, og som et resultat av dette skjer kontakten mellom politi og borger ikke lenger kun ved fysiske møter. I sammenheng med dette viser informantene til at denne rekkevidden, kombinert med de få ressursene som kreves for å lage et innlegg på sosiale medier, gjør at digitalt forebyggende politiarbeid er svært

ressurseffektivt sammenlignet med annet forebyggende politiarbeid, som for eksempel skolebesøk. Om den digitale forebyggingen er effektiv, avhenger derimot av hvor mange budskapet når frem til. Selv om politiet har mulighet til å nå utrolig mange, er det ikke en selvfølge at de faktisk gjør det. Oppgaven har vist at politiet er avhengig av å samle følgere og skape engasjement for å nå befolkningen. Dette reiser en ny problemstilling for politiet, som ellers i samfunnet innehar en iboende autoritet. Oppgaven har også vist at politiet har et tett samarbeid med politienheter i andre land ved utveksling av informasjon, samt bidrar i internasjonale forebyggingsaksjoner. I tillegg spiller private tjenestetilbydere en rolle i det trygghetsskapende arbeidet på internett. Det kommer frem at informantene opplever varierende hell i samarbeidet med disse.

Analysen viser at overgangen av forebygging fra gata til data skaper mange muligheter for det forebyggende arbeidet, men også flere utfordringer. Hvordan skal vi tenke rundt dette? Videre vil jeg trekke frem enkelte av oppgavens funn og diskutere hvordan disse kan forstås.

7.2 Et fjernere politi?

Kritikken mot nærpolitireformen fra 2015 går blant annet ut på at de gjennomgripende endringene i politiets organisering strider mot grunnprinsippene for politiets rolle i samfunnet (Larsson, 2017; Gundhus m.fl., 2018). Grunnprinsippene for politiets rolle i samfunnet ble fastsatt av politirollemeldingen fra 1981, og disse har vært en viktig grunnmur for utviklingen av det norske politiet. Ett av prinsippene som ble fastsatt er at politiet skal være integrert i lokalsamfunnet, og at denne integreringen burde skje gjennom både formell og uformell kontakt (NOU 1981:35, s. 80). Integrasjon er med på å skape et samspill mellom politi og publikum. Oppgaven viser at selv om reformen har skapt mindre fysisk kontakt med nærmiljøet, har den også bidratt til nye tjenester som også kan øke kontakten mellom politi og publikum. Lensmannskontorer og politistasjoner bidrar til nærhet mellom publikum og politiet, men er ikke det eneste virkemiddelet politiet kan ta i bruk for å komme nært folk (Justis- og beredskapsdepartementet, 2020, s. 41). Nettpatruljen kan være et ledd i å redusere den fysiske avstanden til politiet, som poengtert av informant Richard/Vest:

> «*Nettpatruljen kan jo komme inn og hvert fall hjelpe litt på den fysiske avstanden som er der. For uansett, så lenge du har internettilgang, kan du være hvor som helst og sende oss en melding.*»

Oppgavens funn viser hvordan samfunnets utvikling endres av sosiale samfunnskrefter. Å kommunisere med publikum via videoer og beskjeder på plattformer som TikTok og Facebook kan ved første øyekast virke som det stikk motsatte av idealet om nærhet og et lokalt forankret politi. I empirien kom det derimot frem at de ansatte i politiet syntes det var viktig å møte befolkningen der de er. Noen informanter fortalte om en forventing fra publikum til at de befant seg i det digitale rom, og følte på en lettelse for at de endelig kunne være tilstede på nett. I politirollemeldingen fastsettes det også at politiet skal avspeile samfunnets idealer, og at politiets virksomhet bør avspeile hovedprinsippene for vår samfunnsform (NOU 1981:35, s. 76). Når samfunnet endrer seg må politiet følge etter. I en verden hvor digitale virkemidler blir en stadig mer integrert del av vår hverdag, er politiet også nødt til å integrere det inn i deres rolle. Sosial handling blir løsrevet fra lokaliserte aktiviteter, og geografisk inndelte områder og fysiske steder er i følge Giddens (1997, s. 22) ikke lenger den fremste arenaen for sosial reproduksjon. Mange opplever større geografiske avstander til politiet fordi de ikke er like fysisk integrert i lokalsamfunnet som før. Samtidig viser empirien at politiet også føler at de har kommet nærmere publikum. Politiet kan ikke lenger treffes på bygdas lokale lensmannskontor, men de er alltid med deg i hånda, hvor enn du befinner deg. Kan den digitale tilstedeværelsen veie opp for noe av det som er mistet? Består et nært politi av mer enn bare fysisk nærhet?

Lokalsamfunnet har lenge spilt en sentral rolle i politiets arbeid, og tradisjonelt kriminalitetsforebyggende arbeid har gjennom tidene ofte tatt utgangspunkt i politiets tilstedeværelse i lokalmiljø (Gundhus, 2014, s. 187). Kriminalitetsforebygging er også en sosial struktur som har blitt løsrevet fra fysiske forankringer, kriminalitetsforebygging skjer ikke lenger kun gjennom fysisk tilstedeværelse i lokalmiljø og opprettelsen av nettpatruljer er et eksempel på dette. Empirien viser at politiet tar i bruk strategier og tanker som er karakteristiske for lokalorienterte forebyggingsstrategier uten å være fysisk tilstede i lokalmiljøer. Og mine informanter opplever å lykkes med det. De opplever å lykkes med å nå ut til befolkningen, de har tilegnet seg en enorm følgerskare på nett på kort tid. De opplever å lykkes med å knytte tette og uformelle bånd ved å kommunisere med publikum med digitale meldinger samt av det engasjement innleggende de publiserer skaper. De opplever å lykkes med å ta imot tips og forstå hva som rører seg i lokalsamfunnet, de følger med på positive og negative trender, og tips fra befolkningen danner grunnlaget for mye av arbeidet de gjør. Disse opplevelsene står i kontrast til funn i tidligere studier om forholdet mellom publikum og politi når den fysiske avstanden øker (Gundhus, Talberg og Wathne, 2018; Terpstra, 2018). Blant annet finner Gundhus,

Talberg og Wathne (2018, s. 216) at ansatte opplever å tape relasjoner med og innsikt i lokalmiljøer som følge av en større fysisk avstand. Den uformelle kontakten som bidrar til å skape en trygghet og kjennskap mellom politi og befolkning blir redusert. Oppgaven viser at det er flere sider ved forholdet mellom fysisk avstand og relasjoner til publikum, nærpolitireformen skaper ikke *utelukkende* flere relasjoner, men heller ikke *utelukkende* færre.

Oppgavens funn støtter samfunnsbetrakningene til Giddens (1997) og Harvey (1989), sosiale relasjoner og nærhet skapes ikke lenger kun gjennom fysisk samvær. Giddens (1997, s. 22) konstaterer at det har skjedd et skifte i hvordan og hvor sosiale strukturer blir reprodusert; sosiale relasjoner skapes og opprettholdes på nye plattformer. Harvey (1989, s. 204) hevder at konseptet tid og sted ikke lenger kan bli rammet inn av fysiske betingelser. Økt bruk av digitale kommunikasjonsløsninger har forandret betydningen av hva et samfunn er (Jones, 1998, s. 3), og videre endrer det arenaene politiet kan drive forebygging på. I dagens samfunn kan man ved hjelp av den teknologiske utviklingen reise gjennom tid og rom på et nanosekund, og vår opplevelse av nærhet blir følgende påvirket av dette. Vi er ikke lenger avhengig av å være fysisk nær noen for å føle en nærhet, dette kan føre til at behovet for å ha fysisk forankrede treffpunkter reduseres. Kan de nye teknologiene være en måte å kompensere for stadig lengre avstand mellom politi og samfunn? Politiet blir med digitaliseringen av tjenester kanskje et mer abstrakt politi som Terpstra, Fyfe og Salet (2019, s. 2) påpeker, men oppgaven viser at organisasjonen finner nye måter å møte og skape relasjoner med befolkningen.

Selv om vi ikke lenger er avhengig av fysisk nærhet betyr ikke det at behovet for dette faller helt bort. Castells (2010, s. 5) hevder at det fysiske samfunnet og det digitale er så sammenvevd at det er umulig å skille det ene fra det andre. I datamaterialet kom det også frem at noen informanter savnet å være i fysisk kontakt med ungdommene, og at viktige momenter ved forebyggingen, som å lese kroppsspråk, gikk tapt. De digitalt forebyggende tiltakene identifisert i oppgaven kan vise til at heller ikke datakriminalitet er fullstendig løsrevet fra lokalsamfunnet. I intervjuene kom det eksempelvis frem at nettpatruljen bruker mye tid på å informere om hvilke handlinger som er ulovlige på nett, som for eksempel å dele uønskede nakenbilder. Uønsket bildedeling kan skje mellom ukjente, men også blant mennesker i samme lokalsamfunn. Videre kom det også frem at mye av det forebyggende fokuset til Kripos var basert på samarbeid med, og informasjon fra utenlandske politienheter, om kriminalitet som strakk seg over landegrenser. Kriminalitet er ikke nødvendigvis *enten* lokalt *eller* digitalt. Selv om datakriminalitet med sin grenseløse natur kan skje over store geografiske områder, betyr det ikke at den alltid gjør det.

Datakriminalitet består av et mylder av handlinger av ulik karakter, som derfor gjør forebyggingen av den kompleks og utfordrende.

7.3 Kommunikasjon, legitimitet og tillit

Av oppgavens datamateriale kommer det til syne at politiet kommuniserer med befolkningen på nye måter enn før i et forsøk på å skape tillit, og fremme legitimitet og politiets omdømme. Legitimitet er et viktig element i autoriteten politiet innehar blant befolkningen, hvis befolkningen opplever politiets makt som legitim blir de i følge Hough, Bradford og Jackson (2017, s. 277) normativt knyttet til å følge deres regler. Politiet har lenge fokusert på å drive ikke-operasjonell kommunikasjon med publikum, for å selv kontrollere hvilken informasjon publikum får om deres tjenester (Mawby, 2002, s. 54). Det som derimot er nytt er hvordan de tar i bruk sosiale medier for å informere, gi råd og drive relasjonsbygging med innbyggerne. Denne nye formen for kommunikasjon fører til at politiet må utøve oppgavene sine og skape tillit hos befolkningen på nye måter. Ifølge Lee og McGovern (2014, s. 114) blir kommunikasjon mellom publikum og politi mer uformell via sosiale medier enn via andre, mer tradisjonelle kommunikasjonsløsninger. Nettpatruljens kommunikasjon med befolkningen via sosiale medier har vist seg å bestå av en blanding av informativt og underholdende innhold. Politiet blir en del av livet på sosiale medier og slik en del av befolkningens daglige dose med sosiale medier, og befinner seg bare et tastetrykk unna. Politiets tilstedeværelse på nett kan ifølge Lee og McGovern (2014, s. 131) ufarliggjøre politiet, og slik bryte ned barrierer mellom politi og samfunn. Den digitale forebyggingen blir en form for kommunikasjon, og gjennom denne bygger politiet tillit og trygghet sammen med innbyggerne. Den åpne og uformelle to-veis kommunikasjonen mellom innbyggere og politi som skapes ved hjelp av sosiale medier, er et verdifullt verktøy som kan bidra til en større åpenhet mellom politi og borger.

Endringen i kommunikasjon viser hvordan politiet adapterer til å leve i den digitale verden. Det er ikke bare de kriminelle som kan utnytte internetts grenseløshet, oppgaven viser at politiet kan nå langt utenfor sitt distrikt med det forbyggende innholdet de skaper. Nettpatruljen representerer en helt ny måte for politiet å være tilgjengelig på, en polititjeneste som til enhver tid er innen rekkevidde, hvor enn i landet (og verden) man befinner seg. Som et resultat av dette, er ikke forholdet mellom politiet, media og publikum det samme som før (Lee og McGovern, 2014, s. 114). Politiet er ikke lenger passive formidlere gjennom tradisjonelle medier som aviser og TV, de spiller en aktiv rolle i kommunikasjonen med og formidlingen av budskap til borgerne. Å bygge tillit blant befolkningen til politiets kompetanse er et virkemiddel

de kan ta i bruk for å oppnå legitimitet (Hough, Bradford og Jackson, 2017, s. 277). Informanter fra både nettpatruljen og Kripos skisserer en opplevd forventning blant befolkningen om at politiet skal være tilstede og kontrollere internett. Ved å være en aktiv formidler på sosiale medier, og vise at de tar datakriminalitet på alvor, kan politiet oppfylle forventningene befolkningen har til deres håndtering av det digitale rom. Som nevnt i oppgavens teorikapittel viser resultater fra en undersøkelse gjennomført av NorSIS (2019) at befolkningens tillit til politiets håndtering av kriminalitet som skjer på nett er lav. Internett er derfor en arena politiet må prioritere, de må spille en aktiv rolle i det trygghetsskapende arbeidet på nett for å vise frem sin kompetanse og forsterke sin egen legitimitet.

7.4 Et digitalt politi

Oppgaven viser at selv om etablerte yrkeskulturer og oppfatninger om hva politiarbeid er har vært fremtredende i utviklingen av digitalt forebyggende politiarbeid, kan det økte fokuset på et digitalt politi ha satt i gang en endringsprosess. Informantene observerte holdningsendringer over tid, et premiss som må til for at politiet skal kunne fortsette å benytte seg av mulighetene den digitale verden kan gi. Funnene viser til at politiet sakte, men sikkert, integreres inn i den digitale verden. Som tidligere vist i oppgavens teori og analysekapittel, blir yrkeskulturer innad i politiet reprodusert over tid og oppleves å være motvillige for endring (Lofthus, 2009; Jewkes og Andrews, 2005; Gundhus, 2009). Lofthus (2009, s. 199) illustrerer at så lenge politiets fundamentale rolle i samfunnet fremdeles er den samme, vil kulturene innad i yrket fortsette å støte i mot nye endringer. Om innføringen av digitalt forebyggende politiarbeid i seg selv er nok til å endre etablerte yrkeskulturer i et tradisjonsrikt yrke som politiet, kan ikke denne oppgavens empiri svare på. Oppgavens bidrag kan derimot vise at holdningsendringer knyttet til moderne politiarbeid, som patruljering av internett og arbeid med «usynlig» kriminalitet på nett, er mulig. Dette funnet kan trekkes til tidligere funn gjort om påvirkningen av teknologi innad i politiyrket (Chan, 2001; Chan, 2003). Chan (2001, s. 157) fant i sin studie at politiet ikke har et annet valg enn å godta de teknologiske endringene, på grunn av den determinerende kraften det digitale samfunnet har. Hun hevder at de teknologibaserte endringene i politiyrket vil gradvis og kontinuerlig ha en påvirkning på de dypt forankrede yrkeskulturene (Chan, 2001, s. 157). Funnene i denne oppgaven viser til at prediksjonene Chan presenterte for 20 år siden om teknologiens påvirkning på politiyrket, ikke strider langt fra hvordan denne utviklingen har skjedd. Er de teknososiale samfunnskreftene sterke nok til å over tid kunne endre oppfatningen av hva «ordentlig politiarbeid» er?

8. Avslutning

Denne oppgaven har sett på hvordan politiet driver digitalt forebyggende politiarbeid, samt hvordan de forsøker å skape trygghet i det digitale rom. Tradisjonelle teorier knyttet til forebygging som lokalorientert forebygging har vist seg synlige i informantenes skildringer av de forebyggende innsatsene de setter i gang. Tradisjonelle lokalorienterte forebyggingsstrategier tar utgangspunkt i politiets fysiske tilstedeværelse i lokalsamfunnet, men oppgaven har vist at politiet opplever å oppnå en nærhet til publikum også gjennom det digitale, til tross for at den fysiske avstanden kan ha økt. Slik har oppgaven vist til en endring i samfunnet, vi er ikke lenger avhengig av å være fysisk nær hverandre for å oppleve nærhet. Vår forståelse av hva et lokalmiljø er burde således utvides til å også omfatte det virtuelle. Videre har oppgaven vist at politiet forsøker å skape trygghet i det digitale rom gjennom tilstedeværelse og tilgjengelighet. Nettpatruljen representerer et nytt type politi, et politi du kan ha med deg i hånda og bygge relasjoner med, så lenge du har internettdekning.

Det digitale forebyggende politiarbeidet består av mer enn bare tilstedeværelse og patruljering av sosiale medier. Oppgaven viser at Kripos utnytter de tekniske omgivelsene for å forebygge kriminalitet, en strategi som kan trekkes mot tradisjonelle teorier om situasjonell forebygging. Politiet forsøker å redusere de faktiske mulighetene for kriminalitet ved å kartlegge nettsider som består av ulovlig innhold og fjerne mulig skadevare fra utsatte datamaskiner. Videre forsøker de å øke sjansene for å bli oppdaget, i hvert fall den opplevde oppdagelsesfaren, gjennom å omadressere trafikk til nettsider som kan inneholde kriminell aktivitet og produsere og sende ut advarende meldinger. Utviklingen av det digitalt forebyggende politiarbeidet har blitt sett i lys av organisatoriske aspekter. Funnene viser at digitalt forebyggende politiarbeid kan være en effektiv form for forebygging, det er mulig å nå veldig mange på kort tid ved bruk av få ressurser. Oppgaven har også funnet at holdninger innad i organisasjonen om politiets rolle i den virtuelle verden tilsynelatende har endret seg over tid, et tegn på at de digitale samfunnsendringene er så grunnleggende og kraftige at tradisjonelle oppfatninger av hva politiarbeidet burde bestå av ikke klarer å stå imot.

Kommunikasjon har vist seg å være et viktig element i det digitale forebyggende politiarbeidet. Gjennom tilstedeværelsen på sosiale medier inntar politiet en aktiv rolle i kommunikasjonen mellom politi og borger, i et forsøk på å skape tillit og fremme legitimitet. På bakgrunn av retningen verden beveger seg i er det ingen tvil om at politiet er avhengig av å ha digitale

løsninger, ikke bare for å kommunisere med publikum, men også for å skape og opprettholde relasjoner. Betydningen av etablerte digitale kommunikasjonsløsninger mellom politi og befolkning kom spesielt til syne da store deler av samfunnet stengte ned i mars 2020 som et resultat av Covid-19 pandemien. De relasjonene og arenaene som ellers foregår fysisk, ble alle tvunget til å avsluttes eller konvertere til digitale løsninger. Bruken av, og behovet for digital samhandling i samfunnet økte kraftig, og politiets tjenester var intet unntak (Justis- og beredskapsdepartementet, 2020, s. 36). Verdien av å ha et politi som kan nås utover nødnumre og fysiske kontorer har blitt avdekket ytterligere i pandemiens tid.

Et pålogga politi har vist seg å være et politi som skaper tilstedeværelse og nærhet på digitale plattformer, som finner nye måter å kommunisere med befolkningen på, og som legger ned en iherdig innsats i å forsøke å gjøre internett til et tryggere sted for alle. Samtidig er det også et politi som møter på mange utfordringer ved å være logget på nett. Spørsmålet videre blir hvordan politiet velger å utvikle de digitalt forebyggende tjenestene, og hvilke ambisjoner de har for å forsøke å få kontroll på internett. Det digitale samfunnet fortsetter å utvikle seg, og kriminalitetsutfordringene politiet møter på nett er kommet for å bli. Politiet er nødt til å utvikle seg i takt med de digitale endringene for å kunne beskytte samfunnet mot farene internett bringer med seg, for som Jonas/K påpeker: «*Står vi bare stille med hendene i lomma så skjer det ingenting ikke sant, vi må alltid pushe det*».

8.1 Videre forskning

Denne oppgaven har tatt for seg hvordan ansatte opplever å arbeide digitalt forebyggende. Forebygging av datakriminalitet og forebyggende tiltak utført ved bruk av sosiale medier er et felt det er gjort lite forskning på i norsk sammenheng. Som Riksrevisjonen (2021, s. 5) påpeker går andelen lovbrudd begått ved hjelp av internett og digitale verktøy opp, mens andelen av mye annen kriminalitet går ned. Det finnes derfor et stort behov for å opparbeide kunnskap om hvordan politiet kan avverge denne typen kriminalitet. Som oppgaven har vist gir også sosiale medier politiet unike muligheter til å bygge relasjoner og kommunisere med befolkningen. Det vil derfor være hensiktsmessig å forske på hvordan politiet best mulig kan utnytte disse mulighetene, fra et kriminologisk eller medievitenskapelig standpunkt, men også i forhold til befolkningens egen oppfatning av forebygging ved hjelp av sosiale medier.

Antall ord: 38 044

Litteraturliste

Aas, K. F. (2006) "Ta vare på deg selv, lommeboka, mobilen og dine venner", i Eriksen, T. H. (red.) *Trygghet.* 1. Utg. Oslo: Universitetsforlaget, s. 73-96.

Aas, K. F. (2007) Beyond 'the desert of the real': crime control in a virtual(ised) reality, i Jewkes, Y. (red) *Crime online.* 1. Utg. Cullompton: Willian Publishing, s. 160-178.

Abeele, M. V., de Wolf, R. og Ling, R. (2018) Mobile Media and Social Space: How Anytime, Anyplace Connectivity Structures Everyday Life. *Rethinking Media and Social Space*, 6(2), s. 5-14.
https://doi.org/10.17645/mac.v6i2.1399

Algaith, A., Gashi, I., Sobesto, B., Cukier, M., Haxhijaha, S., & Bajrami, G. (2016) Comparing detection capabilities of antivirus prod- ucts: An empirical study with different versions of products from the same vendors. *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W), s.* 48–53.
https://doi.org/10.1109/DSN-W.2016.45.

Appadurai, A. (1996) *Modernity at Large - Cultural Dimensions of Globalization.* 1. Utg. Minneapolis: University of Minnesota Press

Arnø, M.T. (2021) *Norske TikTok-profiler raser mot Vest politidistrikt.* Tilgjengelig fra: https://www.kom24.no/debatt-jonas-andersen-nettpatruljen/norske-tiktok-profiler-raser-mot-vest-politidistrikt/349098 Lest 23.05.21.

Bakketeig, E. (2001) HVORFOR ER FELTET SEKSUELLE OVERGREP MOT BARN PREGET AV STEREOTYPE OPPFATNINGER?. *Nordisk Tidsskrift for Kriminalvidenskab,* 88(4), s. 337-349.

Bennet, S., Maton, K. og Kervin, L. (2008) The 'Digital Natives' Debate: A Critical Review of the Evidence. *British Journal of Educational Technology,* 39(5), s. 775-786.
DOI: 10.1111/j.1467-8535.2007.00793.x

Bjørgo, T. (2015) *Forebygging av kriminalitet.* 1. Utg. Oslo: Universitetsforlaget.

Blakemore, B. (2012) Cyberspace, Cyber Crime and Cyber Terrorism, i Awan, I. og Blakemore, B (red.) *Policing Cyber Hate, Cyber Threats and Cyber terrorism.* 1. Utg. Farnham: Ashgate, s. 5-20.

Bonneau, J. (2012) The science of guessing: Analyzing an anonymized corpus of 70 million passwords. *2012 IEEE Symposium on Security and Privacy*, s. 538–552.
https://doi.org/10.1109/SP.2012.49

Bowling, B., Reiner, R. og Sheptycki, J. (2019) *The politics of the police.* 5. Utg. Oxford: Oxford University Press.

Boyd, D. and Crawford, K. (2012) Critical questions for Big Data: Provocations for a cultural, technological and scholarly phenomenon. *Information, Communication and Society*, 15(5), s. 662–679.
https://doi-org.ezproxy.uio.no/10.1080/1369118X.2012.678878

Boyle, J. (1997) Foucault In Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors. *University of Cincinnati Law Review*, 66, s. 177-205.

Bygrave, L. A og Michaelsen, T. (2009) Governers of Internet, i Bygrave, L. A og Bing, J. (red.) *Internet Governance.* 1. Utg. Oxford: Oxford University Press, s. 92-125.

Bradford, B. (2014) Policing and social identity: procedural justice, inclusion and cooperation between police and public, *Policing and Society*, 24(1), s. 22-43.
DOI: 10.1080/10439463.2012.724068

Braithwaite, J. (2000) The New Regulatory State and the Transformation of Criminology. *British journal of criminology*, 40(2), s. 222-238.
https://doi.org/10.1093/bjc/40.2.222

Brenner, S. W. (2007) Cybercrime: re-thinking crime control strategies, i Jewkes, Y. (red) *Crime online.* 1. Utg. Cullompton: Willian Publishing, s. 12-28.

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., Maimon, D. (2019) *Cybercrime Prevention: Theory and applications.* 1. Utg. Palgrave Macmillan

Bullock, K. og Fielding, N. (2017) Community crime prevention, i Tilley, N. og Sidebottom, A. (red.) *Handbook of Crime Prevention and Community Safety.* 2. Utg. Abingdon: Routledge, s. 57-86.

Calderoni, F. (2010) The European legal framework on cybercrime: Striving for an effective implementation. *Crime, Law and Social Change*, 54, s. 339–357.
DOI: 10.1007/s10611-010-9261-6

Castells, M. (2010) *The rise of the network society: The information age: Economy, society, and culture.* 2. Utg. West Sussex: Wiley-Blackwell.

Chan, J. (2001) The technological game : how information technology is transforming police practice. *Criminal Justice*, 1(2), s. 139–159.
https://doi-org.ezproxy.uio.no/10.1177/1466802501001002001

Chan, J. (2003) Police and new technologies, i Newburn, T. (red.) *Handbook for policing*. 1. Utg. Cullompton: Willan Publishing, s. 655–679.

Christensen, T. Lægreid, P. og Rykkja, L. H. (2017) Reforming the Norwegian police between structure and culture: Community police or emergency police. *Public Policy and Administration.* 33(3), s. 241–259.
https://doi-org.ezproxy.uio.no/10.1177/0952076717709523

Clarke, R. V. G. (1980) "Situational" crime prevention: Theory and practice. *The British journal of Criminology*, 20(2), s. 136 – 147.
https://doi.org/10.1093/oxfordjournals.bjc.a047153

Crawford, A. (2006) Networked governance and the post-regulatory state?: Steering, rowing and anchoring the provision of policing and security. *Theoretical criminology*, 10(4), s. 449-479.

Ellingsen, D. og Lilleaas, U-B. (2020) Ekskluderende maskulinitetskulturer i en mannsbastion – belyst gjennom et norsk politidistrikt. *Søkelys på arbeidslivet*, 37(4), s. 285-298.
https://doi.org/10.18261/issn.1504-7989-2020-04-05

Egge, M. Og Gundus, H.O. (2012) "Social crime prevention in Norway", i Baillergeau, E. og Hebberec, P (red) *Social Crime Prevention in Late Modern Europe : A Comparative Perspective*. 1. Utg. Brüssel: VUB Press, s. 255-277.

Ericsson, K. (2000) Maskulinitet, kriminalitet og kontroll. *Materialisten*, 28(4), s. 7-43.
https://doi-org.ezproxy.uio.no/10.1080/14043850601010422

Eriksen, T. H. (2014) *Globalization.* 2. Utg. New York: Taylor & Francis Ltd.

Finstad, L. (2018) *Hva er politi*. 1. Utg. Oslo: Universitetsforlaget.

Foss, M. S. (2020) Gode skoleresultater – liten endring i yrkesvalg. *SSB analyse 2020/02: Kvinner og realfag.* Tilgjengelig fra: https://www.ssb.no/utdanning/artikler-og-publikasjoner/gode-skoleresultater-liten-endring-i-yrkesvalg

Franko, K. (2020) *Globalization and Crime.* 3. Utg. London: SAGE Publications.

Garland, D. (1996) The Limits of the Sovereign State. Strategies of Crime Control in Contemporary Society. *The British Journal of Criminology*, 36(4), s. 445-471.
https://doi.org/10.1093/oxfordjournals.bjc.a014105

Giddens, A. (1984) *The Constitution of Society.* 1. Utg. Cambridge: Polity Press.

Giddens, A. (1997) *Modernitetens konsekvenser.* Oversatt fra The Consequences of Modernity av Eriksen, A. Oslo: Pax Forlag, 1. Utg.

Gill, M. (2019) Series Editor´s Preface, i *Cybercrime Prevention: Theory and applications.* 1. Utg. Cham: Palgrave Macmillan, s. v-vi.

Gilling, D. (1997) *Crime prevention: Theory, policy and politics.* 2. Utg. London: Routledge.

Goldstein, H. (1979) Improving Policing: A Problem-Oriented Approach. *Crime and delinquency*, 25(2), s. 236-258.
DOI: 10.1177/001112877902500207

Grabosky, P. N. (2001) Virtual Criminality: Old Wine in New Bottles? *Social & legal studies*, 10(2), s. 243-249.
DOI: 10.1177/a017405

Gundhus, H. O. I. (2006) *"For sikkerhets skyld" IKT, yrkeskulturer og kunnskapsarbeid i politiet*. Doktoravhandling. Oslo: Universitetet i Oslo.

Gundhus, H. O. I. (2009). *For sikkerhets skyld: IKT, yrkeskulturer og kunnskapsarbeid i politiet*. Oslo: Unipub.

Gundhus, H. O. I. (2012) Experience or Knowledge? Perspectives on New Knowledge Regimes and Control of Police Professionalism. *Policing*, 7(2), s. 178–194. DOI: 10.1093/police/pas039

Gundhus, H. O. I. (2014) Forebyggende arbeid, i Larsson, P., i Gundhus, H. O. I og Granér, R. (red.) *Innføring i politivitenskap.* 1. Utg. Oslo: Cappelen Damm akademisk, s. 178 - 204.

Gundhus, H. O. I. og Larsson, P. (2014) Fremtidens politi, i Larsson, P., Gundhus, H. O. I og Granér, R. (red.) *Innføring i politivitenskap.* 1. Utg. Oslo: Cappelen Damm akademisk, s. 273-302.

Gundhus, H. O. I., Talberg, N. og Wathne, C. T. (2018) Konturene av en ny politirolle: politiansattes erfaringer med Nærpolitireformen, i Sørli, V. L. og Larsson, P. (red.) *Politireformer – Idealer, realiteter, retorikk og praksis.* 1. Utg. Oslo: Cappelen Damm Akademisk, s. 199-222.

Gundhus, H. O. I., Larsson, P. Sørli, V. L., Talberg, N., Wathne, C. T. (2018) Nærpolitiidealet under press, i Sørli, V. L. og Larsson, P. (red.) *Politireformer – Idealer, realiteter, retorikk og praksis.* 1. Utg. Oslo: Cappelen Damm Akademisk, s. 341-365.

Gundhus, H. O. I., Talberg, N. og Wathne, C. T. (2019) Politiskjønnet under press, i Sunde, I. M og Sunde, N. (red.) *Det digitale er et hurtigtog.* Bergen: Fagbokforlaget, s. 83-113.

Harvey, D. (1989) *The Condition of Postmodernity.* 1. Utg. Cambridge: Blackwell Publishers.

Holmberg, L. (2014) Hva gjør politiet?, i Larsson, P., Gundhus, H.O.I og Granér, R. (red.) *Innføring i politivitenskap.* 1. Utg. Oslo: Cappelen Damm akademisk, s. 153-177.

Holt, T. J. (2019) Computer Hacking and the Hacker Subculture, i Holt, T. J. og Bossler, A. M. (red.) *The Palgrave Handbook of International Cybercrime and Cyberdeviance.* 1. Utg. Cham: Palgrave Macmillan.

Hough, M. Bradford, B. og Jackson, J. (2017) Policing, procedural justice and prevention, i Tilley, N. og Sidebottom, A. (red.) *Handbook of Crime Prevention and Community Safety.* 2. Utg. Abingdon: Routledge, s. 274-293.

Hutchings, A. Clayton, R. og Anderson, R. (2016) Taking Down Websites to Prevent Crime. *2016 APWG Symposium on Electronic Crime Research (eCrime)*. DOI: 10.1109/ECRIME.2016.7487947

Interpol (2021) *Blocking and categorizing content*. Tilgjengelig fra: https://www.interpol.int/Crimes/Crimes-against-children/Blocking-and-categorizing-content Lest 04.04.21.

Intravia, J., Wolff, K. T og Piquero, A. R. (2018) Investigating the Effects of Media Consumption on Attitudes Toward Police Legitimacy. *Deviant Behavior*, 39(8), s. 963-980. DOI: 10.1080/01639625.2017.1343038

Jensen, E. Og Stubberud, R. (2011) *Alt starter og avsluttes med et håndtrykk.* Oslo: Oslo Politidistrikt.

Jewkes, Y. og Andrews, C. (2005) Policing the filth: The problems of investigating online child pornography in England and Wales. *Policing and Society*, 15(1), s. 42-62. DOI: 10.1080/1043946042000338922

Jewkes, Y. (2007) 'Killed by the Internet': cyber homicides, cyber suicides and cyber sex crimes, i Jewkes, Y. (red.) *Crime online.* 1. Utg. Cullompton: Willian Publishing, s. 1-11.

Johannessen, L. E., Rafoss, T. W. og Rasmussen, E. B. (2020) *Hvordan bruke teori?* 1. Utg. Oslo: Universitetsforlaget.

Jones, S. (1998) *Cybersociety 2.0: Revisiting Computer-Mediated Communication and Community*. Thousand Oaks: Sage Publications.

Jones, T. og Newburn, T. (1998) *Private Security and Public Policing*. 1. Utg. Oxford: Claredon Press.

Jones, M. R. og Karsten, H. (2008) Giddens's Structuration Theory and Information Systems Research. *MIS Quarterly*, 32(1), s. 127-157.

Justis- og Beredskapsdepartementet (2015) *Endringer i politiloven mv. (trygghet i hverdagen – nærpolitireformen)*. (2014-2015). Proposisjon til Stortinget 61. Oslo: Justis- og Beredskapsdepartementet.

Justis- og Beredskapsdepartementet (2019) *Handlingsplan mot voldtekt 2019-2022*. Oslo: Justis- og Beredskapsdepartementet.

Justis- og Beredskapsdepartementet (2020) *Politimeldingen – et politi for fremtiden*. (2019-2020). Stortingsmelding 29. Oslo: Justis- og Beredskapsdepartementet.

Karaian, L. (2014) Policing 'sexting': Responsibilization, respectability and sexual subjectivity in child protection/ crime prevention responses to teenagers' digital sexual expression. *Theoretical Criminology*, 18(3), s. 282–299. DOI: 10.1177/1362480613504331

Kelling, G. L., & Wilson, J. Q. (1982) Broken windows: The police and neighborhood safety. *The Atlantic*, March 1.

Knutsson, J. og Søvik, K. (2005) *Problemorientert politiarbeid i teori og praksis*. Oslo: Politihøgskolen.

Konvensjon om datakriminalitet (2006) *Konvensjon om datakriminalitet – ETS nr. 185.*

Kvale, S. (2007) *Doing interviews.* 1. Utg. London: SAGE.

Kvale, S. og Birkmann, S. (2017*) Det kvalitative forskningsintervju.* Oversatt fra InterView: Learning the Craft og Qualitative Research Interviewing av Anderssen, T. M. og Rygge, J. 3. Utg. Oslo: Gyldendal Akademisk.

Lab, S. P. (2020) *Crime Prevention: approaches, practices, and evaluations.* 10. Utg. London: Routledge.

Larsson, P. (2017) From Integration to Contact. *Nordisk politiforskning*, 4(2), s. 170-186. DOI: https://doi.org/10.18261

Larsson, P. og Sørli, V. L. (2018) Reformer i politiet, i Sørli, V. L. og Larsson, P. (red.) *Politireformer – Idealer, realiteter, retorikk og praksis.* 1. Utg. Oslo: Cappelen Damm Akademisk, s. 15-34.

Lee, M. og McGovern, A. (2014) *Policing Media.* 1. Utg. New York: Routledge.

Leishman, F. og Mason, P. (2003) *Policing and the Media: Facts, Fictions and Factions*. 1. Utg. Cullompton: Willan.

Lessig, L. (1999) *Code and Other Laws of Cyberspace.* 1. Utg. New York: Basic Books.

Lie, E. M. (2011) I forkant. 1. Utg. Oslo: Gyldendal Akademisk.

Loader, I. og Walker, N. (2007) *Civilizing Security*. 1. Utg. Cambridge: Cambridge University Press.

Loftus, B. (2009) *Police Culture in a Changing World.* 1. Utg. Oxford: Oxford University Press.

Lomell, H. M (2017) Kriminalstatistikk, i Lomell, H. M og Skilbrei, M. (red.) *Kriminologi.* 1. Utg. Oslo: Universitetsforlaget, s. 29-54.

Lyon, D. (2014) Surveillance, Snowden, and Big Data: Capacities, consequences, critique**.** *Big Data Society*, 1(2), s. 1-13.
DOI: 10.1177/2053951714541861

Maimon, D., Alper, M., Sobesto, B. og Cukier, M. (2014) Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology*, 52(1), s. 33-59.
DOI: 10.1111/1745-9125.12028

Mason, J. (2018) *Qualitative research*. 3. Utg. Los Angeles: SAGE.

Mawby, R. C. (2002) *Policing Images: Policing, communication and legitimacy.* 1. Utg. Cullompton: Willan Publishing.

Mcculloch, J. og Pickering, S. (2009) Pre-Crime and Counter-Terrorism. Imagining Future Crime in the 'War on Terror'. *British Journal of Criminology*, 49(5), s. 628-645.
https://doi.org/10.1093/bjc/azp023

McGuire, M. (2007) *Hypercrime. The New Geometry of Harm*. 1. Utg. Abingdon: Routledge.

Menesini, E., Nocentini, A. og Palladino, B. E. (2016) Cyberbullying: conceptual, theoretical and methodological issues, i Völlink, T., Dehue, F. og McGuckin, Conor (red.) Cyberbullying: From theory to intervention. 1. Utg. London: Routledge, s. 15-25.

Miró-Llinares, F. og Moneva, A. (2020) Environmental Criminology and Cybercrime: Shifting Focus from the Wine to the Bottles, i Holt, T.J. og Bossler, A. M. (red.) *The Palgrave Handbook of International Cybercrime and Cyberdeviance.* 1. Utg. Cham: Palgrave Macmillan, s. 491-511.

Moore, T. og Clayton, R. (2008) The Impact of Incentives on Notice and Take-down, i Johnson, E. M. (red.) *Managing Information Risk and the Economics of Security.* 1. Utg. New York: Springer, s. 199-223.

Nettgruppen (2013) *Tilgjengelige, Tøffe Og Trygge?* Oslo: SaLTo, Feltteamet Alna og Redd Barna.

Newburn, T. (2013) *Criminology.* 2. Utg. London: Routledge

NorSIS. (2019) *Nordmenn og digital sikkerhetskultur 2019.*

NOU 1981:35. *Politiets rolle i samfunnet. Delutredning 1.*

NSD (2021) *Samtykke og andre behandlingsgrunnlag.* Tilgjengelig fra: https://www.nsd.no/personverntjenester/oppslagsverk-for-personvern-i-forskning/samtykke-og-andre-behandlingsgrunnlag/ Lest 04.04.21.

Paulsen, J. E. (2019) Holdninger til høyteknologi, i Sunde, I. M og Sunde, N. (red.) *Det digitale er et hurtigtog.* 1. Utg. Bergen: Fagbokforlaget, s. 23-48.

Payne, B. (2019) Defining Cybercrime, i Holt, T. J. og Bossler, A. M. (red.) *The Palgrave Handbook of International Cybercrime and Cyberdeviance.* 1. Utg. Cham: Palgrave Macmillan, s. 3-26.

Personopplysningsloven (2018) *Lov om behandling av personopplysninger*.

Petersson, O. (2014) Hvem er politiet? i Larsson, P., i Gundhus, H. O. I og Granér, R. (red.) *Innføring i politivitenskap.* 1. Utg. Oslo: Cappelen Damm akademisk, s. 110-133.

Pettersen, L. (2018) Digitalisering - modernitetens flyttebyrå. *Norsk medietidsskrift*, 2018 (4), s. 1-17. https://doi.org/10.18261/ISSN.0805-9535-2018-04-03

Politidirektoratet (2012) *Politiet i det digitale samfunnet : en arbeidsgrupperapport om elektroniske spor, IKT-kriminalitet og politiarbeid på internett.*

Politidirektoratet (2015) *Datakrimstrategien.*

Politidirektoratet (2017) *Politiet mot 2025.*

Politidirektoratet (2020) *I forkant av kriminaliteten.*

Politiet (2020) *Politiets nettpatrulje.* Tilgjengelig fra: https://www.politiet.no/rad/trygg-nettbruk/politiets-nettpatrulje/. Lest 01.02.2021.

Politiet (2021a) *Dette arbeider Kripos med.* Tilgjengelig fra: https://www.politiet.no/om/organisasjonen/sarorganene/kripos/kripos-hovedarbeidsomrader/ Lest: 22.04.21.

Politiet (2021b) *Datakriminalitet*. Tilgjengelig fra: https://www.politiet.no/rad/datakriminalitet/ Lest 14.06.21.

Powell, A., Stratton, G. og Cameron, R. (2018) *Digital Criminology.* 1. Utg. Routledge.

PST (2014) *Åpen trusselvurdering 2014*. Oslo: Politiets sikkerhetstjeneste.

Regjeringen (2020) *Vil lagre IP-adresser for å oppklare og hindre overgrep.* Tilgjengelig fra: https://www.regjeringen.no/no/aktuelt/vil-lagre-ip-adresser-for-a-oppklare-og-hindre-overgrep/id2769943/ Lest 21.06.21.

Renaud , K., Orgeron, C., Warkentin, M. P. og French, E. (2020) Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China. *Public Administration Review*, 80(4), s. 577-589. https://doi.org/10.1111/puar.13210

Rice, R. E, Yates, S.J. og Blejmar, J.(2020). Introduction to the Oxford Handbook of Digital Technology and Society: Terms, Domains, and Themes, i Rice, R. E og Yates, S. J. (red) *The Oxford Handbook of Digital Technology and Society*. 1. Utg. Oxford University Press, s. 4-34.

Riksrevisjonen (2021) *Undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT.*

Sandstrom, G. M. & Dunn, E. W. (2014) Social Interactions and Well-Being: The Surprising Power of Weak Ties. *Personality and Social Psychology Bulletin*, 40(7), s. 910-922. https://doi-org.ezproxy.uio.no/10.1177/0146167214529799

Santos, I. N. og Azevedo, J. (2019) *Space-time compression and hyperlocalisation: the new flâneurs. Comunicação e Sociedade,* 35, s. 259 – 277. http://dx.doi.org/10.17231/comsoc.35(2019).3142

Schjetne, S. (2019) *Politifolk fortviler: Nærpolitireformen skaper et fjernere politi.* Tilgjengelig fra: https://forskning.no/ntb-politi-politikk/politifolk-fortviler-naerpolitireformen-skaper-et-fjernere-politi/1323818 Lest 04.06.21.

Schneider, C. J. (2016) *Policing and Social Media.* 1. Utg. Lanham: Lexington books.

Selzer, N and Sebastian Oelrich, S. (2021) Saint or Satan? Moral Development and Dark Triad Influences on Cybercriminal Intent, i Kranenbarg, M. W. og Leukfeldt, R. (red.) *Cybercrime in Context.* Amsterdam: Springer International Publishing, s. 175-194.

Shakya, H. B. og Christakis, N. A. (2017) Association of Facebook Use With Compromised Well-Being: A Longitudinal Study. *American Journal of Epidemiology*, 185(3), s. 203–211. https://doi.org/10.1093/aje/kww189

Shields, R. (1996) Introduction: Virtual Spaces, Real Histories and Living Bodies, i Shields, R. (red.) *Cultures of Internet : virtual spaces, real histories, living bodies.* 1. Utg. London: Sage, s. 1-10.

Skilbrei, M. (2019) *Kvalitative metoder*. 1. Utg. Bergen: Fagbokforlaget.

Smith, M. J. og Clarke, R. V. (2012) Situational Crime Prevention: Classifying Techniques Using "Good Enough" Theory, i Farrington, D. P. og Welsh, B. C. (red) *The Oxford Handbook of Crime Prevention.* 1. Utg. Oxford: Oxford University Press, s. 292 – 316. DOI: 10.1093/oxfordhb/9780195398823.013.0015

Snl (2020) *Vestland.* Tilgjengelig fra: https://snl.no/Vestland Lest 27.06.21.

Snl (2021) *Territorialprinsippet.* Tilgjengelig fra: https://snl.no/territorialprinsippet_-_folkerett Lest 12.02.21.

Snyder, F. (2001) Sites of Criminality and Sites of Governance. *Social & legal studies*, 10(2), s. 251-256. https://doi-org.ezproxy.uio.no/10.1177/a017406

Staniforth, A. (2017) *Blackstone´s Handbook of Cyber Crime Investigation.* 1. utg. Oxford: Oxford University Press.

Straffeloven. *Lov 28. mai 2005 nr. 28 om straff.*

Sunde, I. M. (2019a) Datakrimretten i fugleperspektiv. *Tidskrift for strafferett*, 19(2), s. 129-147.

Sunde, I. M. (2019b) Sweetie, et politibarn eller en politistyrke på nett, i Sunde, I. M og Sunde, N. (red) *Det digitale er et hurtigtog.* Bergen: Fagbokforlaget, s. 177-208.

Tarter, A. (2017) Importance of Cyber Security. i: Bayerl, P.S., Karlović, R., Akhgar, B. og Markarian, G. (red.) *Community Policing - A European Perspective*. Cham: Springer, s. 213-230.

Terpstra, J. (2018) Local Policing in a Nationalized Police Force. A study on the local teams of the Netherlands' National Force. *Policing: A Journal of Policy and Practice*, 15(1), s. 251–262. https://doi.org/10.1093/police/pay037

Terpstra, J., Fyfe, N. R. og Salet, R. (2019) The Abstract Police: A conceptual exploration of unintended changes of police organisations. *The Police Journal*, 92(4), s. 339-359. DOI: 10.1177/0032258X18817999

Thagaard, T. (2018) *Systematikk og innlevelse.* 5. Utg. Oslo: Fagbokforlaget.

Thorsen, L. R., Lid, S. og Stene, R. J. (2009) Kriminalitet og rettsvesen 2009. *SSB.* Tilgjengelig fra: https://www.ssb.no/sosiale-forhold-og-kriminalitet/artikler-og-publikasjoner/kriminalitet-og-rettsvesen-2009

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

Trædal, T. J. (2017) *Mens andre land satser på nasjonalt «cyber crime centre», risikerer Norge å havne bakpå i kampen mot cyberkriminalitet.* Tilgjengelig fra: https://www.politiforum.no/nyheter/mens-andre-land-satser-pa-nasjonalt-cyber-crime-centre-risikerer-norge-a-havne-bakpa-i-kampen-mot-cyberkriminalitet/137559 Lest 14.05.21.

Turkle, S. (2015) *Reclaiming conversation: the power of talk in a digital age*. 1. Utg. New York: Penguin Press.

Wall, D. S. (2007) *Cybercrime.* 1. Utg. Cambridge: Polity Press.

Wall, D. S. og Williams, M. (2007) Policing diversity in the digital age: Maintaining order in virtual communities. *Criminology & Criminal Justice,* 7(4), s. 391-415. DOI: 10.1177/1748895807082064

Wall, D. S. (2008) Cybercrime and the culture of fear: Social science fiction (s) and the production of knowledge about cybercrime. *Information, Communication & Society,* 11(6), s. 861–884. DOI: 10.1080/13691180802007788

Wathne, T. C. (2016) Kvinners plass i politiet i lys av arbeidsmetoder. *Tidsskrift for kjønnsforskning,* 40(1), s. 3-23. https://doi.org/10.18261/issn.1891-1781-2016-01-02

Weiss, R. S. (1994) *Learning from strangers.* 1. Utg. New York: The Free Press.

Weston, N. J. (2010) Reassurance Policing, i Fisher, B. S. og Lab, S. P (red.) *Encyclopedia of Victimology and Crime Prevention*. 1. Utg. SAGE Publications, s. 758-759. http://dx.doi.org.ezproxy.uio.no/10.4135/9781412979993

Williams, M. L. og Levi, M. (2017) Cybercrime prevention, i Tilley, N. og Sidebottom, A. (red.) *Handbook of Crime Prevention and Community Safety.* 2. Utg. Abingdon: Routledge, s. 454-469.

Wills, J. (2017) Cybercrime: The Invisible Threat. *Law Enforcement Technology*, 44(4), s. 8-11.

Wood, M. A. (2020) Policing's 'meme strategy': understanding the rise of police social media engagement work. *Current Issues in Criminal Justice*, 32(1), s. 40-58. DOI: 10.1080/10345329.2019.1658695

Yar, M. og Steinmetz, K. F. (2019) *Cybercrime and Society.* 3. Utg. Sage.

Zedner, L. (2009) *Security*. 1. Utg. New York: Routledge.

Zuboff, S. (2015) Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), s. 75-89.

Fotnoter

Buisness insider (2014) *Instagram verifies badges.* Tilgjengelig fra: https://www.businessinsider.com/instagram-verified-badges-2014-12?r=US&IR=T

Europol (2021) *Empact.* Tilgjengelig fra: https://www.europol.europa.eu/empact Lest 04.06.21.

Forbrukertilsynet (2021) *Microsoft-Svindel.* Tilgjengelig fra: https://www.forbrukertilsynet.no/microsoft-svindel Lest 15.06.21.

Instagram (i.d.) Nettpatruljen_mrpd. *Nettpatruljen MRPD.* Tilgjengelig fra: https://www.instagram.com/nettpatruljen_mrpd/

Instagram (i.d.) Politietagder. *Politiets nettpatrulje - Agder*. Tilgjengelig fra: https://www.instagram.com/politietagder/

Politivest (2020a) Video 14.07.20, *TikTok*. Tilgjengelig fra: https://www.TikTok.com/@politivest/video/6849343583569448197?is_copy_url=1&is_from_webapp=v1 Sett 12.12.20.

Politivest (2020b) Video 10.09.20, *TikTok.* Tilgjengelig fra: https://www.TikTok.com/@politivest/video/6870942667417685250?is_copy_url=1&is_from_webapp=v1 Sett 12.12.20.

Vedlegg 1: Godkjennelse fra NSD

NSD NORSK SENTER FOR FORSKNINGSDATA

NSD sin vurdering

Prosjekttittel

Digital kriminalitetsforebygging

Referansenummer

286405

Registrert

03.06.2020 av Helene Walquist - helenwal@uio.no

Behandlingsansvarlig institusjon

Universitetet i Oslo / Det juridiske fakultet / Institutt for kriminologi og rettssosiologi

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)

Katja Franko, katja.franko@jus.uio.no, tlf: 90776405

Type prosjekt

Studentprosjekt, masterstudium

Kontaktinformasjon, student

Helene Walquist, helenewalquist@gmail.com, tlf: 92637326

Prosjektperiode

31.05.2020 - 31.12.2021

Status

09.06.2020 - Vurdert

Vurdering (1)

09.06.2020 - Vurdert

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet med vedlegg den 09.06.2020, samt i meldingsdialogen mellom innmelder og NSD. Behandlingen kan starte.

MELD VESENTLIGE ENDRINGER

Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til NSD ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde:
https://nsd.no/personvernombud/meld_prosjekt/meld_endringer.html

Du må vente på svar fra NSD før endringen gjennomføres.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 31.12.2021.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake. Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
NSD vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:

- lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
- formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke viderebehandles til nye uforenlige formål
- dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
- lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: åpenhet (art. 12), informasjon (art. 13), innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), underretning (art. 19), dataportabilitet (art. 20).

NSD vurderer at informasjonen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER
NSD legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og eventuelt rådføre dere med behandlingsansvarlig institusjon.

OPPFØLGING AV PROSJEKTET
NSD vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Vedlegg 2: Informasjonsskriv og samtykkeskjema

Vil du delta i et forskningsprosjekt om digital kriminalitetsforebygging?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å undersøke hvordan politiet arbeider med digital kriminalitetsforebygging av nettkriminalitet. Dette skrivet er et informasjonsskriv, for å gjøre deg som mulig deltaker klar over målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Politiets arbeid må tilpasse seg etter samfunnet, slik at de møter befolkningens behov. Det er klart at befolkningen, og spesielt unge, i dag responderer til og blir påvirket av andre kanaler enn før. En ny utfordring politiet har møtt på i de siste tiårene er kriminalitet som skjer på nett. Samtidig har også politiet fått tilgang til flere plattformer for å drive forebyggende arbeid. Formålet med prosjektet er å undersøke hvordan dette har formet måten politiet arbeider kriminalitetsforebyggende gjennom nye kanaler - det digitale.

Den foreløpige problemstillingen for dette masterprosjektet er:

Hvordan møter politiet forebygging av kriminalitet som skjer på nett?

- Hvordan tar de i bruk digitale hjelpemidler, som sosiale medier, til å forebygge nettkriminalitet?
- Kan prinsippene fra tradisjonell kriminalitetsforebygging overføres til digital kriminalitetsforebygging?

Hvem er ansvarlig for forskningsprosjektet?

Ansvarlig for prosjektet er Institutt for kriminologi og rettsvitenskap ved Universitetet i Oslo.

Hvorfor får du spørsmål om å delta?

Totalt seks til åtte personer har blitt spurt om å delta i dette prosjektet. Du har blitt valgt fordi du er ansatt i politidistriktet/avdelingen jeg ønsker å intervjue for å kunne utforske min problemstilling. Du har blitt valgt gjennom anbefalinger fra min kontaktperson i politidistriktet/avdelingen har anbefalt deg som en som kan kunne bidra med kunnskap og erfaring til mitt prosjekt.

Hva innebærer det for deg å delta?

Metode for å samle inn data er med semistrukturerte intervjuer. Samtalen vil bli ført med

utgangspunkt i overordnende temaer/spørsmål.

Intervjuet vil vare i maksimalt én time, beregnet tid ca. 45 minutter.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Du kan når som helst trekke samtykket tilbake uten å oppgi noen grunn, og alle dine personopplysninger vil da bli slettet. Å velge å ikke delta eller trekke seg vil ikke ha noen negative konsekvenser for deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- Kun student og veileder har tilgang til data.
- All data vil behandles anonymt. Dette vil si at eventuelt navn og kontaktopplysninger vil erstattes med kode som lagres på egen navneliste og oppbevares adskilt fra øvrig data.
- All data oppbevares på sikkert nettverksområde som kun student/veileder har tilgang til. Eventuelle skriftlig materiale vil oppbevares i innelåst skap på instituttets område med begrenset persontilgang. Kun student/veileder har tilgang til skapet.
- Informanter vil IKKE kunne gjenkjennes i publikasjon da datamateriale vil være fullstendig anonymisert.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er juni 2021, med muligheter for utsettelse til september 2021 og desember 2021. All data materiale vil permanent slettes ved prosjektslutt. Eventuelle skriftlige data vil makuleres.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene,
- å få rettet personopplysninger om deg,
- å få slettet personopplysninger om deg, og
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke. På oppdrag fra Institutt for kriminologi og rettssosiologi har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?

Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- Institutt for kriminologi og rettssosiologi Helene Walquist, [redacted]
- Institutt for kriminologi og rettssosiologi ved Katja Franko, [redacted]
- Vårt personvernombud: Roger Markgraf-Bye, [redacted] personvernombud@uio.no

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:

- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen

Katja Franko (Forsker/veileder)

Helene Walquist

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet Digital kriminalitetsforebygging og har fått anledning til å stille spørsmål. Jeg samtykker til:

- å delta i intervju.

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

---

(Signert av prosjektdeltaker, dato)

Vedlegg 3: Søknad til Kripos og Vest politidistrikt

UiO : Universitetet i Oslo
Det juridiske fakultet
Institutt for kriminologi og rettssosiologi

Sjef Kripos Kristin Kvigne

kripos@politiet.no

Dato: 3. juli 2020

Ønske om å intervjue ansatte i forbindelse med et masterprosjekt som omhandler digital kriminalitetsforebygging

Vi søker herved om tillatelse til å intervjue ansatte på Kripos i forbindelse med et masterprosjekt. Veileder for prosjektet er professor Katja Franko. Formålet med masterprosjektet i kriminologi ved Universitetet i Oslo er å studere hvordan politiet arbeider med digital kriminalitetsforebygging i forbindelse med kriminalitet som skjer på nett. Problemstillingen for prosjektet er hvordan politiet forebygger kriminalitet som skjer på nett. Vi ønsker derfor å undersøke hvilke digitale hjelpemidler som tas i bruk, og hvorvidt prinsipper fra tradisjonell kriminalitetsforebygging kan overføres til digital kriminalitetsforebygging.

Intervjuer

Helene Walquist ønsker på grunnlag av dette å gjøre kvalitative intervjuer med de som jobber med kriminalitetsforebygging i avdelingen Nasjonalt Cyberkrimsenter, og spesielt de som har jobbet mye med digitale kriminalitetsforebygging. Hun ønsker å snakke med dem om hvordan det forebyggende arbeidet finner sted gjennom digitale hjelpemidler. I tillegg vil hun ta opp temaet nettkriminalitet. Vi ser for oss å intervjue mellom 3-5 ansatte. For å gjøre det enklest mulig kan intervjuene gjerne gjennomføres på arbeidsplassen. Med hensyn til situasjonen vi er i nå, med Covid-19, kan det også være aktuelt å gjennomføre intervjuene digitalt på en sikker måte ved bruk av UiOs opptaksutstyr.

Forskningsetikk

Forskningsprosjektet skal ikke samle inn og behandle sensitive taushetsbelagte opplysninger. Alle data vil behandles etter gjeldende retningslinjer for håndtering av indirekte personopplysninger, og vil anonymiseres slik at personvernhensyn ivaretas. Prosjektet er også meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelig datatjeneste AS.

Oppstart og gjennomføringsplan

Det vil være ønskelig med oppstart og gjennomføring av datainnsamlingen innenfor perioden august – september 2020. I sin helhet vil prosjektet pågå fram til og med juni 2021. Vi ser med stor glede og interesse fram til en snarlig tilbakemelding og et eventuelt oppstartsmøte om prosjektet.

Postadresse: Postboks 6706 St. Olavs plass 5 0130 OSLO
E-post: krim-info@jus.uio.no
www.jus.uio.no\ikrs

UiO : Universitetet i Oslo
Det juridiske fakultet
Institutt for kriminologi og rettssosiologi

Politimester Kaare Songstad

post.vest@politiet.no

Dato: 11. juni 2020

Ønske om å intervjue ansatte i forbindelse med et masterprosjekt som omhandler digital kriminalitetsforebygging

Vi søker herved om tillatelse til å intervjue ansatte i Vest politidistrikt i forbindelse med et masterprosjekt. Veileder for prosjektet er professor Katja Franko. Formålet med masterprosjektet i kriminologi ved Universitetet i Oslo er å studere hvordan politiet arbeider med digital kriminalitetsforebygging i forbindelse med kriminalitet som skjer på nett. Problemstillingen for prosjektet er hvordan politiet forebygger kriminalitet som skjer på nett. Vi ønsker derfor å undersøke hvilke digitale hjelpemidler som tas i bruk, og hvorvidt prinsipper fra tradisjonell kriminalitetsforebygging kan overføres til digital kriminalitetsforebygging.

Intervjuer

Helene Walquist ønsker på grunnlag av dette å gjøre kvalitative intervjuer med de som jobber med kriminalitetsforebygging i Vest politidistrikt, og spesielt de som har jobbet mye med digitale kriminalitetsforebygging. Hun ønsker å snakke med dem om hvordan det forebyggende arbeidet finner sted gjennom digitale hjelpemidler. I tillegg vil hun ta opp temaer som nettkriminalitet og tradisjonell kriminalitetsforebygging. Vi ser for oss å intervjue mellom 3-5 ansatte. For å gjøre det enklest mulig kan intervjuene gjerne gjennomføres på arbeidsplassen. Med hensyn til situasjonen vi er i nå, med Covid-19, kan det også være aktuelt å gjennomføre intervjuene digitalt på en sikker måte ved bruk av UiOs opptaksutstyr.

Forskningsetikk

Forskningsprosjektet skal ikke samle inn og behandle sensitive taushetsbelagte opplysninger. Alle data vil behandles etter gjeldende retningslinjer for håndtering av indirekte personopplysninger, og vil anonymiseres slik at personvernhensyn ivaretas. Prosjektet er også meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelig datatjeneste AS.

Oppstart og gjennomføringsplan

Det vil være ønskelig med oppstart og gjennomføring av datainnsamlingen innenfor perioden august – september 2020. I sin helhet vil prosjektet pågå fram til og med juni 2021. Vi ser med stor glede og interesse fram til en snarlig tilbakemelding og et eventuelt oppstartsmøte om prosjektet.

Postadresse: Postboks 6706 St. Olavs plass 5 0130 OSLO
E-post: krim-info@jus.uio.no
www.jus.uio.no\ikrs

Vedlegg 4: Intervjuguide

0. Informasjon om prosjektet

- Bakgrunn og formål
  - Undersøke hvordan politiet jobber kriminalitetsforebyggende digitalt og hvordan dette forebyggende arbeidet er i møtet med nettkriminalitet
  - Intervjuer mennesker med tilknytning til kriminalitetsforebyggende arbeid i politiet for å undersøke hvordan de arbeider med digital kriminalitetsforebygging og hvordan dette oppleves av den enkelte.

Start lydopptak

- Informer om anonymitet og taushetsplikt
  - Informer om båndopptak og få muntlig samtykke

1. Innledning

- Navn, alder, stilling
- Hvilke erfaringer innenfor politiet har du fra tidligere av?
  - Har du jobbet med forebygging før?

2. Arbeidsoppgaver

- Hvor mange jobber med digital forebygging hos dere?
- Hvilke arbeidsoppgaver består din jobbhverdag av?
- Hva opplever du som de viktigste arbeidsoppgavene du har for å forebygge kriminalitet?
  - På hvilken måte bidrar dine arbeidsoppgaver til forebygging av kriminalitet?

3. Strategi

- Hvilke mål har din arbeidsplass satt for kriminalitetsforebygging?
- Hvilke mål har din arbeidsplass satt for digital kriminalitetsforebygging?
- Hvilke mål har din arbeidsplass satt for å forebygge nettkriminalitet?
- Er det opp til hver enkelt avdeling/distrikt hvor mye fokus det skal være på digital forebygging, eller blir det satt nasjonale krav?
- Hva ønsker du oppnå med arbeidet du gjør med digitale kriminalitetsforebygging?
- Hvordan opplever du arbeidet med digital forebygging i forhold til andre arbeidsoppgaver du har hatt i politiet?
  - Er fokuset annerledes, en annen holdning til arbeidet/publikum?
- Hvordan opplever du arbeidet med nettkriminalitet sammenliknet med andre kriminalitetstyper?

4. Virkemidler + Formål

- Hvilke digitale virkemidler/hjelpemidler tar dere i bruk i det forebyggende arbeidet?
- Hvilke konkrete kriminalitetsforebyggende tiltak har dere satt inn
    - Hvilken effekt ønsker dere å oppnå med disse?
- Hvordan opplever du at tekniske virkemidler påvirker måten dere driver det forebyggende arbeidet?
- Opplever du at digitale virkemidler har skapt utfordringer for politiarbeidet? I så fall, på hvilken måte?

5. Kontekst

- Hvem er det forebyggende arbeidet rettet mot?
    - Primær (befolkningen generelt/ungdommer generelt), sekundær (faresonen), tertiær (tidligere lovbrytere)
- Hvilke typer kriminalitet forsøker dere å forebygge digitalt?
    - Hvilke typer nettkriminalitet forsøker dere forebygge digitalt?
- For hvilke typer kriminalitet virker det som at den digitale forebyggingen er mest effektiv mot?
- Hvilke utfordringer knyttet til nettkriminalitet møter dere på?
- Hvordan opplever du møtet med publikum gjennom digital kriminalitetsforebygging?
- Hvordan opplever du at tillitten til politiets arbeid er påvirket av det digitale kriminalitetsbildet?

6. Utfordringer/fordeler

- Hvilke utfordringer møter dere på ved forebygging av kriminalitet som skjer på nett?
- Hvilke fordeler finnes det ved å drive kriminalitetsforebygging digitalt?
- Hva opplever du som den største forskjellen mellom tradisjonelt forebyggende arbeid og digitalt forebyggende arbeid?
- Hva opplever du som den største forskjellen mellom forebygging av tradisjonell kriminalitet og forebygging av kriminalitet som skjer over internett?
- Hvordan ser du for deg at dere vil utvikle arbeidet med digital kriminalitetsforebygging videre?

7. Avslutning

- Er noe uklart? Noe du vil spørre om eller legge til?

Stopp lydopptak
Takke for deltagelse