Overvåkning og styring av narkotikadistribusjonen på det mørke nettet

En kvalitativ analyse av kontrollørenes syn på kryptomarkeder

Cecilie Nyhus

Masteroppgave i kriminologi

Institutt for kriminologi og rettssosiologi

Juridisk fakultet

UNIVERSITETET I OSLO

26. november 2020

Overvåkning og styring av narkotikadistribusjonen på det mørke nettet

En kvalitativ analyse av kontrollørenes syn på kryptomarkeder

2020

Overvåkning og styring av narkotikadistribusjonen på det mørke nettet: En kvalitativ analyse av kontrollørenes syn på kryptomarkeder

Cecilie Nyhus

http://www.duo.uio.no

Sammendrag

Tittel: Overvåkning og styring av narkotikadistribusjonen på det mørke nettet: En kvalitativ analyse av kontrollørenes syn på kryptomarkeder

Skrevet av: Cecilie Nyhus

Veileder: Mareile Kaufmann

Institutt for kriminologi og rettssosiologi

Det juridiske fakultet

Universitetet i Oslo

Høst 2020

Hva slags syn har myndighetene om narkotikadistribusjonen på det mørke nettet? Den stadige teknologiske utviklingen gjør det mer utfordrende for myndighetene å følge med på trender og moduser for narkotikahandel på kryptomarkeder. Samtidig kan digital data utnyttes av myndighetene for å effektivisere overvåkning av samfunnsborgerne. Samfunnsendring har alltid vært nært knyttet til teknologisk utvikling, men det digitale blir enda viktigere når det påvirker overvåkning, styring og disiplin.

Med en inngående analyse av overvåkningsdynamikker på det mørke nettet, vil denne oppgaven være et bidrag til overvåkningsforskning ved å videreutvikle allerede eksisterende overvåkningsperspektiver. Dette vil brukes som grunnlag til å forklare hvordan overvåkning påvirker myndighetenes styring på kryptomarkeder. Basert på myndighetenes mangfoldige syn, får vi kunnskap om hva de anser som sine utfordringer med det mørke nettet, og hvordan de ønsker å møte disse. En større innsikt i deres synspunkter kan skape en dypere forståelse i hva som ligger bak kriminalpolitikken som påvirker myndighetenes overvåkning og styring.

Det denne oppgaven vil fokusere på i forbindelse med myndighetenes syn på det mørke nettet, er de krypterte plattformenes mange effekter. Det er spesielt anonymiteten på det mørke nettet som skaper en spenning i myndighetenes synspunkter. Denne spenningen kan belyses som et samfunnsdilemma mellom frihet og kontroll, med personvern og menneskerettigheter på den ene siden og samfunnssikkerhet på den andre. Myndighetenes meninger vil videre belyses ut ifra kryptomarkedenes funksjoner knyttet til narkotikadistribusjon. Sammenlignet med tradisjonelle narkotikamarkeder, kan markeder på det mørke nettet tilby lavere oppdagelsesrisiko, større tilgjengelighet av atskillige narkotiske stoffer og en mindre sannsynlighet for å bli utsatt for direkte fysisk vold. Riktignok vil det foreligge en risiko for å oppleve digital vold knyttet til kjøp av narkotika på krypterte plattformer, og dette bekymrer myndighetene. Dessuten anser de den økte tilgjengeligheten av farlige narkotiske stoffer som urovekkende. Det er likevel de andre samfunnsmessige konsekvensene som følger av narkotikakriminalitet myndighetene betrakter som mest bekymringsfullt. En annen ulempe myndighetene trekker frem, er at deres overvåkning kan være mer utfordrende med krypterte plattformer. Denne avhandlingen vil imidlertid vise at ved hjelp av digitale spor, foregår det flere former for overvåkning på det mørke nettet.

Myndighetenes holdninger knyttet til de ulike aspektene ved det mørke nettet er samlet inn ved å bruke to metodiske tilnærminger: Kvalitative intervju og kvalitativ dokumentanalyse. Det empiriske materialet består av intervjuer med seks myndighetspersoner som er ansatt i toll eller politi og som jobber med å overvåke kryptomarkeder, samt dokumentanalyse av offentlige rapporter som er publisert av Politidirektoratet, Oslo politidistrikt, Europol og EMCDDA. Dette vil analyseres med utgangspunkt i en sammenfletting av sosiologiske og kriminologiske teorier om digitalisering, overvåkning og governmentality. Analysen vil vise at det finnes et mangfold av overvåkningsdynamikker og styringsprosesser på det mørke nettet, og dette vil føre til mer overvåkning og disiplinering for alle parter. Myndighetenes forebyggende arbeid ved å blant annet legge ned de store markedsplassene på det mørke nettet resulterer i en fragmentering av kryptomarkedene. Dette vil trolig ha en negativ innvirkning på myndighetenes fremtidige overvåkning og styring av narkotikadistribusjon på internett.

Forord

Jeg vil beskrive arbeidet med denne masteravhandlingen som en lang prosess som samtidig har gått veldig fort. Nå nærmer denne prosessen seg slutten og i den forbindelse er det flere personer som fortjener en stor takk.

Først og fremst vil jeg takke alle informantene mine. Takk for at dere ønsket å stille til intervju og dele deres tanker og synspunkter om narkotikadistribusjonen på det mørke nettet. Jeg setter ekstra stor pris på at dere tok dere tid til dette i den krevende og utfordrende perioden hvor Norge var rammet av en global pandemi. Jeg vil også takke min portvakt i dette prosjektet. Takk for at du helt fra første telefonsamtale var ivrig på å hjelpe meg med å rekruttere informanter.

Videre ønsker jeg å takke veilederen min, Mareile Kaufmann. Takk for at du hele veien har motivert meg til å jobbe videre med masteravhandlingen og fått meg til å være ekstra strukturert. Dine direkte tilbakemeldinger og gode innspill har vært til stor hjelp.

Merete, takk for all tilrettelegging du har gjort for meg slik at jeg kunne gjennomføre dette masterprosjektet ved siden av jobb.

Takk til pappa, som ved siden av sin støtte, har vært en korrekturleser som har tatt jobben på alvor. Takk til resten av familien min som alltid støtter meg og er stolt av det jeg gjør. Jeg er også veldig heldig som har de beste venninnene i verden. Takk for at dere alltid stiller opp, dere vet hvem dere er.

Til slutt vil jeg takke min kjære André. Takk for all kjærligheten du viser meg hver eneste dag, og for at du gjennom hele denne prosessen har mint meg på at det er et liv ved siden av skole og jobb. Jeg kunne ikke fått en bedre ”nærkontakt” enn deg, for selv om Norge har vært i lockdown har livet med deg vært en lek.

November 2020

Cecilie Nyhus

Innholdsfortegnelse

1 Innledning

I dagens samfunn er vi så omringet av teknologi at vi ofte tar det for gitt (Skardhamar og Klemsdal, 2019). Mye av menneskelig kommunikasjon foregår i dag på internett og sosiale medier. Teknologi har også ført til at vi kan handle alt av varer på internett bare ved noen tastetrykk på datamaskinen, nettbrettet eller smarttelefonen og få det levert direkte på døren eller i postkassen. Dette innebærer også ulovlige varer som våpen og narkotiske stoffer. For å redusere risikoen for å bli fratatt de ulovlige varene, og bli straffet for det av myndighetene, utvikles det stadig smartere løsninger. I takt med strengere straffer har narkotikadistributører blitt mer kreative og teknologi benyttes for økt salgseffektivitet og lavere oppdagelsesrisiko (Politidirektoratet, 2017). En av disse smarte løsningene som har blitt utviklet er markedsplassene på det mørke nettet. Når narkotikaselgere tyr til disse nye, forenklede og smarte metodene, krever det at myndighetene tilpasser sine tiltak for å kontrollere narkotikakriminalitet. At noe av narkotikakriminaliteten går over på digitale plattformer kan også gi myndighetene mulighet til å øke sine digitale overvåkningsløsninger. På bakgrunn av dette skal denne avhandlingen ta for seg myndighetenes synspunkter om det mørke nettet. Det er viktig å forske på deres holdninger fordi de kan ha politiske konsekvenser for samfunnet. Det vil samtidig gi oss mer kunnskap om hva myndighetene mener om digitalisering og overvåkning. Utgangspunktet for å undersøke dette, vil i tillegg til analyse av offentlige rapporter som er publisert av Politidirektoratet, Oslo politidistrikt, Europol og EMCDDA, baseres på intervju med myndighetspersoner som er ansatt i toll og politi, og som jobber med å overvåke på det mørke nettet.

Digital data er sporbart, noe som fører til at myndighetene kan tilpasse og øke sine overvåkningstiltak. Sporbarhet og lagring av digital data på internett kan utnyttes av myndighetene for å effektivisere overvåkning av samfunnsborgerne (Kaufmann og Jeandesboz, 2017; Lyon, 2007). Samtidig kan den stadige utviklingen i teknologi gjøre det mer utfordrende for myndighetene å følge med på trender og moduser for illegale aktiviteter. Overvåkning er ekstra utfordrende på det mørke nettet for myndighetene fordi narkotikahandelen er lagt opp til å være anonym (Politidirektoratet, 2017). Basert på kriminologiske teorier om digitalisering, vil denne avhandlingen videreutvikle allerede eksisterende overvåkningsperspektiver for å forklare overvåkningsdynamikkene og styringsmekanismene på det mørke nettet. Ved å behandle de ulike fagdisiplinene samlet, vil denne oppgaven være et bidrag til digital kriminologi.

I 2014 publiserte journalisten Jonas Vikan en sak om narkotikadistribusjon på det mørke nettet i Adresseavisen hvor han uttrykte at ”virksomheten har bygd seg opp over flere år, og omfanget øker mens bakmennene ikke trues av politi og rettsvesen” (Vikan, 2014). Dette utsagnet kan tolkes som kritikk rettet mot myndighetene og deres fravær på det mørke nettet. Året etter at Vikan (2014) publiserte artikkelen i Adresseavisen, demonstrerte Kripos sin tilstedeværelse på det mørke nettet ved å gå til aksjon mot en norsk gruppe som solgte narkotika på kryptomarkeder, i det som ble kalt operasjon Marco Polo (Kripos, 2017). Dette er bare et av mange eksempler på myndighetenes styring rettet mot narkotikadistribusjonen på det mørke nettet. Blant annet har flere internasjonale aksjoner ført til at myndighetene har stengt ned flere store markedsplasser (Europol, 2017). På bakgrunn av myndighetenes synspunkter, vil nedstenging av markedsplasser som en styringsmekanisme på det mørke nettet diskuteres i denne avhandlingen.

1.1 Kryptomarkeder på det mørke nettet

Internett har hatt en stor utvikling siden 1990-tallet og i dag kan vi si at internett består av minst to ulike områder som følger ulike teknikker og logikker. Det ene området er tilgjengelig med standard søkemotorer som Google og Yahoo (Pergolizzi m.fl., 2017). Det andre området er ikke tilgjengelig gjennom de ordinære søkemotorene og refereres ofte til som dypnettet. På dypnettet finnes det eksklusive nettverk som kun er tilgjengelig ved bruk av krypteringsprogramvarer, og dette kalles for det mørke nettet (Mörch, m.fl., 2018).
For å få tilgang til det mørke nettet kan man blant annet sikre sin anonymitet ved å bruke Onion Routing. Dette innebærer å laste ned en programvare, for eksempel programvaren TOR, som var den første etablerte formen for Onion Routing. Når TOR er lastet ned, vil en del av datamaskinen krypteres og man kan kobles sammen med andre som benytter samme programvare. Dette kan gjøre det mer utfordrende å bli identifisert på internett. Å ta del i denne type nettverk krever teknologisk kunnskap om flere avanserte konsepter (AlQahtani og El-Alfy, 2015). Likevel viser den norske dokumentarserien Insider (Narko på Dark Web, 2020) at å laste ned TOR, benytte seg av kryptert valuta og handle narkotika på det mørke nettet kan være veldig enkelt, og man kan bruke standard søkemotorer som Google til å få den informasjonen man trenger for å gjennomføre det. Hvis man ønsker å handle narkotika på det mørke nettet er man avhengig av en datamaskin, en spesiell anonym nettleser, markedsplassens nettadresse og en form for kryptert valuta, som for eksempel bitcoin. I

tillegg må man handle fra en leverandør som er villig til å selge narkotika til landet man befinner seg i, og en adresse som pakken kan sendes til (Barratt og Aldridge, 2016).

Det har blitt estimert at narkotikadistribusjon står for to tredjedeler av det mørke nettets aktivitet (EMCDDA, 2017). Denne delen av det mørke nettet velger Barratt og Aldridge (2016) å kalle kryptomarkeder. De definerer det som markedsplasser bestående av flere selgere, som tilbyr deltakere anonymitet ved oppgitt lokasjon på et bortgjemt nettverk, og med kryptovaluta som betaling. Kryptomarkedene har også tilbakemeldingsfunksjoner, bestående av anmeldelser og kommentarer, som jeg i denne avhandlingen vil beskrive som en form for overvåkningsmekanisme. Det mørke nettet gir kjøpere og selgere av narkotiske stoffer muligheten til å opptre anonymt, man slipper å møtes ansikt til ansikt og man kan oppholde seg i forskjellige land når man gjennomfører narkotikahandel (Martin, 2014).

1.2 Avhandlingens problemstilling og forskningsbidrag

I dag vet vi ikke så mye om hva myndighetspersonene som jobber med styring på det mørke nettet tenker om utfordringene knyttet til kryptomarkeder. Ambisjonen med denne avhandlingen er å få en større innsikt på dette området, og vil med det gi en bredere forståelse for hva som kan ligge bak kriminalpolitikken som påvirker myndighetenes overvåkning og styring. Med utgangspunkt i dette er den overordnede problemstillingen formulert på følgende måte:

- *Hva slags syn har myndighetene om narkotikadistribusjonen på det mørke nettet?*

Fremfor å se kontrollmyndighetenes meninger ut fra forenklede modeller som kun baserer seg på kriminalitetsbekjempelse, vil denne avhandlingen utdype deres nyanserte holdninger til det mørke nettet. Deres mangfoldige syn vil bidra til kunnskap om hva de anser som sine utfordringer med det mørke nettet, og hvordan de velger å takle disse gjennom overvåkning og styring. For å gå i dybden på dette, har jeg som en forlengelse av hovedproblemstillingen utviklet tre underproblemstillinger som vil skape grunnlaget for avhandlingens analyse og diskusjon. Alle underproblemstillingene vil besvares med utgangspunkt i myndighetenes synspunkter:

- *Hvilke faktorer står bak myndighetenes rasjonalisering av ressurser rettet mot styring på det mørke nettet?*
- *Hvordan foregår overvåkningsdynamikkene mellom kontrollører, narkotikaselgere og narkotikakjøpere på de krypterte markedsplassene?*
- *Hvordan påvirker overvåkningsdynamikkene myndighetenes styring på kryptomarkedene?*

Teknologi og digitalisering er i stadig endring, og denne oppgaven utforsker et viktig aspekt som vil bidra til økt kunnskap om hva myndighetene tenker om den digitale utviklingen, med utgangspunkt i det mørke nettet. Selv om forskning om det mørke nettet har fått økt oppmerksomhet i akademia de siste årene, er studier om dette temaet fremdeles begrenset (EMCDDA, 2017; UNDOC, 2019). Forskningen som eksisterer har som oftest tatt sikte på å studere selve kryptomarkedene (Décary-Hétu og Dupont, 2013; Martin, 2014; Broséus m.fl., 2016; Rhumorbarbe m.fl., 2016; Bakken, Møller, og Sandberg, 2017; Bancroft, 2017; Espinosa, 2019; Aldridge og Askew, 2017; Aldridge, 2019), eller fokusert på kjøpere og selgere som benytter seg av disse markedsplassene til narkotikahandel (Barratt, Ferris og Winstock, 2014; Bakken og Bosnes, 2015; Tzanetakis m.fl., 2015; Bancroft og Reid, 2016; Tzanetakis, 2018). Det foreligger noen hull i den aktuelle forskningen om det mørke nettet som bør utforskes, deriblant studier som adresserer temaet sett fra myndighetenes perspektiv. Denne avhandlingen vil bidra til å tette dette forskningshullet ved å knytte funn fra empirisk materiale som er samlet inn gjennom kvalitative intervju og dokumentanalyse av offentlige rapporter, sammen med teorier om digitalisering, overvåkning og governmentality.

1.3 Avhandlingens oppbygning

Utover dette innledende kapittelet består denne masteravhandlingen av fem kapitler. Kapittel 2 redegjør for aktuell forskning som er valgt ut fra relevansen for videre analyse av temaer som omhandler narkotikadistribusjon på det mørke nettet. Forskningen som presenteres i underkapittel 2.1 omhandler hvem som kjøper og selger narkotika på krypterte markedsplasser, mens studier som beskriver hvordan markedsføringen foregår på kryptomarkeder skisseres i underkapittel 2.2. Deretter vil underkapittel 2.3 beskrive undersøkelser som sammenligner narkotikadistribusjonen på det tradisjonelle narkotikamarkedet med det mørke nettet. Til slutt vil forskningsbidrag som belyser

kryptomarkedenes potensielle skadereduserende og skadeøkende egenskaper presenteres i underkapittel 2.4.

For å kunne analysere temaene som springer ut fra de aktuelle forskningsbidragene videre, vil jeg i kapittel 3 introdusere avhandlingens teoretiske rammeverk. For å få ytterligere innsikt i myndighetenes meninger om overvåkning og styring på det mørke nettet, vil analysen bygge på sosiologiske og kriminologiske teorier om digitalisering (Lupton, 2015; Kaufmann og Jaendesboz, 2016; Powell, Stratton og Cameron, 2018; Skardhamar og Klemstad, 2019) i underkapittel 3.1, overvåkning med fokus på panoptiske teorier (Foucault, 1979; Mathiesen, 1997; Mann og Ferenbok, 2013) og overvåkningsperspektiver som bruker surveillant assemblage som utgangspunkt (Haggerty og Ericsson, 2000; Lyon, 2007) i underkapittel 3.2, samt governmentality (Foucault, 1991; Garland, 1999) i underkapittel 3.3.

Den metodiske tilnærmingen som oppgaven bygger på vil presenteres i kapittel 4, som består av seks underkapitler. Det empiriske materialet for denne avhandlingen baserer seg på to metodiske tilnærminger: Kvalitative intervju og kvalitativ dokumentanalyse. Først vil underkapittel 4.1 beskrive bakgrunnen for valget av disse metodene. Underkapittel 4.2 vil videre forklare hvordan jeg har rekruttert informanter og hvordan intervjuene ble gjennomført. Deretter viser jeg til utvalgsprosessen knyttet til dokumentanalysen i underkapittel 4.3. Mine betraktninger omkring forskningens kvalitet og fremstilling vil i underkapittel 4.4 presenteres før jeg utdyper hvordan jeg har analysert det empiriske materialet i underkapittel 4.5. Metodekapittelet avslutter med underkapittel 4.6 som belyser mine etiske refleksjoner knyttet til denne forskningen.

Fra en beskrivelse av masterprosjektets metodiske fremgangsmåte, presenteres det som er oppgavens sentrale bidrag, nemlig avhandlingens analyse og diskusjon. I kapittel 5 er analyse og diskusjon sammenflettet og følger en argumentativ struktur. Sammen med aktuell forskning, og de teoretiske perspektivene, vil dette gi en fyldigere forståelse av myndighetenes synspunkter om narkotikadistribusjonen på det mørke nettet med fokus på overvåkning og styring. Kapittelet er delt inn i fire underkapitler som diskuterer hver sine poeng og underargumenter. I underkapittel 5.1 vil myndighetenes refleksjoner og meninger om anonymitet på det mørke nettet diskuteres ved å se på de krypterte nettverkenes tosidighet. Dette etterfølges av underkapittel 5.2 som beskriver faktorene utover anonymitet og kryptering som myndighetene trekker frem som utfordrende ved det mørke nettet. Dette

inkluderer deres synspunkter om kryptomarkeders egenskaper knyttet til digital vold, økt tilgjengelighet av farlige narkotiske stoffer og andre samfunnsmessige konsekvenser. Myndighetenes holdninger til det mørke nettet vil kunne ha politiske konsekvenser og påvirke deres styring på kryptomarkedene. Et annet element jeg vil trekke frem, som kan være med på å påvirke myndighetenes styring på det mørke nettet, er overvåkningsprosessene som foregår der. Derfor vil jeg i kapittel 5.3 presentere en kartlegging av overvåkningsdynamikkene på de krypterte markedsplassene. Som en videreføring av dette vil jeg vise hvordan overvåkningsprosessene på det mørke nettet kan påvirke myndighetenes styring i underkapittel 5.4 ved å diskutere kontrollørenes synspunkter om forebygging knyttet til kryptomarkeder, og myndighetenes nedstenging av markedsplasser.

Det sjette og siste kapittelet er en avslutning hvor forskningens funn diskuteres oppsummerende før jeg ytrer mine konkluderende merknader. Hva slags synspunkter myndighetene har om det mørke nettet med fokus på overvåkning og styring vil være grunnlaget for denne avhandlingen. Deres holdninger er nyanserte knyttet til de ulike sidene ved de krypterte nettverkene. På bakgrunn av digitale data sin sporbare egenskap, kan myndighetene overvåke kryptomarkedene samtidig som narkotikaselgere og narkotikakjøpere overvåker myndighetene tilbake. Kjøpere og selgere av narkotika på det mørke nettet overvåker også hverandre. De gjensidige overvåkningsprosessene fører til mer overvåkning og disiplin for alle parter. Med alle disse overvåkningsdynamikkene, er det mørke nettet egentlig så ”mørkt”?

2 Aktuell forskning

Det mørke nettet er et forskningsområde som spesielt de siste årene har fått mer oppmerksomhet. Riktignok er studier om krypterte nettverk fremdeles begrenset og offentlige rapporter etterlyser mer forskning på dette emnet (EMCDDA, 2017; UNDOC, 2019). Dette kapittelet vil basere seg på et utplukk av den aktuelle forskningen som omhandler narkotikadistribusjon på det mørke nettet i de retningene som berører denne oppgavens problemstillinger. Det vil ikke være en fullstendig gjennomgang av all forskning på området, men kapittelet vil kort presentere studier som er særlig relevant for denne avhandlingen.

Den aktuelle forskningen som introduseres omhandler hvem som benytter seg av det mørke nettet for kjøp og salg av narkotiske stoffer, markedsføringen på kryptomarkeder, sammenligning av narkotikahandelen på det tradisjonelle narkotikamarkedet og på krypterte markedsplasser, og til slutt det mørke nettets skadereduserende og skadeøkende egenskaper. Dette vil, sammen med teoriene som presenteres i kapittel 3, danne grunnlaget for avhandlingens analyse og diskusjon. Den aktuelle forskningen tar for seg flere aspekter ved narkotikadistribusjonen på det mørke nettet, men det er ikke forsket nok på myndighetenes synspunkter om dette. Formålet med denne avhandlingen er at den skal bidra til å tette dette forskningshullet ved å belyse holdningene myndighetspersonene som jobber med kontroll rettet mot narkotikadistribusjonen på det mørke nettet har til denne formen for markedskriminalitet. Før vi kommer dit vil dette kapittelet presentere hva de aktuelle forskningsbidragene kan vise oss og hvordan de relateres til denne oppgaven.

2.1 Kjøpere og selgere av narkotika på det mørke nettet

Det foreligger både kvalitative og kvantitative studier som fokuserer på personene som benytter seg av det mørke nettet for kjøp og salg av narkotika. Tzanetakis (2018) er en forsker som har gjennomført kvantitativ analyse på kryptomarkeder, og hun forteller at majoriteten av brukerne er menn i tyveårene som har en historie med sporadisk narkotikabruk. Videre har hun funnet ut at de fleste enten har fast jobb og/eller holder på å gjennomføre høyere utdanning. Disse kjennetegnene skiller seg fra målgruppen for det tradisjonelle narkotikamarkedet, og analysen i denne avhandlingen vil vise at myndighetene mener det mørke nettet legger til rette for en ny brukergruppe og selgergruppe av narkotika.

Dette fører videre til studier som har undersøkt hvorfor noen velger krypterte nettverk til kjøp og salg av narkotika. Barratt, Ferris og Winstock (2014), Bakken og Bosnes (2015) samt Bancroft og Reid (2016) har forsket på ulike nettforum og foretatt kvalitative intervjuer med personer som handler narkotika på det mørke nettet. Disse studiene har kommet frem til at hovedårsakene til at noen velger å handle narkotika kryptomarkeder er lav oppdagelsesrisiko, større tilgjengelighet av mangfoldige narkotiske stoffer og kvaliteten på stoffene man kan få tak i. Ifølge rapport publisert av European Monitoring Centre for Drugs and Drug Addiction (EMCDDA, 2016) er det også noen personer som benytter seg av det mørke nettet for kjøp og salg av narkotika som uttrykk for protest. I denne konteksten er det snakk om kryptoanarkister som er imot kriminalisering av narkotikabruk og mener at de står opp for folket. De legitimerer narkotikahandel på det mørke nettet fordi de mener at det burde være opp til hver enkelt om man ønsker å bruke narkotiske stoffer. Faktorene som disse studiene trekker frem som hovedårsaker til at noen velger å bruke kryptomarkeder for kjøp og salg av narkotika vil diskuteres nærmere i avhandlingens analyse- og diskusjonskapittel med utgangspunkt i myndighetenes synpunkter.

De nevnte forskningsbidragene danner grunnlag for en dypere innsikt i målgruppen for markedsplassene på det mørke nettet, og hva som kan være årsakene til at noen personer oppsøker kryptomarkeder når de skal kjøpe eller selge narkotika. De nevnte forskningene dekker ikke de statlige aktørenes synspunkter om disse faktorene. Kunnskapen om narkotikadistribusjonen på det mørke nettet må utvides til å omfatte myndighetenes perspektiv, i og med at de jobber med overvåking og styring rettet mot narkotikahandelen på de krypterte nettverkene.

2.2 Markedsføringen på kryptomarkeder

Tilgjengeligheten av det brede spekteret av ulike narkotiske stoffer var en av hovedårsakene til at personene foretrakk denne plattformen når de skulle handle narkotika. Dette er en av egenskapene til krypterte markedsplasser som kan kobles til markedsføring. Det foreligger enkelte studier av markedsplassene som ser det fra et markedsperspektiv. Et eksempel er fra Martin (2014) som referer til kryptomarkeder som eBay for narkotiske stoffer. Han mener at de brukervennlige funksjonene, sammen med en relativ høy sikkerhet på internett, har ført til at man kan sammenligne narkotikadistribusjonen på det mørke nettet med legale

markedsplasser på internett. Dette gjør at forholdet mellom kjøper og selger på kryptomarkeder fremstår profesjonelt på samme måte som på lovlige internettsider.

På bakgrunn av at distribusjonen på kryptomarkeder kan sammenlignes med salg på legale nettsider, er det noen som stempler narkotikadistributørene på det mørke nettet som entreprenører (Décary-Hétu og Dupont, 2013). I Bakken, Møller og Sandberg (2017) sin forskning fremstilles en suksessfull selger av narkotika på det mørke nettet som en med god kundeservice, en som innehar mye kunnskap, samt en som følger andre viktig parametere man kan kjenne igjen i markedsføringen på lovlige internettsider. Markedsføringen på det mørke nettet vil i denne oppgaven diskuteres som en overvåkningsmekanisme mellom kjøpere og selgere på kryptomarkeder, med utgangspunkt i tanken om at kjøperne overvåker selgernes omdømme før de velger å handle varer.

Broséus med flere (2016) har undersøkt hvordan det mørke nettet kan ses ut fra et markedsperspektiv med leverandørene i fokus. De kom frem til at selgerne er aktive på diverse ulike kryptomarkeder samtidig, både med samme og med flere ulike brukernavn. Noen av leverandørene var spesialisert på en kategori av narkotisk stoff, mens andre tilbydde forskjellige stoffer. Broséus med flere (2016) mener også at man kan konkludere med at det mørke nettet er strukturert og organisert for å kunne effektivisere smugling. Strukturen og organiseringen baseres blant annet på en tilbakemeldingsfunksjon. Selgere av narkotika på det mørke nettet er avhengig av gode tilbakemeldinger fra kjøperne for å kunne selge produkter. Espinosa (2019) har forsket på hvordan tilbakemeldingsfunksjonene på det mørke nettet kan forebygge salg av narkotika med lav kvalitet og av dårlige selgere. Han kom frem til at ærligere selgere bygger sin tillit på det mørke nettet basert på et såkalt internettomdømme. Myndighetenes synspunkter om både markedsføring og tilbakemeldingsfunksjonen på kryptomarkeder vil fremmes i avhandlingens analyse.

I likhet med lovlige nettmarkeder brukes tilbakemeldingsfunksjonene flittig, og på det mørke nettet vil de med flest positive tilbakemeldinger ha høyere priser på varene sine (Décary-Hétu og Dupont, 2013). Bakken, Møller og Sandberg (2017) beretter i sin forskning at risiko på kryptomarkeder reduseres ved å investere i tillit gjennom tilbakemeldingsfunksjonene. De mener dette vil være til fordel for både selger med økning i potensielle salg og for kjøpere ved at kjøpene er sikrere. Dette er et interessant argument, og denne forskningen har gitt

inspirasjon til å diskutere dette videre i analyse- og diskusjonskapittelet med utgangspunkt i myndighetspersonene som jobber med å kontrollere på det mørke nettet sine meninger.

Det er ikke bare i tilbakemeldingsfunksjonen det foregår kommunikasjon som omhandler kjøp og salg av narkotika på det mørke nettet. I likhet med det legale nettmarkedet foregår det også kommunikasjon på andre forumer eller sosiale medier på internett (Bakken og Demant, 2019). Bancroft (2017) har forsket på kommunikasjonen mellom brukere på det mørke nettet som foregår på diverse internettforum, og der deler de blant annet sine egne erfaringer knyttet til risiko. Dette innebærer informasjon om ulike narkotiske stoffer, hvordan disse stoffene skal brukes, risiko i forbindelse med rettsvesenet, samt tillit til ulike selgere og de forskjellige kryptomarkedene. Markedsføring og tilbakemeldingsfunksjon skiller det kryptomarkedene fra det tradisjonelle narkotikamarkedet. Det er flere forskere som har sett nærmere på ulikheter og likheter mellom disse to ulike måtene for narkotikahandel.

2.3 Tradisjonell narkotikahandel versus krypterte markedsplasser

Det er ikke bare markedsføringen som er annerledes på det mørke nettet sammenlignet med den tradisjonelle narkotikadistribusjonen. Bakken, Møller og Sandberg (2017) har forsket nærmere på likhetene og ulikhetene mellom disse to formene for narkotikahandel. En likhet de trekker frem, er at begge krever at man selv oppsøker det dersom man ønsker å kjøpe narkotiske stoffer. De mener videre at internett har banet vei for et nytt narkotikamarked som skiller seg fra det tradisjonelle markedet ved at kjøpere kan sitte relativt trygt hjemme og bestille ulovlig narkotika gjennom datamaskinene, sammenligne priser og produkter fra ulike selgere, og samtidig unngå kontrollmyndighetene. Denne avhandlingen vil vise at man ikke nødvendigvis kan unngå kontrollmyndighetene helt ved å benytte det mørke nettet fordi det finnes flere ulike overvåkning- og styringsmekanismer som myndighetene kan benytte seg av. Forskningen til Bakken, Møller og Sandberg (2017) viser også at når man først har kommet inn på de krypterte markedsplassene, kan tilbakemeldingsfunksjonene og kommentarene som er der virke salgsfremmende.

Videre i sammenligningen mellom tradisjonelle narkotikahandel og kryptomarkeder, betegner Bakken, Møller og Sandberg (2017) kryptomarkedene som delvis åpne markeder i

likhet med narkotikadistribusjonen som foregår på puber og klubber. Narkotikahandel på det mørke nettet kan karakteriseres som synlige og åpne samt at de baserer seg på å ha konkurransedyktige priser og profesjonell kommunikasjon. Det er i utgangspunktet åpent for alle, men bare dersom man er klar over dens eksistens og har nok teknologisk kompetanse til å få tilgang. Informasjon om det mørke nettet er ikke tilgjengelig for alle, og tilgangen er begrenset fra standard internettsøkemotorer (Lacson og Jones, 2016). På den andre siden kan kryptomarkeder også anses som lukket fordi handel baseres på tillit som oppstår gjennom gjentatte kjøp. I kontrast til puber og klubber vil også det mørke nettet være annerledes ved at nettsidene kan betraktes som ”mellommann” mellom selger og kjøper (Bakken, Møller og Sandberg, 2017). Istedenfor å bruke en person som et ledd mellom narkotikaselger og kjøper, vil nettverkene kunne fungere som dette leddet, eller ”mellommannen”.

Aldridge og Askew (2017) har forsket på hvordan kryptomarkedenes selgere og kjøpere fokuserer på å redusere risiko og samtidig opprettholde en mest mulig effektiv handel. De bruker teori om rasjonelle valg for å forklare det tradisjonelle narkotikamarkedet på tre ulike måter, og mener at dette også kan anvendes på narkotikadistribusjonen på det mørke nettet: Reduksjon i synlighet, reduksjon i avgift og reduksjon i risiko. Reduksjon i synlighet handler om å være mindre synlig for myndighetene og som et eksempel vil anonymiteten på kryptomarkedene gjøre det vanskeligere for myndighetene å overvåke narkotikaselgere, selv om de samtidig er synlig for narkotikakjøperne. Spesielt dette punktet er relevant for denne avhandlingen, da den vil gå nærmere inn på synlighet, usynlighet og gjensidige overvåkningsprosesser. Det andre punktet som Aldridge og Askew (2017) beskriver er reduksjon i avgift. På det mørke nettet kan dette eksempelvis innebære å dele opp postforsendelsene for å sende mindre kvantum av gangen, eller å plassere narkotika sammen med lovlige varer. Det siste punktet Aldridge og Askew (2017) trekker frem er reduksjon av risiko knyttet til distribusjonen. På det mørke nettet er et eksempel på dette at distributørene ikke overleverer stoffer selv, men benytter seg av postgang. Denne avhandlingen vil vise hvordan myndighetenes overvåkning og styring påvirker narkotikaselgernes og narkotikakjøpernes reduksjonstiltak.

2.4 Det mørke nettets skadereduserende og skadeøkende egenskaper

Det er flere studier som argumenterer for at det mørke nettet har flere skadereduserende egenskaper sammenlignet med det tradisjonelle narkotikamarkedet. Tzanetakis med flere (2015) viser til at salg av narkotika på det mørke nettet gir personer større mulighet til å undersøke kvalitet og effekter ved ulike narkotiske stoffer. Selv om det er ulovlig bidrar det til mindre risiko og helsekonsekvenser relatert til narkotikabruk. Rhumorbarbe med flere (2016) har forsket på kvaliteten på narkotiske stoffer de bestilte fra markedsplattformen Evolution. De kom frem til at det viktigste psykoaktive stoffet selgerne hevdet å distribuere var til stede i prøvene som ble mottatt og at stoffene generelt sett ikke skilte seg veldig fra det som hadde blitt beslaglagt på gaten av politiet. Rhumorbarbe med flere (2016) antok at det kunne være flere grunner til at narkotikaen fra det mørke nettet lignet stoffene fra gaten. Disse grunnene var for eksempel at selgere på det mørke nettet kjøpte produktene sine fra gaten, eller at gateselgere og nettbaserte selgere hadde benyttet seg av samme forskyvningskilde.

En annen potensiell skadereduserende side ved narkotikahandel på kryptomarkeder er at det fører til mindre fysisk vold enn distribusjon på andre narkotikamarkeder. I en spørreundersøkelse utført av Barratt, Ferris og Winstock (2016) ble det rapportert at kunder på kryptomarkeder har opplevd færre voldshendelser, og trusler om vold, sammenlignet med alternative kilder for narkotika, som for eksempel gjennom venner eller kjente narkotikaselgere på gaten. Selv om det mørke nettet ikke har bestått av tillit basert på trussel om fysisk vold, slik mye tradisjonell narkotikahandel foregår, er ikke det mørke nettet bare fredfullt. Martin (2018) samt Barratt og Aldridge (2016) kommer i sine studier frem til at istedenfor fysisk vold foregår det trusler om digital vold, og i enkelte tilfeller også gjennomføring av digital vold, på det mørke nettet. Dette er for eksempel svindel, nettmobbing eller publisering av personlig informasjon om hverandre. Denne avhandlingen vil bygge videre på Martin (2018) og Barratt og Aldridge (2016) sine argumenter ved å ta for seg myndighetenes meninger om fysisk vold og digital vold knyttet til det mørke nettet.

Aldridge (2019) diskuterer i sin studie hvordan kryptomarkeder både kan være skadereduserende og produsere mer skadelige utfall. Han tenker at veggen som oppstår på internett kan føre til en økt variasjon i innhold på de narkotiske stoffene, men han mener

videre at dette problemet løses enkelt med den tillitsbaserte tilbakemeldingsfunksjonen, som tidligere er gjort rede for i dette kapittelet. Aldridge (2019) mener på den andre siden at tilgjengelighet av narkotika potensielt kan føre til større skade ved å benytte det mørke nettet. For å eksemplifisere dette, trekker han frem hvordan en person som i utgangspunktet var ute etter å kjøpe en liten mengde cannabis til egen bruk kan bli fristet til å kjøpe større mengder eller andre farligere stoffer. Årsaken til disse fristelsene kan være at personen enkelt kan se potensiale i profitten av å selge narkotika videre på det mørke nettet på grunn av tilbudene man får ved å kjøpe større kvantum. Analyse- og diskusjonskapittelet i denne oppgaven vil ta denne diskusjonen videre og presentere myndighetenes delte meninger om kryptomarkedenes skadereduserende og skadeøkende egenskaper. De aktuelle forskningsbidragene vil sammen med teoretiske perspektiver brukes som inspirasjon og utgangspunkt for denne avhandlingens analyse.

3 Teoretiske perspektiver

Sammen med de aktuelle forskningsbidragene, vil de teoretiske perspektivene jeg presenterer i dette kapittelet brukes som verktøy for å gå i dybden på de ulike synsaspektene myndighetene har om kryptomarkeder. For å skape et nyansert bilde av oppgavens problemstilling er det hensiktsmessig å anvende teori ut ifra det Bratberg (2018) kaller flerfaglighet. Perspektivene jeg vil ta for meg er sosiologiske og kriminologiske teorier om digitalisering (Lupton, 2015; Kaufmann og Jaendesboz, 2016; Powell, Stratton og Cameron, 2018; Skardhamar og Klemstad, 2019), overvåkning med fokus på panoptiske teorier (Foucault, 1979; Mathiesen, 1997; Mann og Ferenbok, 2013) og surveillant assemblage (Haggerty og Ericson, 2000; Lyon, 2007) samt governmentalityteori (Foucault, 1991; Garland, 1999). Narkotikadistribusjon på det mørke nettet, og myndighetenes styring rettet mot de krypterte markedsplassene, er et omfattende fagområde som krever anvendelse av flere ulike teoretiske perspektiver med formål om å utfylle hverandre. De nevnte teoriene vil gi en større innsikt i overvåkning og styringen på det mørke nettet, og myndighetenes synspunkter vedrørende dette.

3.1 Sosiologiske og kriminologiske teorier om digitalisering

Narkotikadistribusjonen på det mørke nettet foregår på digitale markedsplasser, og det er nettopp digitalisering som er årsaken til at disse kryptomarkedene eksisterer. Sosiologiske og kriminologiske teorier om digitalisering er derfor nødvendig å praktisere for å forstå overvåkningen på det mørke nettet. Dette underkapittelet vil blant annet beskrive hvordan egenskapene med digitale data forandrer samfunnet både med nye former for kriminalitet og med overvåkning (Lyon, 2007). Med denne avhandlingen vil jeg bidra til mer forskning som knytter digitalisering, overvåkning og kriminalitet sammen. I avhandlingens analyse vil jeg videreutvikle allerede eksisterende overvåkningsperspektiver, sammen med kriminologiske teorier om digitalisering, til å forklare overvåkningsdynamikker og styringsmekanismer på det mørke nettet.

Før jeg plasser digitalisering i overvåkningskontekst, må digital teknologi forklares. Lupton (2015) definerer digital teknologi som kodede objekter som tas opp og videreføres ved å bruke digital medieteknologi. Han utdyper dette videre med å si at digital teknologi både tar

for seg maskinvarene, altså dataenhetene, og programvarene, som innebærer servere og programmene som er på dataenhetene. Hvordan digital overvåkning foregår i dag er i stor grad påvirket av stordata. Stordata kan defineres som kulturelt og teknologisk studiefenomen basert på teknologi, analyse og metode. Det innebærer en stor mengde datasett, verktøy for å manipulere og analysere de, samt en teknologisk måte å tenke og forske på. Det er ikke bare de store mengdene med data, men det innebærer også hvordan dataene brukes. I dagens samfunn har vi ikke bare mer data, men det har også oppstått en helt ny måte å analysere dataene på (Boyd og Crawford, 2012).

En ny datadreven styring som har blitt flittig brukt av myndighetene de senere årene er algoritmer. Algoritmer kan defineres som en rekke med datakoder som forteller maskinen hvordan man skal fortsette, basert på en serie av instruksjoner til å ankomme på et spesielt sted. Eksempelvis brukes det til å samle inn informasjon om de som bruker datamaskinene, før de sorters for å få mening ut av dataene, kunne forutse fremtidig handling og foreslå det for brukerne (Lupton, 2015). Bellanova (2017) kaller myndighetenes styring ved hjelp av dette for algoritmisk governmentality. Dette er styring av maskiner og etterretningsdatasystemer som automatisk prosesserer data fra ulike kilder ved statistisk beregning. Etterretning er prosessen hvor man bringer en stor mengde informasjon sammen i en kontekst for å få et meningsfylt bilde (McCulloch og Pickering, 2009). Digital data fungerer som oversettelser av mennesker, ting, oppførsel og relasjoner til informasjon som kan lagres, håndteres og visualiseres av maskiner (Bellanova, 2017). Det er flere årsaker til at myndighetene overvåker det mørke nettet, men innsamling av etterretningsinformasjon gjøres blant annet for å målrette deres fremtidige overvåkning og styring.

Basert på utviklingen av stordata kan det digitale best forstås ut ifra et sosiologisk perspektiv med eksisterende sosiotekniske kategorier basert på et sett av ”affordances” som Kaufmann og Jaendesboz (2016) har beskrevet. Digital data kan anses som tellbar informatikk gjennom lagring. Videre er det søkbart og sporbart, og det kan fabrikkeres og tolkes. Det digitale må av den grunn analyseres sammen med politikk og samfunnet, og derfor anses det å være noe sosialt. Det digitale samfunnet står for det naturlige av teknologi som er basert på strukturelle og sosiale endringer. Samtidig vil teknososialitet ta for seg de prosessene, kulturene og praksisene som er i hverdagslivet (Powell, Stratton og Cameron, 2018). I denne oppgavens analyse- og diskusjonskapittel vil det digitale plasseres sammen med overvåkning, styring og narkotikapolitikk.

Overvåkning har i senmoderne tid blitt påvirket av digitalisering og teknologisk utvikling (Salter, 2010). Studier av overvåkning har foregått i lang tid, men overvåkningsstudier isolert sett er relativt nytt i akademia (Lyon, 2007). Det kan være flere grunner til at overvåkning har fått mer oppmerksomhet i forskning de senere årene, men den ene grunnen er at teknologien i samfunnet hele tiden utvikles raskere og får flere brukere (Lyon, Haggerty og Ball, 2012; Sunde og Sunde, 2019). Det senmoderne samfunnets oppbygning og utvikling av teknologi har endret dynamikkene i makt, identitet, institusjonell praksis og relasjoner. Datamaskiner kan lagre og håndtere store mengder data, og dette har vært med på å utvikle samfunnet. Dessuten har det vært en generell trend at overvåkning har vært mer synlig og usynlig på en og samme tid. Vi kan se overvåkningskameraer over alt hvor vi går, men det er mindre synlig hvor overvåket vi blir (Lyon, Haggerty og Ball, 2012). Overvåkningen på det mørke nettet er ikke like visuelt som et overvåkningskamera på gaten, men denne avhandlingen vil kartlegge overvåkningsdynamikkene som er på kryptomarkedene.

Digital kriminologi har begynt å se på overvåkning i forbindelse med kriminalitetsforskning (Powell, Stratton og Cameron, 2018). Kriminologifaget har flere verktøy for å utforske kriminalitet i forbindelse med det digitale, og det foreligger kriminologisk forskning på temaer som cyberkriminalitet og cyberterrorisme. Powell, Stratton og Cameron (2018) mener imidlertid at de tradisjonelle kriminologiske teoriene ikke alltid er tilstrekkelig i studier av internett. De hevder videre at digital kriminologi kan gi en mer fruktbar plattform, og som tar moderne kriminologisk teori og forskning et steg videre. Powell, Stratton og Cameron (2018) ønsker en bredere disiplin som krysser både teknologi, sosiologi, kriminalitet, avvik og straff. Digital kriminologi representerer en samhandling mellom kritisk, kulturell og sosioteknologisk teori. Min forskning behandler flere av disse fagdisiplinene samlet, og vil med det være et bidrag til digital kriminologi med myndighetenes synspunkter på narkotikadistribusjonen som foregår på det mørke nettet som utgangspunkt.

Digitalisering, overvåkning og det mørke nettet henger sammen. Det mørke nettet har skapt en slags spenning hos kriminologer, i og med at de krypterte internettplattformene kan ha flere funksjoner (Powell, Stratton og Cameron, 2018). På den ene siden ønsker myndighetene å få oversikt og regulere organisert internettkriminalitet. Alt innhold på det mørke nettet er ikke nødvendigvis ulovlig, men anonymiteten kan legge til rette for et miljø med slike aktiviteter. Kryptering, brukeranonymitet og forfalskning av lokasjon, kan fra myndighetenes side anses som mistenkelig aktivitet fremfor et verktøy av demokrati (Politidirektoratet,

2017). På den andre siden er det noen som benytter det mørke nettet på grunn av deres bekymring over personvern eller på bakgrunn av menneskerettigheter og internettfrihet (Tzanetakis, 2017). I denne avhandlingen vil jeg se på denne tosidige spenningen hos myndighetspersonene som jobber med overvåkning og styring på det mørke nettet.

Som en oppsummering av sammenhengen mellom digitalisering og overvåkning, skiller digitale overvåkningsteknologier seg fra eldre overvåkningspraksiser ved at dataene kan lagres, og det finnes teknikker som kan manipulere disse dataene. Digital teknologi har skapt nye former for overvåkning, blant annet til det som det kan defineres som dataveillance, også kalt panspektrisk overvåkning (Lupton, 2015). Panspektrisk overvåkning illustrerer hvordan overvåkning baseres på et bredere spekter av digital teknologi og bruk av data. Dette innebærer systematisk overvåkning av mennesker eller grupper, ved personlige datasystemer, for å regulere eller styre deres handlinger (Andrejevic og Gates, 2014). Det mørke nettet ble utviklet for å være en plattform hvor man kunne opptre anonymt, men denne avhandlingen belyser hvordan overvåkning er mulig på kryptomarkedene. Panspektrisk overvåkning er bare en av mange overvåkningsmodeller som eksisterer. I neste underkapittel skal andre overvåkningsperspektiver knyttes til det mørke nettet.

3.2 Overvåkning: Fra panoptikon til surveillant assemblage

Samfunnsendring har alltid vært nært knyttet til teknologisk utvikling, men det digitale blir enda viktigere når det påvirker overvåkning, styring og disiplin. Svært mye av samtidens sosiale liv relateres til det digitale og leves gjennom digitale plattformer (Skardhamar og Klemsdal, 2019). Denne digitale utviklingen har påvirket narkotikadistribusjonen i en digital retning, og det mørke nettet er en ny arena hvor kjøp og salg av narkotika har fått fotfeste. Dette påvirker myndighetenes overvåkning og styring, hvor de også er nødt til å følge den digitale utviklingen. Politiet har siden september 2018 hatt en nettpatrulje som er til stede på internett i sosiale medier som Snapchat, Instagram og Facebook (Trædal, 2018). Imidlertid finnes det per dags dato ikke en egen myndighetspatrulje som kun jobber med overvåkning og styring på det mørke nettet. Overvåkning anses som en av de viktigste komponentene i senmoderne tid (Haggerty og Ericson, 2000). Denne avhandlingen vil vise at det finnes flere ulike overvåkningsmekanismer på det mørke nettet. Selv om myndighetene i Norge ikke har

egen patrulje som kun jobber med overvåkning på det mørke nettet, finnes det noen myndighetspersoner som overvåker kryptomarkeder som en av flere arbeidsoppgaver.

Det mørke nettet kan anses som en motstand til myndighetenes overvåkning og styring. Dersom internett har et potensiale for økning i overvåkning, har det også et potensiale for økning i motstand til overvåkning (Mehta og Darier, 1998). Motstand til overvåkning er en nødvendig utvikling av overvåkning og den eksisterer i mange former (Martin, van Brakel, Bernhard, 2009). Det mørke nettet er et eksempel på motstand til overvåkning, og kryptering benyttes i forsøk på å forbli anonym og skjule personlig identitet (Tzanetakis, 2017). I det følgende vil jeg forklare nærmere de ulike overvåkningsprosessene og motstand til overvåkning som foregår på det mørke nettet.

Overvåkning stammer fra det franske verbet ”surveiller” som betyr å våke over. Det kan videre defineres som fokusert, systematisk og rutinebasert oppmerksomhet til personlige detaljer med formål om å påvirke, styre eller beskytte (Salter, 2010). Det innebærer å finne ut hvem som er hvor og hva de gjør, enten i den fysiske eller virtuelle verden, og på et gitt tidspunkt (Bennett og Regan, 2004). Selv om overvåkning har gjennomgått en stor utvikling gjennom historien har det eksistert like lenge som menneskeheten selv og har alltid basert seg på innhenting av informasjon (Lyon, 2007). I dag overvåker myndighetene personer med formål om å forebygge kriminalitet, og ikke bare for å etterforske illegale handlinger. Fordi kvaliteten og kvantiteten av etterretning om kriminelle grupper er begrenset, trenger statlige aktører å samle inn så mye informasjon som mulig i håp om å kunne forebygge eller stanse kriminalitet (Salter, 2010). Kontrollmyndighetenes overvåkningssystemer er spesielt designet for å sortere menneskers aktiviteter og karakteristika for etterretningsformål. I tillegg til innsamling av informasjon for etterretning, er ansatte i politi og toll til stede på det mørke nettet for å forebygge kriminalitet. Myndighetene rasjonaliserer sin overvåkning med at de ønsker å redusere risiko for potensiell skade (Bennett og Regan, 2004). Ifølge myndighetene kan narkotika anses som skadelig for samfunnet, og myndighetenes tilstedeværelse på det mørke nettet kan potensielt gjøre markedsplassene mindre attraktive for kjøp og salg av narkotika. Dette vil diskuteres nærmere i denne avhandlingens analyse- og diskusjonskapittel.

For å demonstrere hvordan overvåkning foregår på det mørke nettet, vil denne oppgaven bruke flere overvåkningsperspektiver. En modell som flere av perspektivene bygger på, er Foucaults (1979) panoptikon. Denne panoptiske modellen har i dag blitt gjenopprettet og fått

økt oppmerksomhet i studier av overvåkning (Aas, Gundhus og Lomell, 2009). Panoptikon var en arkitektur først presentert av Bentham (Foucault, 1979). Panoptikonarkitekturen har en bygning i midten hvor en fangevokter kan observere fangene i alle fengselscellene som har gjennomsiktige vinduer med lys bak. Fangene kan ikke se fangevokteren, og er derfor uvitende om når de blir overvåket og ikke. Resultatet er det Foucault (1979) anser som en perfekt maktoperasjon, hvor myndighetene skal disiplinere borgerne til selvdisiplin. Denne selvdisiplinen er ikke alltid en bevisst prosess, men kan foregå uten at de som overvåkes selv er klar over det. Selvdisiplineringsprosessen vil forklares nærmere i neste underkapittel som omhandler governmentality. Myndighetene overvåker markedsplassene på det mørke nettet, og jeg vil i denne avhandlingen komme med eksempler på at de som benytter seg av det mørke nettet for kjøp og salg av narkotika er klar over politi og toll sin tilstedeværelse, men de er ikke klar over når de overvåkes. Jeg vil tolke denne overvåkningsdynamikken videre og argumentere for at myndighetene disiplinerer kjøpere og selgere på kryptomarkedene til å disiplinere seg selv. Jeg vil belyse dette ytterligere i analyse- og diskusjonskapittelet i denne oppgaven, og blant annet argumentere for at disiplin og selvdisiplin vil føre til større utfordringer for myndighetene knyttet til deres styring på kryptomarkeder.

Mehta og Darier (1998) har forsket på forholdet mellom panoptikon og internett. De kaller relasjonen for ”panoptisk effekt på en elektronisk motorvei”, og mener med dette at internett har noen panoptiske kvaliteter som kan påvirke hvordan folk samhandler med hverandre og med data (Mehta og Darier, 1988, s. 107). Videre forklarer de at overvåkning på internett kan ses som mini-panoptikoner. Hvorvidt myndighetenes overvåkning på det mørke nettet kan kategoriseres som et mini-panoptikon på samme måte kan diskuteres. Mehta og Darier (1998) mener at myndighetenes makt er mindre åpenbar, men det betyr bare at disiplineringen og normaliseringseffektene er enda større på flere måter. Det er ikke direkte synlig at politi og toll er til stede på det mørke nettet, likevel viser diverse forum at kjøpere og selgere på kryptomarkedene er klar over myndighetenes tilstedeværelse. Selv om myndighetenes makt er mindre synlig, kan disiplineringen være enda større enn om den hadde vært mer visuell.

Det er ikke bare myndighetene som overvåker kjøpere og selgere på kryptomarkedene. På det mørke nettet foregår det flere former for overvåkningsprosesser. Om panoptikon kan anvendes på dagens myndighetskontroll, og ikke minst til styring rettet mot narkotikadistribusjonen på det mørke nettet, kan således diskuteres. Panoptikon kritiseres for å ikke være en dekkende modell til å forstå dagens overvåkningspraksiser (Mathiesen, 1997).

Mens noen mener at panoptikon kan forklare overvåkning i dag, mener andre at panoptikon ikke lenger er egnet til å beskrive maktrelasjonene i dagens samfunn hvor digital informasjon alltid er tilgjengelig (Haggerty og Ericson, 2000). På bakgrunn av panoptikons begrensninger oppfordres det til å benytte seg av, eller supplere med, andre perspektiver for å forklare overvåkning i dagens samfunn (Salter, 2010). Derfor vil jeg også presentere andre overvåkningsperspektiver for å illustrere overvåkningsdynamikkene på det mørke nettet.

Mathiesen (1997) mener at Foucault overser massemedias påvirkning på overvåkning, som han mener har skapt en ny dynamikk hvor mange også ser få, og ikke bare situasjoner hvor få ser mange. For å forklare dette bedre introduserte han begrepet synoptikon. Mathiesen (1997) mener at panoptikon og synoptikon sammen vil beskrive samfunnet som et toveis overvåkingssamfunn ved at de interagerer med hverandre. Overvåkning involverer ofte deltakelse av den som overvåkes, noe som gjør at den som overvåkes innehar en viktig rolle (Lyon, 2007). Jeg vil vise i denne avhandlingen at kjøpere og selgere på det mørke nettet overvåker myndighetene. De kan overvåke myndighetene ved å følge med på mediene og lese i myndighetenes offentlige rapporter om hvilke satsningsområder de har. Likeledes kan de gjennom aviser få informasjon om markedsplasser som legges ned, og få opplysninger knyttet til tilslag og arrestasjoner som politiet gjør i forbindelse med narkotikasaker fra det mørke nettet.

Et annet perspektiv som demonstrerer hvordan overvåkning kan foregå nedenfra og opp, er det Mann og Ferenbok (2013) refererer til som sousveillance. De sammenligner overvåkning i senmoderne tid som et samfunn hvor fangene i panoptikonmodellen kan se tilbake på sine fangevoktere. Vi lever i en tid hvor mennesker ikke bare ser tilbake på myndighetene, men ved å gjøre det, kan man potensielt drive sosial og politisk endring. På det mørke nettet er det ikke bare politi og toll som overvåker, og jeg vil vise i analysen at kjøpere og selgere av narkotika på kryptomarkedene disiplineres av myndighetene til gjensidig overvåkning. Dupont (2008) argumenterer for at internett skaper et uskarpt skille mellom de som overvåker og de som blir overvåket.

Samfunnsborgere overvåker ikke bare myndighetene, men de overvåker også hverandre. Dette kaller Andrejevic (2005) lateral surveillance, eller lateral overvåkning som betyr sidestilt overvåkning. Mens panoptikonmodellen baserer seg på en hierarkisk modell ovenfra og ned, vil lateral overvåkningsmodell illustrere at samfunnsborgere også overvåker andre

samfunnsborgere (Andrejevic, 2005). På det mørke nettet overvåker kjøpere og selgere hverandre, blant annet ved å benytte kryptomarkedenes tilbakemeldingsfunksjon. Likeså er det også noen kjøpere som selv tester narkotikaen de har handlet på det mørke nettet for å undersøke kvaliteten på stoffene.

På grunn av alle de ulike overvåkningsprosessene som foregår i dagens samfunn, foretrekker Haggerty og Ericson (2000) surveillant assemblage over panoptikon. De kritiserer blant annet panoptikon for å ikke ta høyde for dagens teknologiske og digitale utvikling fordi overvåkning blir annerledes når vi har større mengder digital data. Surveillant assemblage skapes ved å anvende komplekse metoder basert på teknikker fra militæret, policing og markedsstrategier, på personlig informasjon. For å forklare dette kan man se for seg en jordstengel som sender ut planteskudd i ulike retning hvor hver av de tar en egen rot (Lyon, 2007). Sammenlignet med panoptikon har surveillant assemblage et mindre sentralisert fokus. Perspektivet tar høyde for at det eksisterer et hierarki, men den består av en form der alt er tilkoblet hverandre og vokser på ulike nivåer i planten (Haggerty og Ericson, 2000). Dette innebærer at surveillant assemblage ser på overvåkning som flytende, noe som Foucault har blitt kritisert for å overse (Lyon og Bauman, 2013). På det mørke nettet flyter overvåkningen fra flere hold, da alle overvåker hverandre. Myndighetene overvåker kjøpere og selgere, denne overvåkningen er gjensidig, og kjøpere og selgere overvåker også hverandre. Denne flytende overvåkningsprosessen kan derfor forklares med perspektivet surveillant assemblage. Alle disse overvåkningsdynamikkene på det mørke nettet vil bli beskrevet i denne oppgaven. På bakgrunn av myndighetenes overvåkning på det mørke nettet (panoptikon), kjøpere og selgeres overvåkning av myndighetene (synoptikon/sousveillance), overvåkning mellom kjøpere og selgere (lateral surveillance), og at alle overvåker hverandre (surveillant assemblage), vil denne avhandlingen argumentere for at det mørke nettet kanskje ikke er så ”mørkt”.

Panoptikonmodellen har også blitt kritisert for å ikke ta høyde for dagens teknologiske og digitale utvikling. Som nevnt i forrige underkapittel, er overvåkning annerledes når vi har større mengder digital data som har resultert i økt strategisk og fremtidsrettet fokus (Lyon, 2007). I dagens samfunn er det ikke bare fysiske kropper som overvåkes, men også abstrakte digitale kropper, hvor en person kan inneha flere ”personer” ved at man overvåkes ut ifra hvilke grupper man kan være en del av. Surveillant assemblage opererer ved å abstrahere menneskelige kropper fra deres opprinnelige kontekst og lager det som Haggerty og Ericson

(2000) kaller datadoubles. Vi blir målt uten å fysisk snakke ansikt til ansikt som tidligere, og det er her blir man koblet fra sin egen kropp for byråkratiske formål. Fraværet av fysisk kontroll og tilstedeværelse er erstattet med et vidt spekter av databaser og fjernkontroll. Denne endringen i teknologisk overvåkning skaper nye strategier og styringspraksiser (Salter, 2010). Når myndighetene overvåker markedsplassene på det mørke nettet, og forsøker å identifisere de som kjøper og selger narkotika der, ser de ikke individene som enkeltpersoner. Dette eksempelet kan illustrere hvordan individene kobles fra sin egen kropp, og blir sett på som et brukernavn tilhørende en digital profil på kryptomarkedene. Jeg vil imidlertid videreutvikle datadoublesperspektivet, og argumentere for at datadoubles kan være bakgrunnen for at digital data om en person kan kobles tilbake til en persons fysiske kropp. Når myndighetene bruker sin overvåkning av digital data på det mørke nettet for å identifisere personer, er dette et uttrykk for styring. En styring som kan forklares med governmentalityteori (Foucault, 1991).

3.3 Governmentality

Jeg har allerede nevnt at når myndighetene overvåker på det mørke nettet, kan det resultere i at kjøpere og selgere av narkotika på kryptomarkedene disiplineres til selvdisiplin. Myndighetenes styring og disiplin på de krypterte markedsplassene kan illustreres med governmentalityteori. Foucault (1991) introduserte begrepet governmentality i 1978 for å forstå hva som er spesifikt for maktutøvelse i det moderne samfunnet. Han argumenterte for at governmentality hadde en felles grunn for alle moderne former for politiske tanker og handlinger. Garland (1999) hevder at governmentalitylitteraturen gir god innsikt i hvordan kriminalitet kontrolleres, og derfor vil det være en anvendelig teori i denne masteravhandlingen som retter søkelyset på myndighetenes styring på det mørke nettet. Jeg vil koble governmentalityteori til myndighetspersonenes tilstedeværelse på det mørke nettet som involverer både direkte og indirekte styring.

Governmentalitybegrepet kan deles inn i to deler: *Government* som betyr styring og *mentality* som betyr rasjonalitet. Dette betyr at staten styres ut ifra iboende rasjonelle prinsipper eller lover (Neumann, 2003). Governmentality består av to poler: Statens evne til å styre borgerne, og evnen til å få borgerne til å styre seg selv. Dette gjøres gjennom bestemte måter å tenke på (rasjonaliteter), gjennom spesifikke måter å handle på som påvirker styringen (teknologier), samt myndighetenes maktutøvelse mot samfunnsborgerne (Garland, 1999). Den første polen,

statens evne til å styre borgerne, gjøres gjennom det Foucault (1991) betegner som disiplin. Dette kan defineres som metoder myndighetene benytter seg av for å muliggjøre styring av samfunnsborgernes bevegelser for å sørge for at de underkues og tvinges til å være føyelige og nyttige. Den andre polen er statens evne til å få borgerne til å styre seg selv. For å gjøre samfunnsborgerne selvregulerende vil staten styre på avstand med utgangspunkt i for eksempel overvåkning (Garland, 1999). Samfunnsborgerne selvdisiplineres fordi de overvåkes, og denne selvdisiplineringsprosessen er ikke alltid bevisst. I denne avhandlingen vil jeg vise eksempler på myndighetenes direkte og indirekte styring på det mørke nettet. Myndighetenes direkte styring inkluderer aksjoner hvor de stenger ned store markedsplasser, samt identifisering og straffeforfølgning av kjøpere og selgere på kryptomarkedene. Samtidig vil jeg vise at denne direkte styringen også kan anses som indirekte styring ved at det bidrar til at kjøpere og selgere disiplineres til selvdisiplin. Kjøpernes og selgernes selvdisiplin består blant annet av å utvikle nye strategier for å motstå myndighetenes styring og overvåkning. Avhandlingens analyse- og diskusjonskapittel vil også beskrive hvordan kjøpernes og selgernes overvåkning av kontrollørene disiplinerer dem til selvdisiplin, ved at myndighetene også er nødt til å øke sin teknologiske kompetanse.

Myndighetenes indirekte styring på det mørke nettet vil illustreres ut ifra et forebyggende perspektiv. Å ha politi og toll til stede på det mørke nettet kan anses som en strategi for å forebygge tilbøyeligheten til å benytte seg av disse markedsplassene for kjøp og salg av narkotika. Garland (1999) har sett mye på selvdisiplin, men jeg vil trekke samfunnsborgernes selvdisiplin tilbake til de klassiske myndighetenes rolle. Myndighetenes overvåkning på det mørke nettet kan forstås som det første steget for kjøpernes og selgernes selvdisiplineringsprosess. Tidligere fokuserte myndighetene på å etterforske og straffe kriminalitet, mens nå har det vært et skifte til samfunn som har større fokus på å forebygge kriminalitet (Lomell, 2012). Myndighetene benytter seg av teknikker som sikter på å forebygge lovbrudd som kan skje i fremtiden, og det blir gitt mer ressurser til forebyggende strategier for å identifisere trusler før kriminalitet finner sted (Ashwort og Zedner, 2014). Med dette kan det forstås at myndighetene overvåker for å disiplinere folk til å avstå fra skadelige handlinger. Hvorfor myndighetene prioriterer sine ressurser rettet mot styring og overvåkning på det mørke nettet vil illustreres i oppgavens analyse- og diskusjonskapittel, basert på kvalitative intervjuer og analyse av offentlige rapporter.

Nyliberalisme kan legges til grunn for samfunn med økt fokus på risikohåndtering og forebygging (Garland, 2013). Hovedprinsippene ved nyliberalisme er at menneskelige aktører er ansvarlig for sine egne valg og utfall. Det bygger på markedsøkonomiens makt og konkurranse, som skal skape de beste utfallene for alle (Lupton, 2015). Sentralt i disse strategiene er at styring av sjelen gjøres gjennom å skape frie subjekter som er ansvarlige for egne liv (Rose og O´Malley, 2006). Det ideelle subjektet til nyliberalistisk tenkning er en selvregulerende person som tar ansvar for sin egen skjebne. Individer er forventet å være selvrefleksive og se deres liv som et prosjekt som krever investering og energi (Lupton, 2015). Myndighetenes indirekte styring på det mørke nettet vil forsøke å utnytte individenes frie og selvrefleksive tanker, med mål om at de selv vil velge å frastå fra å benytte det mørke nettet til kjøp og salg av narkotika. Basert på dette kan markedsplassene på det mørke nettet forstås ut fra en nyliberalistisk tilnærming på bakgrunn av styringsmekanismene som finnes der. Markedsføringen som kryptomarkedene baserer seg på, for eksempel gjennom kommentarfelt og tilbakemeldinger fra kunder, kan også anses for å være bygget på nyliberalistisk tenkning. Når en kjøper skal handle fra en selger på det mørke nettet, gjennomfører vedkommende en risikokalkulering basert på kommentarene i tilbakemeldingsfunksjonen.

Som en forlengelse av governmentality og nyliberalisme, har beregning fått et nytt nivå i det postmoderne samfunnet hvor styring og risikotenkning har blitt dominante temaer i politikken (Lyon, Haggerty og Ball, 2012). I likhet med all ressursbruk av statlige midler er også myndighetenes valg om å ha tjenestepersoner til å jobbe på det mørke nettet, fattet etter en risikovurdering. Beregning av risiko foregår begge veier. Myndighetene bruker ressurser rettet mot styring på det mørke nettet basert på sin risikovurdering, parallelt med at kjøpere og selgere på det mørke nettet overveier risiko ved å bli identifisert og straffet av myndighetene. De gjensidige prosessene med risikovurderinger fra flere hold, påvirker den samlede styringen, disiplinen og overvåkningen. For å finne ut hva myndighetene mener om deres prioritering av ressurser rettet mot narkotikadistribusjon på det mørke nettet, har jeg intervjuet tjenestepersoner som jobber med overvåkning på det mørke nettet, og analysert offentlige rapporter publisert av offentlige myndigheter.

4 Metode

Innledningsvis uttrykte jeg min interesse angående myndighetenes synspunkter om narkotikadistribusjonen på kryptomarkeder. Hva som ligger bak myndighetenes prioriteringer av ressurser rettet mot det mørke nettet, overvåkningsdynamikker som finnes der og hvordan disse påvirker myndighetenes styring, ble videre trukket frem som kjerneområder denne avhandlingen skal behandle. Forskning på myndighetenes holdninger om dette er viktig fordi det kan bidra til en bedre innsikt i hva som ligger bak politiske avgjørelser i forbindelse med myndighetenes overvåkning og styring på internett. I dette kapittelet vil jeg ta for meg den metodiske fremgangsmåten for å undersøke disse feltene nærmere.

Opprinnelig var betydningen av begrepet metode "veien til målet" (Kvale og Brinkmann, 2019, s. 140). På veien til mitt mål, som er å finne ut hva slags syn myndighetene har på narkotikadistribusjonen på det mørke nettet, har jeg valgt kvalitativ forskningsmetode. På bakgrunn av oppgavens problemstillinger og de teoretiske perspektivene som ble presentert i kapittel 3, er det mest hensiktsmessig å behandle kvalitative data i dette masterprosjektet. For å kunne gå i dybden på kontrollmyndighetenes holdninger til narkotikadistribusjon på det mørke nettet vil denne avhandlingen kombinere kvalitative forskningsintervju og kvalitativ dokumentanalyse. Mens de kvalitative intervjuene baseres på samtaler med ansatte i politi og toll som jobber med styring rettet mot narkotikadistribusjonen på det mørke nettet, tar dokumentanalysen utgangspunkt i offentlige rapporter som er publisert av Politidirektoratet, Oslo politidistrikt, Europol og EMCDDA.

Dette metodekapittelet vil i underkapittel 4.1 først beskrive hva som kjennetegner kvalitativ forskningsmetode med hovedfokus på de to metodene jeg har brukt for å samle inn det empiriske materialet: Kvalitative intervju og kvalitativ dokumentanalyse. Denne introduksjonen gjøres for å belyse hvorfor disse metodiske tilnærmingene egner seg til denne oppgaven. Videre i underkapittel 4.2 vil jeg først beskrive prosessen med rekruttering og utvalg for de kvalitative forskningsintervjuene og hvordan intervjuene ble gjennomført, før jeg i underkapittel 4.3 forklarer fremgangsmåten for utplukk av rapporter til dokumentanalysen. Deretter vil jeg dele mine betraktninger knyttet til forskningens kvalitet og fremstilling i underkapittel 4.4, som etterfølges av underkapittel 4.5 med en forklaring av hvordan analysen av det empiriske materiale har blitt utført. Avslutningsvis vil jeg presentere mine etiske refleksjoner knyttet til dette masterprosjektet i underkapittel 4.6.

4.1 Kvalitativ forskningsmetode og triangulering

I kvalitativ forskningsmetode henviser begrepet ”kvalitativ” til kvalitet, og i denne settingen refererer dette til egenskaper eller karaktertrekk ved fenomener (Repstad, 1987). For å oppnå en forståelse av sosiale fenomener er metoden kjent for å skape en nærhet mellom forsker og de som studeres (Thagaard, 2011). Kvalitativ forskningsmetode er hensiktsmessig å bruke til dette masterprosjektet fordi det bidrar til å fremme nyansene i de ulike synspunktene myndighetene har om narkotikadistribusjonen på det mørke nettet. For å gjøre dette vil jeg ta utgangspunkt i hermeneutisk tradisjon, som innebærer en vektlegging av fortolkning (Fangen, 2004). Oppgaven vil også ha et forstående formål, da jeg ønsker å forstå dybden av et spesifikt tema, nærmere bestemt, myndighetenes synspunkter om narkotikadistribusjonen på det mørke nettet (Bukve, 2016). Dette krever at jeg setter meg inn i de ulike holdningene og meningene myndighetene har til kryptomarkeder, og det gjør jeg vet å kombinere to metodiske tilnærminger: Kvalitative forskningsintervju og kvalitativ dokumentanalyse.

Kvalitativt forskningsintervju anses som den mest passende metoden for å forstå menneskers syn på et bestemt emne (Thagaard, 2011). Jeg har gjennomført kvalitative intervjuer av ansatte i politi og toll som jobber med styring rettet mot narkotikadistribusjonen på det mørke nettet med formål om å få frem bredden av deres holdninger til kryptomarkeder. Sellerberg og Fangen (2011) anbefaler å kombinere flere metodiske tilnærminger i større forskningsprosjekter. Derfor har jeg i tillegg til kvalitative intervju, valgt å foreta dokumentanalyse av noen offentlige rapporter som er publisert av Politidirektoratet, Oslo politidistrikt, Europol og EMCDDA. Fremfor å basere analysen på transkripsjon fra intervjuene alene, vil en kombinasjon med utdrag fra offentlige rapporter gi en større innsikt i myndighetenes synspunkter knyttet til narkotikadistribusjonen på det mørke nettet. Å kombinere to metodiske tilnærminger i et forskningsprosjekt kalles metodetriangulering. I denne masteravhandlingen har transkripsjonene fra de kvalitative intervjuene og utdrag fra de offentlige rapportene blitt triangulert til å analysere ett og samme tema (Fangen, 2004).

4.2 Kvalitative forskningsintervju

Kvalitative forskningsintervju skal skape et godt grunnlag for å få dybdeinnsikt i informanters erfaringer, tanker og følelser (Thagaard, 2011). Formålet med denne avhandlingen er å oppnå en bedre forståelse av myndighetenes erfaringer, tanker og følelser

knyttet til narkotikadistribusjon på det mørke nettet. De kvalitative intervjuene kan forklares som både deskriptive og fokuserte (Kvale og Brinkmann, 2019). De er deskriptive fordi de går i dybden av, og beskriver, de nyanserte synspunktene informantene har om det mørke nettet. At intervjuene omhandler et spesifikt tema, er nettopp det som gjør at intervjuene også anses som fokuserte. For dette masterprosjektet var det nyttig å velge ut myndighetspersoner som hadde kunnskap om dette fagområdet, og valget falt derfor på å intervjue personer som er ansatt i toll og politi som jobber med styring rettet mot narkotikadistribusjonen på det mørke nettet. Dette underkapittelet vil i det følgende ta for seg prosessen med rekruttering og utvalg av informanter, etterfulgt av en beskrivelse av intervjuenes gjennomføring.

4.2.1 Rekruttering og strategisk utvalg

For å innhente et relevant utvalg til et forskningsprosjekt er det avgjørende å tenke på hvem man velger ut som informanter (Creswell og Poth, 2018). For dette masterprosjektet har jeg intervjuet sentrale myndighetspersoner som jobber med styring rettet mot narkotikakriminalitet på det mørke nettet. Det mørke nettet er et relativt nytt forskningsområde, og det er et emne som ikke alle har utbredt kunnskap om (EMCDDA, 2017). Det var derfor nødvendig å velge ut myndighetspersoner som ville ha nok kompetanse om temaet til å kunne svare på spørsmål om deres holdninger knyttet til kryptomarkeder. Mitt utvalg av informanter anses derfor for å være strategisk, som vil si at informantene velges bevisst ut fra hva som skal forskes på og som har kvalifikasjoner som er strategiske i forhold til prosjektets problemstilling (Thagaard, 2011). For å kunne gjennomføre dette masterprosjektet ut ifra planen jeg hadde var det helt nødvendig å utføre rekrutteringen strategisk.

Rekruttering av informantene startet i februar 2020 og ble gjort ved at jeg benyttet meg av en portvakt. En portvakt er en sentral person i et miljø som har kunnskap om hvem som kan være relevant å snakke med i forbindelse med et forskningsprosjekt (Fangen, 2004). Gjennom en kontaktperson jeg kjenner fra min jobb i Tolletaten fikk jeg kontaktinformasjon til flere potensielle informanter. Jeg henvendte meg til de aktuelle personene på e-post med litt informasjon om prosjektet og med spørsmål om dette var noe de kunne tenke seg å være med på. Når de kom med positiv tilbakemelding, sendte jeg et informasjonsskriv (se vedlegg 1) med informasjon om prosjektets formål og hva det ville si å delta på et intervju. Når informantene fremdeles var positive til å stille til intervju etter å ha lest informasjonsskrivet,

ble det avtalt tid for gjennomføring. På denne måten kunne informantene ta en avgjørelse om deltakelse i prosjektet uten ytre press og etter å ha fått tilstrekkelig informasjon om hva det vil si å delta. På grunn av covid-19 pandemiens inntreden i Norge ble kontakten med flere informanter brutt før den i slutten av april 2020 ble gjenopprettet med de fleste. Det første intervjuet ble derfor gjennomført i mai 2020 og det siste i juni 2020.

Jeg rekrutterte informanter basert på et tilgengelighetsutvalg. Det vil si at informantene ble rekruttert både på bakgrunn av at de var relevante for dette prosjektet, og fordi de var tilgjengelig for meg (Thagaard, 2011). Til slutt satt jeg igjen med seks informanter som jobbet enten i Tolletaten eller i politiet, og med myndighetskontroll rettet mot narkotikadistribusjonen på det mørke nettet. Informantene hadde ulik utdanningsbakgrunn og arbeidserfaring. Utvalget bestod av både personer med operativ bakgrunn og sivilt ansatte som hadde høyere akademisk utdanning. Antall år med narkotikahandel på internett som arbeidsfelt strakk seg fra halvannet år til 15 år hos informantene. Formålet med intervjuene er ikke å oppnå statistisk representativitet, men snarere å finne et godt eksempel (Fangen, 2011). Til dette prosjektet kom jeg frem til seks gode eksempler på myndighetspersoner som kunne dele sine synspunkter om kryptomarkeder. Representativitet og validitet rundt rekrutteringen vil beskrives nærmere i underkapittel 4.4.2.

4.2.2 Gjennomføring

Etter at informantene hadde sagt seg villig til å stille til intervju, måtte jeg velge ut passende lokasjon for gjennomføring. Når man skal velge lokasjon til forskningsintervju, er det viktig å tenke på arenaer som intervjuobjektene kan føle seg mest fri til å snakke om ulike temaer (Thagaard, 2011). På grunn av covid-19 pandemien ble intervjuene gjennomført på ulike måter. To av intervjuene ble foretatt på et tilgjengelig møterom på informantenes arbeidsplasser. Dette er å anses som fordelaktig da dette er deres kjente og trygge område. Det var likevel ikke mulig å utføre alle intervjuene på informantenes arbeidsplasser på grunn av koronarestriksjoner. Derfor ble to av intervjuene gjennomført på et møterom i et av Tolletatens bygninger der jeg selv jobber, men utenfor min egen arbeidstid. Møterommet var i en annen etasje enn jeg ellers arbeider og rett på innsiden av inngangsdøren. På denne måten ivaretok jeg informantenes anonymitet, og ingen av mine kollegaer møtte på informantene. Selv om disse intervjuene ble holdt på min arbeidsplass fremfor deres, følte jeg ikke at det hadde særlig stor betydning. Jeg fikk inntrykk av at de snakket like fritt og var like tilpass

som de andre informantene.

På grunn av koronarestriksjoner, og etter ønske fra to av informantene, ble disse intervjuene avholdt på videosamhandlingssystemet Teams. Jeg benyttet mobiltelefon til videointervjuene og hadde lyden på høyttaler med båndopptaker liggende ved siden av. Begge disse intervjuene ble gjennomført etter at Norge hadde vært "lukket" noen måneder på grunn av covid-19. Begge informantene hadde derfor hatt hjemmekontor og brukt videosamhandlingssystemet Teams aktivt til møter i flere uker i forkant av intervjuene. I de senere årene har datastøttede intervjuer blitt svært utbredt (Kvale og Brinkmann, 2019). En stor fordel med dette er at man kan snakke med mennesker som ellers ikke ville vært tilgjengelig ved ordinært intervju, og nettopp på grunn av covid-19 pandemien var det tilfellet her. Uten denne datateknologien er det ikke sikkert at disse to intervjuene kunne blitt gjennomført, i alle fall ikke innenfor den begrensede tidsperioden jeg hadde til rådighet. Det kan tenkes at det er mindre personlig å gjennomføre et intervju over videotjeneste sammenlignet med et personlig møte. På den andre siden hadde hjemmekontor vært normen for de fleste den perioden, noe som gjør at videosamhandling nå har blitt en hverdagslig måte å gjennomføre møter på. Begge informantene oppholdt seg hjemme under videointervjuene og var derfor i sine egne kjente omgivelser. Selv om fire av intervjuene ble gjennomført ansikt til ansikt og to av intervjuene ble gjennomført over videosamtale viser innsamlet intervjudata at dette trolig ikke hadde særlig stor betydning.

Alle intervjuene ble lagt opp til å være delvis strukturerte. Det vil si at jeg på forhånd hadde planlagt fastlagte temaer forut for intervjuene, men rekkefølgen ble bestemt underveis slik at jeg kunne følge det informanten fortalte og samtidig sørge for å få informasjon om alle temaene jeg ville belyse. I tillegg gjør delvis strukturerte intervju det lettere å legge opp til at en informant kan ta opp emner som ikke er forberedt på forhånd (Thagaard, 2011). Jeg laget en intervjuguide (se vedlegg 2) før intervjuene som inneholdt temaer og forslag til spørsmål jeg ønsket å stille. Ved å ha delvis strukturerte intervjuer fikk jeg gjennomgått de temaene jeg ønsket samtidig som at intervjuene ble fleksible (Kvale og Brinkmann, 2019). Intervjuguiden ble justert litt etter det første intervjuet. Dette var fordi jeg følte at noen av spørsmålene måtte omformuleres, noen av spørsmålene måtte flyttes på og det kom opp flere temaer i det første intervjuet som jeg også ønsket å ta for meg i de andre intervjuene.

De første minuttene i et intervju er betydningsfulle og før informanter begynner å snakke fritt

ønsker de ofte en klar oppfatning av intervjueren (Kvale og Brinkmann 2019). Derfor fortalte jeg om min egen utdanningsbakgrunn samt litt om jobben min som ansatt i Tolletaten etter at vi hadde gjennomgått informasjonsskrivet og det informerte samtykket. Etter dette startet intervjuene med innledende spørsmål om informantenes arbeidserfaring og arbeidsoppgaver. Deretter stilte jeg spørsmål angående narkotikadistribusjon på det mørke nettet og kontrollen av disse markedsplassene. Informantene fikk først åpne og vide spørsmål angående deres meninger omhandlende narkotikahandel på det mørke nettet før de ble konfrontert med et par forskningsfunn om temaet. Dette var for å først kunne få frem informantenes egne meninger og synspunkter på generelt grunnlag uten å bli påvirket av forskningsfunnene jeg senere presenterte. Alle intervjuene bar preg av å gå litt frem og tilbake på de ulike temaene, noe som er vanlig i delvis strukturerte intervjuer (Fangen, 2004).

Intervjuene ble avsluttet med en debrifing hvor jeg lurte på om informantene hadde noe mer de ønsket å legge til eller om det var noe de lurte på. Noen brukte denne delen til å utdype flere av temaene fra intervjuet, mens andre ikke hadde mer å legge til. De seks intervjuene varte omkring 45 minutter, hvor det korteste var på 40 minutter og det lengste var på en time. Jeg forsøkte så godt det lot seg gjøre å fremstå nøytral til det som ble sagt og kom med flere oppfølgingsspørsmål. Jeg ga ofte oppmuntrende signaler med å si ”ja” og ”mhm”, i tillegg til at jeg hadde øyekontakt med informantene og nikket til det som ble sagt. Dette gjorde jeg for å signalisere min interesse for det informantene sa og for at de skulle fortsette å prate.

Det ble benyttet båndopptaker til intervjuene, og dette er som regel å foretrekke dersom man får tillatelse til det. Da vil alt som blir sagt bli bevart, man kan ha et større fokus på hva informanten sier fremfor å ta notater og dataene vil være fyldigere. Det var lett for meg å fokusere på det informantene sa og det var enklere å komme med relevante oppfølgingsspørsmål når jeg slapp å notere. Jeg hadde penn og papir fremfor meg i tilfelle jeg ønsket å notere ned noe underveis, men det ble ikke brukt på noen av intervjuene. Å notere underveis kan også redusere personlig kontakt med informantene (Thagaard, 2011). Det fremkom i informasjonsskrivet at det var ønskelig for meg å ta opp intervjuene på bånd, så det var ingen overraskelse for informantene at jeg tok frem båndtoppakeren. Likevel valgte jeg å vise båndopptakeren før hvert intervju og spurte om det var greit at jeg tok opptak. Samtlige informanter godtok dette og flere av informantene var kjent med båndopptaker fra før på grunn av deres egen jobb. Informert samtykke ble også gjennomført muntlig og bevart på lydopptakeren frem til prosjektets slutt. Dette var å foretrekke fremfor å oppbevare ark

med signaturer til alle informantene. I underkapittel 4.6.2 beskrives informert samtykke nærmere.

4.3 Dokumentanalyse

Dokumentanalyse har en lang tradisjon i kvalitativ forskning og det benyttes ofte i kombinasjon med intervju (Thagaard, 2011). Kvalitativ dokumentanalyse innebærer å analysere foreliggende materiale som er relevant for spørsmålene vi arbeider med å finne ut av i et forskningsprosjekt (Kalleberg, Malnes og Engelstad, 2009). For dette masterprosjektet har jeg derfor valgt å gjennomføre dokumentanalyse av offentlige rapporter som er publisert av diverse myndigheter i tillegg til de kvalitative intervjuene. Finstad (2006, s. 67) har uttrykt at ”Det politipolitiske skjønnet kan leses ut av offentlige utredninger, stortingsmeldinger og overordnete styringsdirektiver”. De offentlige rapportene vil analyseres for å finne ut hva myndighetene som har publisert dokumentene mener om narkotikadistribusjonen på det mørke nettet.

Dokumentanalyse handler om å sette dokumenter i en gitt kontekst (Lindgren, 2011). For å gjøre dette måtte jeg finne dokumenter som var relevant for temaet jeg skulle ta for meg i dette prosjektet. Jeg satt meg derfor flere kriterier for utvalg av rapportene til dokumentanalysen. Kriteriene innebar at dokumentene var offentlige, utstedt av offentlig myndighet, at de tok for seg temaet om kryptomarkeder og myndighetens utfordringer knyttet til dette, og at publikasjonene var fra 2017 til dagens dato. For å finne disse offentlige rapportene har jeg benyttet meg av søkemotoren Google til å søke etter publikasjoner som oppfylte kravene jeg hadde satt. Jeg forespurte også informantene jeg intervjuet til denne masteravhandlingen om de visste om dokumenter som oppfylte de nevnte kriteriene. Til slutt satt jeg igjen med to norske og fem internasjonale rapporter. I dette underkapittelet vil jeg først redegjøre for de norske rapportene jeg valgte ut for analyse, etterfulgt av en beskrivelse av de internasjonale rapportene.

4.3.1 Politidirektoratets trusselvurdering og Oslo politidistrikts rapport om trender

Basert på kriteriene jeg hadde satt meg og søkene jeg foretok, satt jeg igjen med to offentlige og nasjonale rapporter som tok for seg temaet om narkotikadistribusjonen på det mørke nettet. Den ene rapporten er ”Politidirektoratets trusselvurdering (2017): Trusler og

utfordringer med IKT-kriminalitet" (Politidirektoratet, 2017). Denne rapporten ble publisert i 2017 og er et resultat av et oppdragsbrev sendt til Politidirektoratet fra Justis- og beredskapsdepartementets på bakgrunn av deres strategi for å bekjempe IKT-kriminalitet. Dokumentet er skrevet av Kripos med støtte fra Politiets sikkerhetstjeneste (PST).

Den andre norske rapporten jeg har analysert i denne avhandlingen er "Trender i kriminalitet 2018-2021: Digitale og glokale utfordringer" (Oslo politidistrikt, 2018). Rapporten er publisert i 2018, og er skrevet for å gi en samlet fremstilling av kriminalitetsutviklingen i Oslo politidistrikt. Formålet med rapporten er å gi et styringsgrunnlag for politidistriktets øverste ledelse.

4.3.2 IOCTA og EMCDDA

I tillegg til de to norske politirapportene, kom jeg frem til fem internasjonale rapporter som oppfylte kravene jeg hadde satt for rapportene til dokumentanalysen. Tre av disse dokumentene er trusselvurderingsrapportene "Internet Organised Crime Threat Assessment" (IOCTA). Hvert år publiserer Europol IOCTA-rapporter, og dokumentanalysen håndterer rapportene fra 2018, 2019 og 2020. Europols mål med disse rapportene er å gi et overblikk på hvordan kriminalitetsutviklingen er, hvilke trusler man kan forvente i fremtiden, og trender av kriminalitet på internett. IOCTA-rapporten fra 2020 skiller seg litt fra de to foregående rapportene da de har benyttet kvalitative intervjuer fremfor kvantitative spørreundersøkelser.

De to siste rapportene som ble benyttet i dokumentanalysen er publisert av "European Monitoring Centre for Drugs and Drug Addiction" (EMCDDA), en etat i EU. Rapportene setter søkelys på land som er medlem av EU, samt Norge og Tyrkia. Den ene rapporten som omfattes av dokumentanalysen ble publisert i 2017 og har tittelen "Drugs and the Darknet: Perspectives for Enforcement, Research and Policy", (EMCDDA, 2017) og den andre rapporten har tittelen "EU Drug Markets Report" og ble utgitt i 2019 (EMCDDA, 2019).

4.4 Forskningens kvalitet og fremstilling

Frem til nå har dette metodekapittelet beskrevet hvordan det empiriske materialet har blitt samlet inn. Det er flere elementer knyttet til disse dataene som kan påvirke forskningens kvalitet, og dette vil beskrives nærmere i dette underkapittelet med utgangspunkt i kvalitetsindikatorene pålitelighet, gyldighet og generaliserbarhet. Selv om disse indikatorene

stammer fra kvantitativ forskning, er de også relevant når man skal vurdere kvaliteten av kvalitative studier (Brymann, 2012).

4.4.1 Forskningens pålitelighet

Forskningens pålitelighet, også kalt reliabilitet, innebærer forskningsresultatenes troverdighet og hvorvidt et resultat kan reproduseres på et annet tidspunkt av andre forskere (Kvale og Brinkmann, 2019). Dersom en annen forsker skulle anvendt samme metode som meg, er målet at vedkommende skulle kommet frem til et tilnærmet likt resultat. For å sikre god reliabilitet har jeg i dette metodekapittelet beskrevet de metodiske tilnærmingene jeg har brukt: Kvalitative forskningsintervju og kvalitativ dokumentanalyse. Jeg har også gjengitt hvordan det empiriske materialet er samlet inn, og i underkapittel 4.5 beskriver jeg hvordan dette er analysert.

Forskerens førforståelse og forkunnskaper kan ha innvirkning på pålitelighet (Halvorsen, 2008). Det er vanskelig, om ikke umulig, å kunne studere noe uten en viss førforståelse. Førforståelse kan også anses som viktig og nødvendig for å finne ut hva man skal se etter i forskningen. Jeg startet tidlig i prosessen med å tilegne meg kunnskap og lese meg opp på informasjon om det mørke nettet og narkotikadistribusjonen på kryptomarkeder for å starte idémyldringen. Informasjonen jeg hentet inn ble en del av det som kalles for en førforståelseshorisont, men det kan også ha vært med på å gi et større helhetsbilde enn hva jeg ellers ville hatt dersom jeg kun hadde samlet inn mitt eget materiale. Forkunnskapene jeg har med meg inn i dette prosjektet kan også være utgangspunktet for å stille gode spørsmål under intervjuene (Fangen, 2011).

Sammen med min førforståelse i form av informasjonsinnhenting og min tidligere studieerfaring, er den også basert på min arbeidserfaring som toller. Selv om det var jobben min som toller som gjorde at jeg først ble oppmerksom på og interessert i temaet om det mørke nettet, er det et fagfelt jeg aldri har jobbet med selv. Jeg anså derimot min bakgrunn fra Tolletaten som fordelaktig i forskningsintervjuene fordi jeg forstod informantenes ”sjargong”. Jeg følte også at vi kunne komme raskt inn på temaene jeg ønsket å ta opp uten å gå mange omveier med begrepsforklaringer. Samtidig hevdes det at å undersøke miljøer som forskere kjenner til fra før, kan være med på å redusere avstand mellom forsker og informant (Thagaard, 2011). I dette masterprosjektet har jeg intervjuet ansatte i Tolletaten hvor jeg selv

er ansatt, i tillegg til ansatte i politiet, som vi samarbeider mye med. Jeg kjente likevel ikke noen av mine informanter forut for intervjuene.

For at intervjudataene skulle oppnå størst grad av pålitelighet, stilte jeg mest mulig åpne spørsmål og fulgte opp det informantene sa med relevante oppfølgingsspørsmål. Dette var for å få mer dybde i svarene deres, men også for å kontrollere at jeg forstod det informantene sa på riktig måte. I avhandlingens analyse- og diskusjonskapittel bruker jeg hovedsakelig sitater fra informantene og direkte utdrag fra rapportene, noe som også kan forsterke forskningens pålitelighet ved at leser selv kan vurdere disse opp mot forskningens funn. En annen faktor som kan ha påvirket forskningens pålitelighet er en av informantenes forutsetning for å kunne stille til intervju. Denne forutsetningen var at informantens leder skulle få innsyn i den aktuelle informantens sitater som skulle bli brukt i masteravhandlingen. Det kan godt være at informanten hadde lederen sin i bakhodet gjennom hele intervjuet og at svarene derfor bar preg av dette. Dette vil i så fall være med på å kunne påvirke forskningens pålitelighet. Likevel følte jeg selv at han ga gode svar og jeg fikk ikke noe inntrykk av de var preget av at informanten ikke svarte slik vedkommende selv ønsket. Det var en annen informant som også ønsket å få tilsendt sitatene jeg kom til å benytte i denne avhandlingen. Å oversende sitater til informantene og få tilbakemelding på disse kan derimot være med på å styrke forskningens pålitelighet, da man utelukker eventuelle misforståelser eller feil.

4.4.2 Forskningens gyldighet

Gyldighet, også kalt validitet, kommer til anvendelse gjennom hele forskningsprosessen og innebærer at det er en sammenheng mellom problemstilling, studiens utforming og forskningsresultatene (Tjora, 2017). Utvikling av problemstilling, valg av metodisk tilnærming, utvalgsprosessen og til slutt innsamling av det empiriske datamaterialet kan påvirke forskningens gyldighet. I et forskningsprosjekt er ressurser i form av blant annet tid, økonomi, personell og tilgjengelighet begrenset. Dette gjør at man i en forskningssituasjon må foreta visse utvalgsbeslutninger, samtidig som man må tilstrebe å oppnå at forskningsresultatet skal gi best mulig bilde av virkeligheten (Kvale og Brinkmann, 2019).

Etter å ha definert en problemstilling er valg av metode en av de første beslutningene som kan påvirke forskningens gyldighet. Jeg har tidligere i dette metodekapittelet argumentert for at kvalitativ metode er best egnet til dette masterprosjektet for å finne ut hva myndighetene

mener om narkotikadistribusjonen på det mørke nettet og deres utfordringer knyttet til dette. Et annet moment som kan påvirke forskningens gyldighet er oppsettet av intervjuguiden (Kvale og Brinkmann, 2019). Å utarbeide en intervjuguide var en relativ omfattende prosess. Flere punkter ble vurdert og forkastet underveis. Riktignok var ikke intervjuguiden helt optimal og en liten del ble endret etter det første intervjuet. Dette kunne jeg unngått ved å preteste intervjuguiden, men jeg vurderer justeringen som relativ liten og at dette sannsynligvis har hatt moderat innvirkning på resultatet og videre på forskningens gyldighet.

For å tilstrebe at forskningsprosjektet oppnår størst mulig grad av gyldighet, er det viktig å velge ut et representativt utvalg slik at resultatet på best mulig måte beskriver virkeligheten (Thagaard, 2011). Etter å ha evaluert spørsmålene mine i intervjuguiden, var det neste jeg vurderte hvorvidt det kan foreligge en viss utvalgsproblematikk i prosjektet mitt. Resultatene fra informantene skal i utgangspunktet gjenspeile holdningen til den totale mulig populasjonen (Kvale Brinkmann, 2019). Det vil si at utvalget mitt optimalt skulle vært representativt for alle myndighetspersoner innenfor toll og politi som jobber med narkotikadistribusjon på det mørke nettet. Selv om jeg kun har seks informanter er den totale mulige populasjonen for informasjon såpass begrenset at jeg vurderte mulige validitetsproblemer innenfor dette feltet som relativt liten. Kontroll på det mørke nettet er et arbeidsfelt relativt få arbeider med, og flere av informantene poengterte at det per dags dato ikke eksisterer en egen patrulje med tjenestepersoner som kun jobber med kontroll av narkotikadistribusjonen på det mørke nettet. På den andre siden er det heller ikke et formål med denne masteravhandlingen å oppnå statistisk representativitet, men som tidligere nevnt i dette metodekapittelet, snarere å finne et godt eksempel (Fangen, 2011).

4.4.3 Forskningens generaliserbarhet

Den siste kvalitetsindikatoren jeg vil ta for meg er generaliserbarhet. Generaliserbarhet betyr at denne forskningen kan være relevant utover det som har blitt forsket på her. Det kan argumenteres for at generaliserbarhet ikke alltid er ønskelig eller oppnåelig i kvalitativ forskning (Brymann, 2012). Denne studien kan være vanskelig å generalisere til en hel populasjon, men det er heller ikke hensiktsmessig i dette tilfellet. Avhandlingen skal ta for seg nyanser av ulike syn som myndighetspersoner har på den krypterte formen for markedskriminalitet, men det kan ikke generaliseres til hva alle som jobber med dette mener om temaet. Forskningen utforsker de norske kontrollmyndighetenes synspunkter, med innfall

av noen europeiske myndigheters holdninger basert på utdrag fra offentlige rapporter. Samtidig kan man med denne masteravhandlingen som utgangspunkt, få en generell innsikt i hvordan kryptomarkeder kan overvåkes og håndteres av myndighetene.

4.5 Deduktiv, induktiv og abduktiv tilnærming

Denne avhandlingen har et formål om å finne ut hva slags syn myndighetene har på narkotikadistribusjonen på det mørke nettet. På veien har jeg tatt flere avgjørelser som har påvirket avhandlingens forskningsfunn. Arbeidet med denne masteravhandlingen startet med en deduktiv tilnærming, som betyr at teori testes i henhold til innsamlet datamateriale (Thagaard, 2011). Allerede under arbeidet med avhandlingens prosjektbeskrivelse hadde jeg i utgangspunktet sett for meg politikultur som en hovedteori og ønsket å knytte dette opp mot kontrollmyndighetenes side av narkotikadistribusjon på det mørke nettet. Dette endret seg etter hvert som prosjektet begynte å ta form, og datamateriale ble innhentet. Jeg gikk over til å utvikle mitt analytiske prosjekt med bruk av sosiologiske og kriminologiske teorier om digitalisering, overvåkningsperspektiver og governmentality. Disse teoriene viste meg ny innsikt i kriminalpolitiske perspektiver, og derfor anså jeg de som mer passende til denne oppgaven. På denne måten utviklet masterprosjektet seg i en mer induktiv retning på bakgrunn av å være mer empiribasert fremfor å basere seg på testing av teori. En induktiv tilnærming vil være mer fleksibel og ha få retningslinjer som styrer informasjonen som innhentes (Kvale og Brinkmann, 2019).

Kvalitative studier har tradisjonelt hatt induktiv tilnærming, men de fleste kvalitative forskningsbidrag i dag kan karakteriseres ved en veksling mellom induktive og deduktive faser. Det vil si at forskeren veksler mellom å basere seg på empiriske observasjoner og utviklingen av ideer fra teoretiske perspektiver (Fangen, 2004). I arbeidet med denne avhandlingen startet jeg med et teoretisk utgangspunkt, men dette endret seg etter hvert som jeg intervjuet informantene og leste rapportene til dokumentanalysen. Dette beskriver hvordan prosessen gikk over til å behandle et samspill mellom induktiv og deduktiv tilnærming, en kombinasjon som kalles for abduktiv tilnærming. Abduktiv tilnærming baserer seg på at man forholder seg til empiri, men anerkjenner betydningen av teorier og perspektiver enten i forkant av eller i løpet av forskningsprosessen (Kvale og Brinkmann, 2019). I løpet av denne masteravhandlingens prosess har min tilnærming vært abduktiv fordi jeg har vekslet mellom empiri og teori. I det følgende skal jeg gå nærmere inn på hvordan jeg

har analysert det empiriske materialet. Først vil jeg ta for meg de analyseprosessen med de kvalitative intervjuene, deretter vil jeg gjøre det samme for dokumentanalysen.

4.5.1 Fra intervju til analyserte sitater

Analyse og tolkning i et forskningsprosjekt starter allerede ved etablering av kontakt med informantene. Videre vil analysen påvirke beslutninger knyttet til hvilke temaer som skal utdypes i intervjuene, noe jeg tidligere har beskrevet gjennomføringen av i dette metodekapittelet. En viktig fase i analysearbeidet i forbindelse med kvalitativ metode er tidspunktet fra kontakten mellom forsker og informant er avsluttet (Thagaard, 2011). Dette tar oss videre til prosessen hvor intervjuene går fra å være muntlige samtaler og til skriftlig tekst. Å transkribere betyr å skifte fra en form til en annen og transkripsjoner er oversettelser fra talespråk til skriftspråk (Kvale og Brinkmann, 2019). I denne fasen skifter den muntlige informasjonen fra intervjuene over til skriftlig informasjon. Alt av intervjumateriale fra båndopptakeren er transkribert og det er kun gjort av meg. Transformering av lydfilene fra lydopptakeren til skriftlig form gjør at det blir lettere å få oversikt over dataene, samtidig som at det er begynnelsen på selve analysen.

I min transkripsjon har jeg til en viss grad forsøkt å bevare språkets muntlige form. Det vil si at jeg har beholdt setningene slik de fremkom i intervjuene, men jeg har fjernet lyder som for eksempel ”hmm” og ”ehm”. Jeg har også redusert antall utfyllingsuttrykk i sitater der det ble brukt mye. Dette er ord som ofte brukes i dagligtalen, blant annet ord som ”altså”, ”da” og ”liksom”. Det er avhandlingens formål som vil påvirke hvor detaljert transkripsjonen er nødt til å være (Halvorsen, 2008). Jeg var ute etter å studere myndighetenes synspunkter om det mørke nettet gjennom deres generelle beskrivelser, og jeg regnet derfor ikke med at disse omskrivingene ville ha innvirkning på analysen. Jeg betrakter derimot denne omskrivingen som fordelaktig i og med at deres synspunkter kommer tydeligere frem når det ikke er så mange utfyllingsutrykk. Jeg har også skrevet om eventuelle dialekter til bokmålsform for å ivareta informantenes anonymitet, da det i denne avhandlingen ikke har vært relevant å fokusere på dialekter.

Jeg har benyttet meg av en temasentrert analytisk tilnærming, som vil si at temaene, eller kategoriene, er i fokus. Analyse av materiale som er basert på temasentrerte tilnærminger, innebærer at vi sammenligner informasjon om hvert tema fra alle intervjuene. Hovedformålet

med dette er å gå i dybden på de enkelte temaene (Thagaard, 2011). For å systematisere og sortere tekstene jeg hadde transkribert, benyttet jeg Nvivo analyseverktøy. Der laget jeg ulike kategorier for å få et økt fokus på de temaene jeg ville ta for meg, mens mindre relevante ting fra intervjuene ble analysert i mindre grad. Denne prosessen her kalles for abstraksjonsprosessen (Sollund, 2007). Abstraksjonsprosessen var basert på at jeg lagde ulike kategorier, eller koding som det også kalles (Kvale og Brinkmann, 2019).

Jeg lagde et kodenotat hvor jeg skrev ned betegnelsene på de ulike kodene og bruke Nvivo analyseverktøy til å hjelpe meg med å sette sitater fra de ulike intervjuene sammen i de kategoriene de hørte til. Noen av kodene sprang ut fra de ulike temainndelingene i intervjuene, inkludert temaene *vold* og *tilgjengelighet av farlige narkotiske stoffer* som jeg har blitt inspirert til å bruke på bakgrunn av den aktuelle forskningen jeg presenterte i kapittel 2. *Nedstenging av markedsplasser* var et annet tema jeg hadde i intervjuene, og dette var på bakgrunn av min inspirasjon fra governmentalityteori. Andre koder ble til på bakgrunn av intervjuene, og ble derfor laget etter at jeg hadde gjennomført transkriberingen. Disse kodene var for eksempel *forebygging* og *samfunnsproblem*. Utfordringene med koding kan være at utdragene blir tatt ut fra den opprinnelige konteksten og inn i en ny kodet kontekst (Brymann, 2012). For å minimere sjansene for å miste den sosiale settingen sitatene er tatt ut fra, tok jeg også med mitt spørsmål sammen med sitatene som ble kodet. Dersom det var en gjennomgående samtale om et gitt tema over flere sitater med flere oppfølgingsspørsmål av meg, markerte jeg alt og kodet dette samlet.

4.5.2 Fra offentlige rapporter til analyserte dokumenter

Når det kommer til dokumentanalysen, gikk jeg inn i de offentlige rapportene jeg hadde valgt basert på kriteriene jeg hadde satt meg, noe jeg tidligere har gjort rede for i dette metodekapittelet. Deretter tok jeg ut de kapitlene som berørte temaene narkotikadistribusjon på det mørke nettet og gikk gjennom disse. Videre anvendte jeg det som stod i de offentlige rapportene med denne masteravhandlingens problemstillinger og temaer. Utdragene fra rapportene som jeg ønsket å bruke kodet jeg i Nvivo analyseverktøy sammen med sitatene fra intervjuene. Jeg brukte de samme kodene for rapportene som for de kvalitative intervjuene. Jeg besluttet at dette var den mest systematiske måten å gjøre dette på, i og med at sitatene fra intervjuene og utdragene fra rapportene skulle trianguleres til å analysere ett og samme tema (Fangen, 2004).

Sammenlignet med data som forskeren selv har samlet inn i felten, skiller dokumentanalyser seg fra dette ved at dokumentene er skrevet for et annet formål enn det forskeren skal bruke dem til (Thagaard, 2011). Jeg har samlet inn mitt eget intervjumateriale, men for dokumentanalysen har jeg tatt myndighetenes rapporter ut av dens opprinnelige kontekst, tolket disse, og anvendt det til min avhandling. Rapportene er likevel relevant til denne avhandlingen fordi de er publisert av offentlig myndighet, og omhandler det mørke nettet i lys av kontroll på kryptomarkeder. Disse rapportene kan derfor uttrykke myndighetenes meninger knyttet til narkotikadistribusjon på krypterte internettplattformer.

4.6 Etiske refleksjoner

Forskningsetikk kommer til anvendelse i de tilfellene hvor forskere må forholde seg til etiske problemstillinger (Materstvedt, 2018). Som forsker må man skape en balanse mellom ønsket om å innhente interessant kunnskap i forskningen og respekt for informantenes integritet (Kvale og Brinkmann, 2019). Det foreligger flere etiske dilemmaer til de ulike prosessene i forskningen. De nasjonale forskningsetiske komiteer (NESH) har utarbeidet forskningsetiske retningslinjer for å gi kunnskap til forskere om de forskningsetiske normene. Dette har de gjort for å skape god vitenskapelig praksis og for å forebygge vitenskapelig uredelighet (NESH, 2016).

En del av NESH (2016) sine retningslinjer sikter til personvern. The General Data Protection Regulation (GDPR) var en ny personvernlov som kom til anvendelse i Norge den 20. juli 2018. Den trådde i kraft på bakgrunn av ønsket om en felles personvernopplysningslov for Den europeiske union hvor formålet blant annet var å sikre vern av personopplysninger (Regjeringen, 2018). I og med at dette masterprosjektet skulle behandle personopplysninger falt det inn under denne personopplysningsloven. Jeg kommuniserte med informantene hovedsakelig gjennom e-post, men jeg hadde noen samtaler via telefon. Jeg skulle også oppbevare lydopptak fra intervjuene på båndopptaker frem til prosjektets slutt. Det var derfor klart at dette prosjektet ville innebære behandling av personopplysninger. På bakgrunn av dette, meldte jeg masterprosjektet inn til Norsk samfunnsvitenskapelige datatjeneste (NSD) og fikk det godkjent (se vedlegg 3). Det ble besluttet å ikke søke Politidirektoratet eller Tolldirektoratet da dette prosjektet ikke var ute etter taushetsbelagt informasjon.

4.6.1 Informert samtykke

For å kunne sikre informanters integritet er informert samtykke, konfidensialitet og utgivelse av informasjon om mulige konsekvenser av å delta i forskningsprosjektet nødvendig (NESH, 2016). Informert samtykke innebærer at informantene skal få informasjon om forskningsprosjektets hovedformål og om mulige risikoer ved å delta i prosjektet (Fangen, 2004). NESH (2016) sine retningslinjer uttrykker at det informerte samtykket skal være fritt, og uten å være utsatt for noen form for press. Dette innebærer at man sikrer at informantene deltar frivillig og får informasjon om deres rett til å trekke seg fra forskningsprosjektet når som helst. Dette er viktig, fordi det innebærer en respekt av menneskers evne til å fatte egne beslutninger samtidig som at det vil være med på å sikre at informantene ikke skal ta skade av å delta i prosjektet. NESH (2016) sine prinsipper innebærer videre at informantene skal få tilstrekkelig med informasjon om forskningsfeltet, hva som er forskningens formål, hvem som har tilgang til informasjonen, hvordan resultatene er tenkt brukt og potensielle følger ved å delta. Kombinert med et fritt og informert samtykke, uttrykker NESH (2016) viktighetene av at det også er uttrykkelig. At samtykket er uttrykkelig innebærer at informantene gir klart uttrykk for at de forstår hva det innebærer å delta i forskningsprosjektet.

Før jeg avtalte intervju med mine informanter oversendte jeg et informasjonsskriv (se vedlegg 1) på e-post, med informasjonen NESH (2016) henviser til. Etter at informantene hadde lest informasjonsskrivet jeg hadde sendt på e-posten planla vi tid for intervju. Hvert intervju startet med informert samtykke inneholdende spørsmål om personene hadde lest informasjonsskrivet og om de hadde forstått informasjonen (se vedlegg 2). Deretter ga jeg informantene mulighet til å stille spørsmål dersom det var noe i informasjonsskrivet eller annet ved prosjektet som var uklart. Til slutt stilte jeg spørsmål om de samtykket til å delta, og at de nevnte personopplysningene om dem ble behandlet frem til prosjektets slutt. Informantene måtte svare bekreftende på dette for at samtykket skulle være gjeldende og intervjuene kunne starte. Det muntlige informerte samtykket ble frem til prosjektets slutt bevart sikkert på båndopptaker i låsbart skap som kun jeg hadde tilgang til.

4.6.2 Konfidensialitet og konsekvenser ved å delta

I informasjonsskrivet fremkom det også informasjon om konfidensialitet og hvem som har tilgang til deres personopplysninger. De som skal gjøres til gjenstand for forskning har krav på at all informasjon de deler blir behandlet konfidensielt (NESH, 2016). Som tidligere nevnt

i metodekapittelet, benyttet jeg meg av en portvakt for rekruttering av informanter. Dette kan potensielt utfordre punktet om konfidensialitet. I dette prosjektet fikk jeg kun kontaktinformasjon til flere potensielle informanter av portvakten, og portvakten vet ikke hvem jeg endte opp med å rekruttere til dette masterprosjektet.

Konfidensialitet innebærer også at forskningsmaterialet må anonymiseres samt at informasjon må oppbevares sikkert og tilintetgjøres ved prosjektslutt (Thagaard, 2011). Når det kommer til oppbevaring av personlig informasjon, ble båndopptakeren oppbevart i et låsbart skap som kun jeg hadde tilgang til. Videre vil informantenes personlige informasjon i form av opptak på båndopptakeren makuleres ved prosjektets slutt i november 2020. At informantene anonymiseres, vil si at deres personlige opplysninger ikke publiseres i masteravhandlingen. For å beskytte informantenes personvern, men fremdeles kunne skille på dem, har jeg i denne oppgaven byttet ut informantenes virkelige navn med fiktive navn (Kvale og Brinkmann, 2019). Jeg har valgt å gi alle informantene herrenavn, da jeg ikke ønsker å avsløre informantenes kjønn. Informantenes alder eller etnisitet vil heller ikke bli presentert, da det ikke er relevant for denne oppgaven. Det er et nokså begrenset antall mennesker som jobber med styring rettet mot narkotikadistribusjonen på det mørke nettet i Norge. Derfor valgte jeg å ikke gå nærmere inn på hvem som jobber på hvilket arbeidssted utover at alle de seks informantene er enten ansatt i politiet eller i Tolletaten. Jeg refererer derfor til alle informantene som kontrollører i denne avhandlingen. For å ivareta informantenes anonymitet har jeg i denne avhandlingen også utelatt deler av deres utsagn som potensielt kunne inneholde identifiserbar informasjon.

Retten til beskyttelse av personlig informasjon innebærer at informanten ikke skal kunne identifiseres. Det er særlig i forbindelse med forskerens fortolkning av informanten at dette er et problem. Informanten kan bli konfrontert med et perspektiv på seg selv og sin situasjon som han eller hun verken kan eller vil bli konfrontert med (Thagaard, 2011). Som nevnt tidligere, var forutsetningen til den ene informanten for å kunne delta i prosjektet at vedkommens leder måtte få oversendt sitatene jeg skulle bruke i masteravhandlingen. Dette løste jeg ved å sende sitatene til informanten, slik at det var opp til informanten selv å eventuelt videreformidle dette til leder. Det var også en annen informant som ønsket å få oversendt sitatene jeg tenkte å benytte i oppgaven. Dette kan, som jeg tidligere har nevnt under kapittelet om forskningens pålitelighet, også være med på å styrke forskningen. Ved å sende sitatene deres til dem på e-post før jeg skulle bruke de i avhandlingen, fikk

informantene mulighet til å gi tilbakemelding til dette slik at potensielle misforståelser eller feil kunne lukes vekk.

I tillegg til ivaretakelse av konfidensialitet, er det viktig å reflektere over hvorvidt informantene vil ta skade av å delta i forskningen. Det anses å ha minimale konsekvenser å delta i dette masterprosjektet og informantene vil trolig ikke ta skade av å delta i disse intervjuene. Temaet for intervjuene er verken av personlig karakter eller omhandler såre temaer. Som forklart i dette underkapittelet, er de fleste potensielle negative konsekvensene knyttet til konfidensialitet ivaretatt.

4.6.3 Etiske refleksjoner knyttet til dokumentanalysen

Det er også etiske utfordringer knyttet til en dokumentanalyse. Fordelen med dokumentanalyse er at underliggende syn og rasjonaliteter i en organisasjon kan komme frem i publikasjoner (Bryman, 2012). Jeg har i dette prosjektet analysert rapporter som er publisert av Politidirektoratet, Oslo politidistrikt, Europol og EMCDDA. Jeg har gjort det med formål om å avdekke deres meninger om kryptomarkeder og deres utfordringer knyttet til denne formen for markedskriminalitet.

Noen er skeptiske til en slik dokumentanalyse, i og med at rapportene i utgangspunktet er skrevet for et annet formål. I min dokumentanalyse av rapportene blir tekstene tatt ut av sin opprinnelige kontekst og anvendt til mitt prosjekt. Man kan ikke spørre et dokument om det som fremkommer av informasjon, og derfor kan opplysningene i noen tilfeller miste sin opprinnelige kontekst. Denne interpretasjonen av informasjon var jeg imidlertid nødt til å gjøre selv før jeg anvendte utdragene til temaene til dette masterprosjektet. Jeg har også hovedsakelig fremstilt direkte utdrag fra rapportene i analysen. Slik vises det som faktisk står i dokumentene før det blir anvendt til mitt tema, og leseren kan selv se hva som opprinnelig stod i rapportene. Det er også verdt å nevne at offentlige rapporter som er publisert av offentlig myndighet ofte er skrevet med offentligheten i tankene (Bryman, 2012). Alt tatt i betraktning, vil rapportene gi en orientering om myndighetenes standpunkter knyttet til det mørke nettet, og spesielt sammen med intervjumaterialet vil dette være fruktbar data. Dette leder oss videre til analyse- og diskusjonskapittelet, hvor det empiriske materialet analyseres.

5 Analyse og diskusjon

Sunde og Sunde (2019) belyser den teknologiske utviklingen i samfunnet med å bruke metaforen ”hurtigtog” for å forklare at det teknologiske hele tiden oppnår raskere fart, blir mer avansert og får flere passasjerer om bord. Derfor er det viktig å forske på områder hvor den teknologiske utviklingen til enhver tid påvirker samfunnet. Med denne analysen vil jeg bidra til kunnskap om en ny plattform som narkotikahandelen har fått fotfeste i på bakgrunn av den teknologiske og digitale utviklingen - det mørke nettet. I dag vet vi ikke nok om hva myndighetene mener om digitalisering og narkotikadistribusjon, men i dette analyse- og diskusjonskapittelet vil jeg bidra med kunnskap om myndighetenes holdninger til dette feltet. Dette bidraget innebærer en beskrivelse av hva myndighetene anser som utfordrende med kryptomarkedene, en kartlegging av overvåkningsdynamikkene på det mørke nettet, og en presentasjon av hvordan disse elementene kan påvirke myndighetenes styring. Analyse og diskusjon vil foregå parallelt, og sammen med teoretiske perspektiver vil denne sammenflettingen gi en større innsikt i disse temaene.

Det empiriske materialet er basert på kvalitative intervju og dokumentanalyse. Jeg har intervjuet seks norske myndighetspersoner som er ansatt i toll og politi, og som jobber med kontroll av narkotikadistribusjonen på det mørke nettet, heretter referert til som kontrollører. Dokumentanalysen jeg har utført baserer seg på rapporter publisert av Politidirektoratet, Oslo Politidistrikt, Europol og EMCDDA. I Norge og ellers i Europa har diskusjonen rundt narkotikahandel fått stor plass i politikken, og det blir brukt mye ressurser rettet mot narkotikakontroll. Norge har vært et av de strengeste landene i kampen mot narkotika, og i dag kan man få opptil 21 års fengsel for narkotikakriminalitet - den lengste fengselsstraffen man kan få i Norge (Christie, 2000). I denne avhandlingen vil jeg presentere funn om myndighetenes meninger knyttet til narkotikadistribusjon på det mørke nettet, og med det kan vi finne ut mer om hva som ligger bak den strenge kriminalpolitikken rettet mot narkotika. Oppgavens overordnede problemstilling er i den hensikt formulert på følgende måte: *Hva slags syn har myndighetene om narkotikadistribusjonen på det mørke nettet?*

For å forklare myndighetenes synspunkter knyttet til det mørke nettet vil governmentalityteori anvendes. Governmentality består av statens evne til å styre borgerne, og deres evne til å få borgerne til å styre seg selv. Dette gjøres gjennom bestemte måter å

tenke på (rasjonaliteter), gjennom spesifikke måter å handle på som påvirker styringen (teknologier), samt myndighetenes maktutøvelse mot samfunnsborgerne (Garland, 1999). Basert på et governmentalityperspektiv vil staten derfor styre ut ifra iboende rasjonelle prinsipper eller lover (Neumann, 2003). Det første av tre underproblemstillinger som vil bli besvart i dette analyse- og diskusjonskapittelet er: *Hvilke faktorer står bak myndighetenes rasjonalisering av ressurser rettet mot styring på det mørke nettet?* For å svare på dette vil jeg i underkapittel 5.1 argumentere for at det oppstår en tosidig spenning hos kontrollørene som omhandler de ulike funksjonene på krypterte nettverk med utgangspunkt i anonymitet. Synspunkter som myndighetene har om andre utfordringer knyttet til det mørke nettet utover kryptering og anonymitet vil presenteres i underkapittel 5.2. De tre elementene som vil trekkes frem her er egenskapene med det mørke nettet knyttet til digital vold, tilgjengelighet av farlige narkotiske stoffer og andre samfunnsmessige konsekvenser som følger av narkotikakriminalitet.

Myndighetenes rasjonalisering av ressursbruk rettet mot det mørke nettet leder videre til overvåkning på kryptomarkedene og oppgavens andre underproblemstilling: *Hvordan foregår overvåkningsdynamikkene mellom kontrollører, narkotikaselgere og narkotikakjøpere på de krypterte markedsplassene?* Dette vil besvares i underkapittel 5.3 med en kartlegging av disse ved å ta i bruk perspektiver basert på panoptikon og surveillant assemblage. Som tidligere nevnt i teoridelen, baserer Foucaults panoptikonmodell på en overvåkningspraksis hvor fangevokterne kan se fangene i fengslene, men fangene er uvitende om de blir overvåket eller ikke (Foucault, 1979). For å forklare hvordan overvåkning foregår på det mørke nettet, vil jeg i likhet med flere andre forskere før meg argumentere for at panoptikonmodellen ikke er tilstrekkelig alene, og at modellen derfor må suppleres med andre perspektiver inkludert synoptikon, sousveillance, dataveillance og lateral surveillance (Mathiesen, 1997; Mann og Ferenbok, 2013; Lupton, 2015; Adrejevic, 2005).

Selv med supplerende overvåkningsmodeller basert på Foucaults panoptikon, vil jeg vise at surveillant assemblage vil forklare overvåkningen på det mørke nettet på en mer helhetlig måte. Surveillant assemblage baserer seg på at overvåkning skjer fra alle kanter i en form der alt er tilkoblet hverandre (Haggerty og Ericson, 2000). I dette analyse- og diskusjonskapittelet vil jeg også videreutvikle konseptet datadoubles som Haggerty og Ericson (2000) presenterer. Datadoubles er små elektroniske koder som omhandler informasjon fra våre fysiske kropper, og det argumenteres for at på grunn av det digitale

formatet av data, virker det som om våre datadoubles ikke lenger er knyttet til våre fysiske kropper (Lyon, 2007). Jeg vil ta datadoublesperspektivet et steg videre og vise hvordan myndighetenes overvåkning på kryptomarkeder fører til at personers datadoubles kan brukes som identitetsmarkører til å spore tilbake til de fysiske kroppene.

Etter en kartlegging av overvåkningsdynamikkene på det mørke nettet, vil myndighetenes styring knyttet til narkotikadistribusjonen på det mørke nettet illustreres på bakgrunn av avhandlingens tredje underproblemstilling som er følgende: *Hvordan påvirker overvåkningsdynamikkene myndighetenes styring på kryptomarkedene?* Underkapittel 5.4 vil besvare dette ved å skissere myndighetenes synspunkter om styring rettet mot narkotikadistribusjonen på det mørke nettet med fokus på forebygging og nedstenging av markedsplasser.

5.1 ”Men digitalt skal det være så identitetsløst”: De krypterte nettverkenes tosidighet

Det mørke nettet legger til rette for at man kan opptre anonymt, og det eksisterer mange ulike oppfatninger om akkurat dette. De forskjellige meningene kommer på bakgrunn av det som kan belyses som et samfunnsdilemma mellom frihet og kontroll (Tzanetakis, 2017). For noen betraktes kryptomarkeder som åsteder, mens for andre er det plattformer som uttrykker selvstendighet (Bancroft, 2019). På den ene siden benytter noen seg av krypterte nettverk på bakgrunn av personvernhensyn, menneskerettigheter og internettfrihet (Dupont, 2008). Denne bruken gjøres med hensikt for å gjennomføre trygg kommunikasjon. På den andre siden legger krypterte nettverk til rette for ulovlige aktiviteter. Ifølge offentlige rapporter publisert av Europol (IOCTA, 2018) og EMCDDA (2016) innebærer dette kriminelle aktiviteter som terrorplanlegging, deling av barnepornografi og kjøp og salg av narkotiske stoffer. Krypterte nettverk innehar mangfoldige funksjoner, og myndighetspersoner har delte meninger om dette. Å få kunnskap om myndighetenes meninger knyttet til det mørke nettet er betydningsfullt, fordi deres syn på narkotikadistribusjonen kan ha politiske konsekvenser i form av styring og overvåkning.

Krypterte nettverk basert på Onion Routing var ikke utviklet med formål om å være en plattform for kriminelle handlinger, men ble produsert av det amerikanske forsvaret for å

holde sensitiv informasjon hemmelig (EMCDDA, 2017). Onion Routing fungerer ved at kommunikasjon ikke foregår direkte, men går gjennom en programvare som består av flere lag. Den første etablerte programvaren for Onion Routing var programvaren som refereres til som TOR (AlQahtani og El-Alfy, 2015). Det som opprinnelig var laget for at sensitiv informasjon ikke skulle bli overvåket av uvedkommende, benyttes nå av samfunnsborgere til blant annet ulovlige aktiviteter, og som myndighetene aktivt overvåker. Jeg vil senere i avhandlingen beskrive hvordan de krypterte nettverkene som i utgangspunktet var funnet opp for å være motstand til overvåkning, nå til stadighet blir overvåket.

To år etter at det amerikanske forsvaret utviklet anonymiseringsprogrammet TOR, ble kildekoden frigitt for videreutvikling på bakgrunn av midler fra diverse selvstendige bedrifter og den ideelle organisasjonen Free Haven Project (EMCDDA, 2017). I dag er TOR fremdeles den foretrukne programvaren på det mørke nettet blant kriminelle (Europol, 2020). Tanken, og utviklingen av et program som kunne skjule digitale spor til brukere, var i utgangspunktet å ha en plattform for beskyttet og trygg kommunikasjon. Kontrolløren Peder trekker frem sine synspunkter omkring dette:

> Altså, det er jo det det egentlig var beregnet for da. Trygg kommunikasjon, rett og slett. Hvis du lever i en totalitær eller autoritær stat hvor myndighetene overvåker kommunikasjon og du er uenig med myndighetene, så kan du kommunisere fritt ved å bruke det mørke nettet. Det er jo positivt. […]

Denne informanten mener det mørke nettet kan være nyttig for fri kommunikasjon dersom man bor i en totalitær stat. Selv om programvaren TOR i utgangspunktet ikke ble laget for ulovlige aktiviteter, har imidlertid begrepet ”darknet”, oversatt til det mørke nettet på norsk, mystiske, kriminelle og truende assosiasjoner (Tzanetakis, 2017). I dag er det fremdeles noen som benytter seg av det mørke nettet med legale hensikter, for eksempel menneskerettighetsorganisasjoner som vil beskytte personers identitet mot autoritære regimer, eller personer som bare ønsker å uttrykke seg anonymt på bakgrunn av ytringsfrihet (Dupont, 2008; Mirea, Wang og Jung, 2019). Det er ikke bare kriminelle som ønsker å være anonyme på internett, det mørke nettet kan også være et fristed for personer med lovlige intensjoner. Kontrolløren Kjetil hevder at det mørke nettet også kan brukes for varslinger til media: ”Se på varslersaker - medier som har oppretta egne kanaler på det mørke nettet for varslinger til media. Der kan det absolutt være nyttig”. Med dette sitatet anerkjenner denne

informanten at det kan være positivt for samfunnet at personer kan melde informasjon anonymt til journalister. Anonymiteten som TOR og andre lignende Onion Routing programvarer legger til rette for, og som kan være med på å skjule digitale spor, vil også bidra til at informasjon kan komme ut til samfunnet. Journalister kan innhente informasjon om saker som kanskje ellers aldri ville sett dagens lys.

Riktignok er av de viktigste temaene innenfor nyere sikkerhetsstudier i overvåkningsfeltet, analyse av forholdet mellom økt overvåkning og personvern (Salter, 2010). Utviklingen i teknologi og digitalisering er i dag basert på stordata og algoritmer, noe som kan føre til økt overvåkning og statlig styring. Tzanetakis (2017) mener at dette kan bidra til mindre frihet og trussel mot personvern. Stordata refererer til den store mengden med moderne databaser og teknikkene for å analysere meningen med disse dataene (Boyd og Crawford, 2012). Algoritmer kan defineres som en rekke med datakoder som forteller maskinen hvordan man skal fortsette videre basert på en serie av instruksjoner for å komme frem til et spesielt sted (Lupton, 2015). Ved bruk av stordata og algoritmer oversettes digital data fra personer, ting, handlinger og relasjoner til informasjon som kan lagres, håndteres og visualiseres av maskiner (Bellanova, 2017). Dette skaper en diskusjon om ivaretakelse av menneskers rettigheter i forbindelse med personvern, og et argument for å benytte seg av det mørke nettet for deling av informasjon kan være ønsket om å beskytte sin personlige informasjon (Tzanetakis, 2017). For noen kan overvåkningen som foregår i dagens samfunn bety at vi har nådd slutten på personvern (Lyon, 2007). Med fokus på personvern, forteller kontrolløren Ole at det finnes mange lovlige sider på det mørke nettet:

> Vi har jo masse mørke sider som er helt legale. Vi gjør det rett og slett bare for å begrense tilgangen til informasjonen. Jeg tenker jo framover. At i starten av www så var det ikke et problem fordi det var såpass lite data. At tilgangsstyring ikke var behovsstyrt. Men nå når det har blitt så stort, så er vi på en måte mer avhengige av å dele det opp. […] Men fra et personvernmessig hensyn så klarer jeg ikke å se at det er så negativt.

Med dette utsagnet uttrykker informanten at på bakgrunn av internettutviklingen vil man i noen tilfeller ønske å avgrense tilgangen til informasjon, og at det mørke nettet har en positiv funksjon for nettopp dette. Kontrolløren Ole forteller videre at: ”Det er jo litt det samme som kryptovalutabiten, at vi kanskje ikke stoler så mye på bankene. Det er den tanken om at

desentralisert valuta, som ikke nødvendigvis er styrt av verdensbanken, er bra da. […]". Med dette sitatet erkjenner informanten at det er fordelaktig at vi selv kan velge å legge vår tillit til for eksempel verdensbanken, eller om vi heller foretrekker å benytte oss av kryptovaluta. Forholdet mellom personvern og myndighetenes styring uttrykkes også i rapporten "Trusler og utfordringer innen IKT-kriminalitet" (Politidirektoratet, 2017, s. 28):

> Økt fokus på personvern og sikkerhet i samfunnet har bidratt til at det utvikles internettjenester som i økende grad tilrettelegger for anonymitet og kryptert kommunikasjon. Kriminelle har blitt flinkere til å utnytte disse tjenestene. Slik teknologi gjør det vanskeligere for politiet å avdekke kriminalitet på internett, herunder identifisere de kriminelle og hvor i verden de befinner seg.

Ut fra min analyse av dette utdraget tolker jeg at det alltid vil være et spenningsforhold mellom personvern og kriminalitet, og at det økte fokuset på personvern de senere årene har skapt flere utforinger for myndighetene. Personvern kan defineres som retten til å forhindre utlevering av sin personlige informasjon til andre, og det finnes lover for å forhindre at dette skal skje (Taddicken, 2014). The General Data Protection Regulation (GDPR) var en ny personvernlov som tredde i kraft sommeren 2018. GDPR ble opprettet for å ha en felles personvernopplysningslov for Den europeiske union (Regjeringen, 2018). På bakgrunn av dette har det blitt utviklet flere tjenester på internett som tilrettelegger for at man kan opptre anonymt og kommunisere uten å oppgi personlig informasjon. Dette er for å beskytte at personlig informasjon skal komme på avveie og potensielt misbrukes av andre.

Fra analysen kommer dilemmaet som berører anonymitet på internett tydelig frem. Vi ser at kryptering på det mørke nettet kan hjelpe personer i totalitære stater, få varslere til å dele informasjon med media på en trygg måte, og det kan være med på å beskytte personvern. På samme tid kan det mørke nettet legge til rette for illegale aktiviteter og gjøre det mer utfordrende for myndighetene å overvåke dette på internett. Spørsmålet er hvor mye frihet samfunnet er villig til å gi opp for å øke samfunnssikkerheten. Svaret på dette spørsmålet vil variere mellom personer, grupper og institusjoner på bakgrunn av deres egeninteresse (Tzanetakis, 2017). Som følge av dette kan vi si at det mørke nettet er tosidig, og for kriminologer skaper denne tosidigheten en spenning (Powell, Stratton og Cameron, 2018). En slik spenning er også å finne hos de seks informantene som ble intervjuet for denne avhandlingen. Ikke bare har de ulike meninger seg imellom, men flere av informantene

opplever samtidig en intern spenning i sine egne synspunkter. Frem til nå har det blitt presentert eksempler fra kontrollørene på det mørke nettet som ser at krypterte plattformer kan ha positive og legale funksjoner sett fra norske myndighetspersoners ståsted. Det var også noen kontrollører som hadde et mer kritisk blikk rettet mot det det mørke nettet:

> Jeg synes jo generelt at folk får stå fram med hvem de er. Det er misforstått det med internettet. At vi i den fysiske verden skal ha identitet, men digitalt skal det være så identitetsløst. Det passer ikke. Jeg vet jo at det er noen teknologier som kan brukes til for eksempel å stå fram for journalister, eller varslersaker, eller hva det måtte være for å kunne si ifra uten risiko for represalier. Generelt er jeg mest tilhenger av at folk har lov til å mene hva man vil, men da får de stå fram med hvem de er. Det må du i den fysiske verden.

Dette sitatet er fra kontrolløren Tore, og med sitt utsagn anerkjenner han at det mørke nettet kan ha noen positive funksjoner, men utover dette forstår han ikke hvorfor man skal være identitetsløs og anonym på internett når man må stå frem med hvem man er i livet utenfor internett. Anonymiteten som det mørke nettet legger til rette for kan på samme tid utnyttes til å gjøre ulovlige handlinger. Basert på dokumentanalysen jeg har gjort av "EU Drug Markets Report" (EMCDDA, 2019) tolker jeg at fra myndighetene i EU sitt ståsted kan kryptering, brukeranonymitet og forfalskning av lokasjon anes som mistenkelig aktivitet fremfor et verktøy av demokrati. Videre står det i denne rapporten at de krypterte funksjonene på det mørke nettet gjør det vanskeligere for myndighetene å få oversikt og regulere organisert internettkriminalitet.

Kontrolløren Jan er i likhet med kontrolløren Tore skeptisk til det mørke nettets funksjon, og han tror ikke at det er behov for disse krypterte internettplattformene: "Det er jo et sted som vil være veldig gråsone uten noe kontroll og ingen instanser som kontrollerer det som skjer der. Så i den grad det vanlige internettet er det, så er i hvert fall ikke det mørke nettet det. […] Jeg tror ikke vi trenger darknet, jeg tror ikke det". Kontrolløren Jan mener at det mørke nettet kan være et risikofylt sted hvor det ikke er kontrollører som kan gripe inn dersom man blir utsatt for uønskede hendelser. Uttalelsen om at det ikke er noen form for kontroll på det mørke nettet vil utfordres senere i dette analyse- og diskusjonskapittelet, da jeg vil argumentere for at det finnes flere former for overvåkning og styring på kryptomarkeder.

I rapporten ”Trusler og utfordringer innen IKT-kriminalitet” (Politidirektoratet, 2017, s. 15) fremkommer det at: ”Kriminelle på det mørke nettet kan kommunisere tilnærmet anonymt, samt skaffe seg illegale produkter som kan brukes til kriminelle handlinger”. I min analyse av dette utdraget, tolkes det at Politidirektoratet fokuserer på de negative aspektene sett fra myndighetenes ståsted når det kommer til det mørke nettet. De mener at krypteringen legger til rette for anonym kommunikasjon blant kriminelle, og fungerer som en plattform hvor kriminelle kan få tak i illegale produkter som brukes til kriminelle handlinger.

Anonymiteten på krypterte plattformer kan brukes med både lovlige og ulovlige intensjoner. Jeg har presentert informantenes nyanserte meninger om hvorvidt det mørke nettet burde eksistere, og hvorvidt de legale funksjonene på krypterte plattformer veier opp for de illegale funksjonene. Noen av kontrollørene mener i utgangspunktet at det mørke nettet har legale og positive funksjoner sett fra myndighetenes ståsted, mens andre mener at vi ikke har behov for krypterte nettverk fordi vi burde stå frem med hvem vi er slik vi må i livet utenfor internett. Ansatte i toll og politi som jobber med å kontrollere det mørke nettet deler varierende syn om det mørke nettets tosidighet. De har ulike synspunkter sammenlignet med hverandre, men det oppstår også en intern spenning hos hver enkelt informant om hvorvidt de mener det mørke nettet har positive sider ved seg sett fra myndighetenes ståsted, og om krypterte nettverksplattformer burde eksistere på bakgrunn av dette. Vi kan spørre oss selv om hvor mye frihet og personvern samfunnet er villig til å gi opp for å beskytte seg mot kriminalitet, og analysen av kontrollørenes utsagn viser at det de mener er viktigst i dette dilemmaet vil variere ut ifra deres egeninteresse (Tzanetakis, 2017). Analysen viser ingen klar felles holdning blant myndighetene om kryptering og anonymitet på internett, men den fremmer imidlertid deres nyanserte synspunkter.

Myndighetenes kriminalpolitikk som omhandler styring og overvåkning rettet mot narkotikadistribusjon på det mørke nettet, vil være påvirket av krypterte nettverks tosidighet. De er nødt til å veie de to motstridende sidene opp mot hverandre når de skal prioritere sine kontrollressurser. I analysen jeg har gjort av rapporten ”Trusler og utfordringer innen IKT-kriminalitet” (Politidirektoratet, 2017), fremkommer det at Politidirektoratet argumenterer for at myndighetenes styring blir vanskeligere ved det mørke nettets eksistens. De uttrykker også at samfunnets økte fokus på personvern fører til intensivering av kryptert kommunikasjon, noe som enkelte kan utnytte i forbindelse med ulovlige handlinger. Selv om krypterte nettverk har legale og positive funksjoner sett fra de norske og europeiske myndighetenes

ståsted, må de likevel bruke ressurser rettet mot styring av det mørke nettet med fokus på personer som benytter seg av kryptering for illegale hensikter. Det er flere faktorer med det mørke nettet som myndighetene anser som utfordrende, og som ligger bak deres rasjonalisering av ressursbruk.

5.2 "At Bønna røyker hasj er på en måte ikke et samfunnsmessig problem": Digital vold, økt tilgjengelighet og andre samfunnsmessige konsekvenser

Frem til nå har avhandlingen vist at krypterte nettverk innehar flere funksjoner. I den hensikt noen personer velger å bruke det mørke nettet for å utføre illegale handlinger, ser myndighetene seg nødt til å bruke ressurser på at tjenestepersoner skal overvåke dette. Nå skal oppgaven ta for seg myndighetenes syn på kryptomarkeder utover utfordringene som knyttes til anonymitet og kryptering. Dette gjøres for å bedre forståelsen av hvorfor myndighetene prioriterer sine ressurser rettet mot overvåkning og styring for å beskytte samfunnsborgerne. Det er viktig å forstå hva myndighetene tenker om kryptomarkeder, da deres meninger kan ha virkning på kriminalpolitikken og hvordan de skal møte utfordringene knyttet til det mørke nettet. For å gjøre dette vil avhandlingen basere seg på det grunnleggende i et governmentalityperspektiv som er at myndighetene vil styre samfunnet basert på rasjonelle prinsipper eller lover (Neumann, 2003). I senere tid har fokus på risikohåndtering i økende grad påvirket hva som ligger bak de rasjonelle prinsippene og lovene myndighetene har (Garland, 2013). Det betyr at når myndighetene skal fordele sine ressurser, gjennomfører de beregninger basert på samfunnsborgernes risiko.

Kontrolløren Tore ble stilt spørsmålet om hvorfor han tror at myndighetene bruker så mye ressurser rettet mot narkotikakontroll, og han ga følgende svar: "*Det er jo fordi at noen skor seg på andres elendighet".* Informanten mener at myndighetene bruker ressurser på styring i forbindelse med narkotikadistribusjonen på det mørke nettet fordi det består av plattformer som legger til rette for at noen kan tjene på personers narkotikabruk, som kontrolløren Tore her referer til som elendighet. Myndighetene anser det som sin oppgave å styre og overvåke på det mørke nettet fordi noen personer tjener penger på andres problemer, i dette tilfellet selgere som utnytter seg av narkotikabrukere. Med dette kan vi forstå det slik at det er myndighetenes rasjonelle prinsipp å bruke ressurser i forbindelse med styring relatert til

narkotikadistribusjonen på det mørke nettet. Dette underkapittelet vil trekke frem tre eksempler som myndighetene mener er utfordrende med kryptomarkeder, og som kan være noen av årsakene til at de bruker ressurser på styring og overvåkning relatert til narkotikadistribusjonen på det mørke nettet: Digital vold, økt tilgjengelighet av farlige narkotiske stoffer og andre samfunnsmessige konsekvenser. Jeg vil videre argumentere for at myndighetenes synspunkter om de disse faktorene påvirker deres overvåkning og styring på det mørke nettet.

5.2.1 Fysisk og digital vold på det mørke nettet

Det er flere grunner myndigheten trekker frem som viktige årsaker til å prioritere ressurser i forbindelse med styring rettet mot narkotikadistribusjon på det mørke nettet. En av årsakene som kontrollørene snakker om, og som det fremkommer i offentlige myndighetsrapporter, er forholdet mellom narkotikadistribusjon og vold. Flere forskere mener at risikoen for å bli utsatt for fysisk vold i forbindelse med handel på kryptomarkeder er lavere sammenlignet med det tradisjonelle narkotikamarkedet (Barratt, Ferris og Winstock, 2016: Martin, 2018). Administratorene på kryptomarkedene markedsfører sine markedsplasser med at de kan tilby et tryggere miljø å handle narkotika på da man unngår møter ansikt til ansikt med selgere som potensielt kan ende i vold (EMCDDA, 2017). Under intervjuene ble informantene konfrontert med forskningsfunnene som konkluderer med at narkotikadistribusjonen på det mørke nettet fører til lavere risiko for å bli utsatt for fysisk vold sammenlignet med det tradisjonelle narkotikamarkedet. Kontrolløren Jan reflekterte over disse forskningsfunnene:

> […] Du sitter trygt bak din egen datamaskin i din egen stue og bestiller dette her og får det levert i din egen postkasse. Sånn sett så utsetter du deg ikke for en fare i den forstand i det at man ferdes i skumle miljøer eller noe sånt. Så du klarte jaggu meg å se en positiv side med det og.

I utgangspunktet hadde kontrolløren Jan et skeptisk syn på kryptomarkeder, men han var enig i forskningsfunnene som tilsa at narkotikadistribusjonen på det mørke nettet kan være en plattform med lavere risiko for å bli utsatt for fysisk vold sammenlignet med andre narkotikamarkeder. Kontrolløren Kjetil var også enig i at det mørke nettet kan føre til en lavere risiko for narkotikabrukene å oppleve fysisk vold, men han var likevel kritisk til

tanken om at narkotikadistribusjon på det mørke nettet fører til mindre vold på et generelt nivå:

> Det mørke nettet er ikke lik den fysiske verden, så det er helt sikkert riktig at det er mindre vold der, men det gjelder kun i det siste leddet i narkotikakjeden. Voldspotensialet i leddene før, på de store kvantaene, er sikkert det samme. På en måte er volden stort sett ikke rettet mot den ene brukeren, men det er gjerne på leddet før med kriting, gjeld og den type ting. Risikoen for vold kan jo være den samme der, for selgerne må jo skaffe stoffet fra et eller annet sted. Så enten legger dem ut alt cashet, eller så låner dem, og det er gjerne der volden oppstår. Men brukeren slipper hvert fall å oppsøke lugubre steder på gata, bli svindla og rana.

Med dette sitatet hevder informanten at i narkotikakjeden oppstår vold som regel i leddene før det kommer til personen som skal kjøpe sin brukerdose av narkotika. Han mener at det kanskje er mindre fysisk vold rettet mot kjøper i det siste leddet i narkotikakjeden på det mørke nettet, men det er vanskelig å dokumentere hvorvidt det foregår mindre vold i leddene før, som for eksempel under produksjon av narkotika og ved narkotikasmugling. Foreløpig foreligger det lite informasjon om hvordan selgere på det mørke nettet får tak i sin narkotika og generelt koblingen til det tradisjonelle narkotikamarkedet (EMCDDA, 2017). På tross av lite dokumentert informasjon om denne forbindelsen, trekker også kontrolløren Ole frem at narkotikadistribusjon på det mørke nettet kan føre til mindre fysisk vold mot brukeren i siste leddet i narkotikakjeden, men at det ikke betyr fravær av vold totalt sett:

> Jeg tenker jo at det er kjempebra, men da er det snakk om vold mot bruker, altså helt i siste ledd. Det er mange ledd i prosessen, og her har vi kanskje bare fått et annet ledd i midten. Men mindre vold mot bruker er jo alltid bra. Da blir det mindre annen kriminalitet som følger av narkotikakriminalitet. Jeg tenker absolutt at det er bra for bruker, men det betyr nok ikke at det er fravær av vold knytta til distribusjonen.

I likhet med kontrollørene Kjetil og Ole fremkommer det i min analyse av ”EU Drug Markets Report” (EMCDDA, 2019) at myndighetene fra EU også mener at knytningen mellom narkotikabruk og fysisk vold på et generelt nivå vil være lik, uavhengig om narkotikaen kommer fra det mørke nettet eller det tradisjonelle narkotikamarkedet. Selv om det mørke nettet kan bidra til mindre fysisk vold mot narkotikakjøperen i siste leddet av narkotikakjeden, kan det være andre risikoer knyttet til narkotikahandel på kryptomarkedene.

Det er ikke bare i forbindelse med for eksempel produksjon og smugling vold kan oppstå. Det står videre i EMCDDA (2019) rapporten at myndighetene fra EU mener det er både en direkte og indirekte sammenheng mellom bruk av narkotika og vold. Bruk av narkotika og voldelig kriminalitet kan oftere forekomme på bakgrunn av at de involverte er ruset på narkotika, noe som vil anses å være en direkte effekt. Den indirekte effekten av narkotika og vold kan være tilfeller hvor narkotikabrukere må utføre kriminelle og voldelig kriminalitet for å finansiere narkotikabruket sitt. Bruk av narkotika vil ha både denne direkte og indirekte effekten uavhengig om stoffene er kjøpt på det mørke nettet eller på gaten.

I en spørreundersøkelse utført av Barratt, Ferris og Winstock (2016) ble det rapportert at kunder på kryptomarkedet har opplevd færre hendelser med vold og trusler om vold på kryptomarkedet sammenlignet med alternative kilder for narkotika, som for eksempel gjennom venner eller kjente narkotikaselgere på gaten. At enkelte forskere mener at narkotikadistribusjonen på det mørke nettet fører til lavere risiko for å bli utsatt for fysisk vold, vil samtidig bety at de mener det tradisjonelle narkotikamarkedet har høyere risiko for å bli utsatt for fysisk vold. Det vil ikke nødvendigvis alltid være en større risiko for å bli utsatt for fysisk vold ved handel på det tradisjonelle narkotikamarkedet. I rapporten ”Drugs and the darknet: Perspectives for enforcement, research and policy” (EMCDDA, 2017, s. 25) står det at:

> However, the extent to which this occurs is likely to vary considerably according the organisation of drug markets in different locations. Overall, not all drug markets are characterised by the risk of violence (Coomber, 2015). Moreover, many drug users obtain their drugs through peer or friendship networks, so the extent to which obtaining drugs places users at risk of violence or other problems is likely to be highly variable.

I dette utdraget kan det tolkes at myndighetene fra EU mener risikoen for fysisk vold kan variere uavhengig om det er på internett eller på gaten. De mener videre at narkotikadistribusjon på det tradisjonelle markedet ikke alltid kan karakteriseres med høy risiko for vold fordi mange narkotikabrukere får tak i narkotika gjennom venner og andre lignende kontakter. Kontrolløren Peder illustrerer denne sammenligning mellom risiko for vold mot narkotikabrukere som handler på det mørke nettet og på gaten:

> Du kan være uheldig på Vaterlandsparken i Oslo og bli banka opp eller rana. Men du kan også ha en god leverandør som du kan gå til å få ting trygt i Oslo. Samme gjelder jo på det mørke nettet. At stort sett hvis du oppfører seg fint på en måte, og har en god dialog, så går det greit med de fleste.

Informanten mener at vold kan variere både på internett og på gaten, og at det som regel er lav risiko for et voldelig utfall så lenge man har en god dialog. Fellesnevneren for narkotikahandel på det mørke nettet og på det tradisjonelle narkotikamarkedet, er at man kan være både heldig og uheldig når det kommer til risiko. At markedsplassene markedsfører seg med at de kan tilby en lavere risiko for å bli utsatt for fysisk vold, kan gi en økt følelse av trygghet. I rapporten "Trusler og utfordringer innen IKT-kriminalitet" (Politidirektoratet, 2017, s. 26) står det: "Dette gir også kriminelle økt følelse av trygghet (les: lavere risikoopplevelse), og sannsynligvis er det lettere å distansere seg fra negative konsekvenser når handlingene foregår i det digitale rom der ofrene er langt unna". Politidirektoratet hevder at kryptomarkeder kan anses som attraktive plattformer for narkotikasalg fordi det digitale skaper en avstand til selgeres tanker knyttet til de potensielle negative konsekvensene. Kontrolløren Peder forteller at det mørke nettet kan virke tryggere på grunn av fraværet av personlig og fysisk interaksjon mellom kjøper og selger, men han legger til at man som kjøper må utlevere informasjon om hvem man er og hvor man bor:

> […] Det kan godt være at du har gode erfaringer med noen selgere som selger bra produkter til en lav pris og leverer pakken din akkurat som den skal. Men neste selger kan plutselig være en som er identitetstyv og som kan utnytte deg, svindle deg, true og presse. Det finnes mye dritt på det mørke nettet. Hvis man sammenligner om ungdommen skulle kjøpe narkotika på gata istedenfor på det mørke nettet, kan det kanskje anses som å være tryggere å kjøpe på det mørke nettet ved at du har et større utvalg. Du har ingen interaksjon, verken personlig eller fysisk med selger, og du får ting hjem i en postkasse. Samtidig så må du jo levere ut informasjon om hvem du er og hvor du bor. Det kan jo være utrygt. […]

Utviklingen av teknologi og digitalisering har skapt nye former for vold. Selv om fraværet av fysisk kontakt med narkotikaselgere på det mørke nettet reduserer risikoen for fysisk vold mot narkotikabrukeren, beretter kontrolløren Peder at det vil være andre risikoer knyttet til kryptomarkeder, som for eksempel å bli svindlet. Kontrolløren Tore illustrerte dette på

følgende måte i intervjuet: ”Straffen er mer digital i den digitale verden”. Istedenfor fysisk vold foregår det trusler om digital vold, og i noen tilfeller også gjennomføring av digital vold, på det mørke nettet (Barratt og Aldridge, 2016). Dette innebærer for eksempel svindel, publisering av personlig informasjon om hverandre og nettmobbing (Martin, 2018). Å definere dette som vold, gjøres på bakgrunn av at det innebærer et forsøk på ødeleggelse av noens digitale liv (Bancroft, 2019). Noen forskere mener at svindel er en forventet risiko ved bruk av det mørke nettet (Masson og Bancroft, 2018). Kontrolløren Arne forteller at han i noen tilfeller har sett eksempler på dette: ”[…] Det har vært noen svindelforsøk ved at kjøpere har fått stjålet pengene sine, og ikke få det de har bestilt”. Fra min analyse av ”Drugs and the darknet: Perspectives for enforcement research and policy” (EMCDDA, 2017), kan det tolkes at myndighetene fra EU mener tilbøyeligheten til å svindle kan være større på det mørke nettet nettopp fordi man ikke har en fysisk kontakt til den man svindler.

Man utsetter seg for en viss risiko for å bli utsatt for svindel i forbindelse med en narkotikahandel uavhengig om det er på internett eller på gaten. Det foreligger likevel noen andre former for digital vold på det mørke nettet som man ikke vil utsette seg for på det tradisjonelle narkotikamarkedet (Martin, 2018). Selv om en selgers lokasjon er anonym gjennom krypterte pengetransaksjoner, vil en leveringsadresse være påkrevd for kjøperen for å kunne motta narkotikaen. Dette kan føre til en risiko for ”doxing”, som betyr å publisere identifiserbar informasjon om et individ (Mörch, m.fl., 2018). Dette kan videre brukes til utpressing om å publisere slik personlig informasjon som kan gjøre at de potensielt kan identifiseres av myndighetene (EMCDDA, 2017). Kontrolløren Peder beretter at det kan være noen aspekter ved det mørke nettet man ikke vil se i det tradisjonelle narkotikamarkedet:

> Men det kan kanskje være at andre negative effekter er større, sånn som ID-tyveri og denne typen trusler. Ting som du ikke kan oppleve ved å gå i en park i Oslo og kjøpe anonymt av en fyr du ikke vet navnet på. Du vil jo måtte utlevere hvem du er når du kjøper noe på nettet. Eller du kan selvfølgelig ha en falsk profil og en falsk postkasse, og du kan unngå det. Men det er nok mindre vold, og vi får bare se det positive i det. Færre blir banka opp.

I dette utsagnet forteller informanten at det finnes metoder som kjøperen kan bruke for å redusere risikoen for å bli utsatt for doxing og ID-tyveri. Generelt når man skal kjøpe og selge narkotika, uavhengig av hvilken plattform man velger å benytte, vil det være diverse

risikoer man kan utsette seg for. Det finnes likevel tiltak man kan iverksette for å redusere de ulike risikoene for å bli utsatt for digital vold. På tross av de negative effektene ved det mørke nettet, hevder kontrolløren Peder, fra et myndighetsståsted, at det likevel er noe positivt i at det er mindre direkte fysisk vold for narkotikakjøperen ved å handle narkotika på det mørke nettet.

Frem til nå har jeg presentert digital vold som noe som ikke er fysisk, men i det følgende vil jeg argumentere for at digital vold også kan anses som fysisk vold. På internett foreligger det store mengder med digital data om oss, og disse kan misbrukes av andre til å utføre digital vold. Haggerty og Ericson (2000) henviser til vår personlige digitale data som datadoubles, og de mener at disse i mindre grad er knyttet til den fysiske kroppen vår. Jeg vil senere i underkapittel 5.3.3 forklare hvordan kontrollørene bruker datadoubles til å finne personers identitet, og med det knytter de datadoubles tilbake til personers fysiske kropp. Med dette som utgangspunkt hevder jeg at digital vold også er å anse som noe fysisk. Når noen på det mørke nettet bruker en persons datadoubles til å utføre digital vold, vil personen som datadoubles stammer fra føle dette direkte i sin fysiske kropp. For eksempel vil en person som utsettes for svindel, doxing eller ID-tyveri basert på sine datadoubles på det mørke nettet, føle dette fysisk på kroppen sin. For selv om volden på det mørke nettet er mer digital, betyr ikke det at den ikke er fysisk.

Alle kontrollørene er enig i det faktum at narkotikadistribusjonen på kryptomarkeder kan tilby en lavere risiko for å bli utsatt for direkte fysisk vold for narkotikabrukeren sammenlignet med det tradisjonelle narkotikamarkedet. Informantene mener at dette er utelukkende positivt sett fra myndighetenes side, spesielt fordi mindre direkte fysisk vold mot narkotikabrukere betyr mindre annen kriminalitet som følge av narkotikakriminalitet. Samtidig var det flere av informantene som trakk frem at det på et generelt grunnlag ikke betyr at det mørke nettet fører til mindre vold, fordi den vil være lik på de andre nivåene i narkotikakjeden, som for eksempel ved smugling og produksjon av narkotika. De hevdet videre at selv om forskning har vist at det er mindre vold knyttet til det mørke nettet, så gjenspeiler det kanskje ikke det totale bildet av sammenhengen mellom vold og narkotikadistribusjon på kryptomarkeder. Generelt er det forbundet mange risikoer med narkotikadistribusjon uavhengig av hvor handelen foregår.

Den teknologiske og digitale utvikling har ført til nye former for vold. På det mørke nettet kan risikoen for å bli utsatt for direkte fysisk vold muligens være lavere, men man kan være uheldig og risikere å bli utsatt for digital vold som innebærer blant annet svindel, ID-tyveri og doxing (Martin, 2018). Dette er former for trusler som man ikke vil risikere å bli utsatt for ved å handle narkotika ved det tradisjonelle narkotikamarkedet. Jeg har i dette underkapittelet forklart at digital vold også kan anses for å være fysisk vold, fordi det vil føles fysisk i en persons kropp. Et offer for digital vold vil kunne føle dette fysisk i kroppen sin. Det mørke nettet er ikke bare fredfullt, og man utsetter seg for flere risikoer ved å ferdes der. Disse risikoene er å anse som noen av årsakene til at myndighetene mener at de har et ansvar om å rette sin styring mot kryptomarkedene. Videre skal myndighetenes synspunkter om kryptomarkedenes egenskaper relatert til tilgjengeligheten av farlige narkotiske stoffer presenteres.

5.2.2 Økt tilgjengelighet av farlige narkotiske stoffer

Ved siden av digital vold, er det også andre aspekter ved det mørke nettet som ligger bak årsakene til myndighetenes overvåkning og styring på kryptomarkeder. Blant annet legger det mørke nettet til rette for en økt tilgjengelighet av farlige narkotiske stoffer (Martin, 2018). Myndighetene hevder at tilgjengeligheten av atskillige narkotiske stoffer på det mørke nettet gjør denne arenaen for narkotikadistribusjon ekstra farlig. I rapporten ”Trusler og utfordringer innen IKT-kriminalitet” (Politidirektoratet, 2017, s. 16) står det at det mørke nettet: ”gjør det også mer sannsynlig at nye internasjonale trender og nye stofftyper når norske brukere raskere”. Basert på min analyse av dette utdraget, anfører Politidirektoratet at kryptomarkeder legger til rette for at nye og farlige stofftyper spres til Norge raskere enn det ellers ville gjort. For eksempel kan relativt store kvantum av enkelte typer stoffer selges på det mørke nettet. Dette er svært potente stoffer som man ser sjeldent på de tradisjonelle narkotikamarkedene. Kontrolløren Ole forteller hva han mener om økt tilgjengelighet av farlige narkotiske stoffer på det mørke nettet:

> Også er jo tilgjengeligheten høyere, da alle har tilgang til internett. Noe som gjør at det som kanskje kunne vært et lite problem blir et større problem. […] Narkotika vi vanligvis ser veldig sjelden, selges formentlig helt åpenlyst. Det ser ut som at svært potente stoffer selges i kvantum som er store. […]

Med dette utsagnet sikter informanten til at narkotikadistribusjonen på det mørke nettet kan forsterke en persons allerede eksisterende problemer, blant annet fordi potente stoffer selges i store kvantum på kryptomarkedene. Myndighetene er svært bekymret over dette på grunn av dødeligheten ved disse farlige og potente stoffene. Et eksempel på dette er fra mars 2017, da en 15 år gammel gutt ble funnet død på gutterommet sitt i Oslo. Trolig døde han av karfentaniloverdose, og politiet mistenkte at stoffet var kjøpt på det mørke nettet. Karfentanil er et ekstremt potent stoff og regnes som 10.000 ganger sterkere enn morfin (Letvik, 2017). Slike narkotiske stoffer kan være utfordrende å få tak i på det tradisjonelle narkotikamarkedet, men de kan være lett å få tak i på kryptomarkedene. Kontrolløren Tore omtaler den økte tilgjengeligheten av farlige stoffer på det mørke nettet som skremmende:

> Det er så supertilgjengelig bare ved noen tastetrykk. Tidligere var det kanskje litt mer knotete og du måtte inn og snakke med et kriminelt miljø. Mens nå er det jo alt for enkelt å få tak i sånne typer rusmidler, som er gjerne hjemmemekka, eller mekka av noen som ikke nødvendigvis har laboratorisk kompetanse. Det er skremmende lettvint å få tak i.

Ifølge informanten er det veldig enkelt å få tak i rusmidler som ofte er laget av personer som ikke nødvendigvis har laboratorisk kunnskap. Disse farlige stoffene selges på tvers av landegrensene og Politidirektoratet hevder at internasjonale trender får større aktualitet i Norge gjennom distribusjon på det mørke nettet. Det står videre skrevet i rapporten ”Trender i kriminalitet 2018-2021: Digitale og glokale utfordringer” (Oslo Politidistrikt, 2018, s. 87) at: ”Internetthandelen og markedsføringen der, medfører at nye, syntetiske rusmidler kan spres raskt”. I dette utsagnet antydes det at Oslo politidistrikt mener markedsføringen på det mørke nettet kan være årsaken til at de internasjonale trendene spres raskere til Norge. Myndighetene anser dette som bekymringsfullt fordi det fører til at syntetiske og farlige stoffer kan spres mer effektivt enn det ellers ville gjort på det tradisjonelle narkotikamarkedet. Kontrolløren Tore er mest bekymret over at det mørke nettet gjør tilgangen til narkotika lettere for førstegangskjøpere:

> Det som uroer meg mest er egentlig førstegangskjøpere og nybegynnerne sin lette tilgang til narkotika. Du må ha kontakt med et miljø hvis du skal handle narkotika i den fysiske verden, men på nettet så kan min sønn bare sende inn en bestilling. Det er

> skremmende synes jeg. […] Det blir så stor forskjell i tilgjengeligheten da. Det tenker jeg er største problemet med det.

I dette utsagnet sier informanten at det største problemet med kryptomarkeder er den enkle tilgangen på narkotika. Tilgjengelighetene av de farlige narkotiske stoffene på kryptomarkeder, og kjøpernes tilbøyelighet til å handle disse rusmidlene, kan kobles til markedsmodellen som det mørke nettet er basert på. Et stort skille mellom narkotikadistribusjonen på det mørke nettet og narkotikahandel på det tradisjonelle narkotikamarkedet, er hvordan markedsføringen foregår. Markedsplassene på det mørke nettet ligner andre nettsider hvor man handler lovlige varer på internett (Martin, 2018). Markedsføringen og tilbakemeldingsfunksjonen på kryptomarkeder benyttes aktivt med formål om å øke salgene av narkotiske stoffer. Kontrolløren Kjetil henviser til en spesifikk selger på det mørke nettet som selv prøvde å blande ulike narkotiske stoffer, og delte sine erfaringer med dette:

> […] Det var en som var veldig opptatt av å prøve andre stoffer og kombinere med dopet for få forskjellig virkninger. Han dreiv og lagde sånne cocktailer, og ikke nødvendigvis bare med ulovlige stoffer. ”Bare du blander denne med nok koffein, så skjer det”. Han dreiv og lagde cocktailer, og etter hvert begynte han å lage sine egne piller. Han eksperimenterte og blandet dop med alle mulige andre virkestoffer for å gi forskjellige effekter.

Selgeren som informanten henviser til, baserer sin markedsføring på å fortelle om sine erfaringer med mål om å selge ulike narkotiske stoffer. Å dele slike erfaringer for å øke salg kan være urovekkende ifølge myndighetene. Myndighetspersonene er bekymret over at det mørke nettet øker tilgjengeligheten for farlige og potente rusmidler, spesielt fordi kryptomarkedene også kan være mer tilgjengelig for nye brukergrupper. Basert på analyse av rapporten ”Internet Organised Crime Threat Assessment” (Europol, 2017) hevder Europol at det mørke nettet åpner opp for handel med ulovlige stoffer til nye kunder som vanligvis ikke ville hatt tilgang, eller som ellers ville vegret seg for å handle fra kriminelle selgere på tradisjonelle narkotikamarkeder. At man kan opptre anonymt på det mørke nettet, kan også gjøre at det virker mindre skremmende sammenlignet med å kjøpe narkotika gjennom andre kanaler. Denne økte tilgjengeligheten kan øke lysten for spesielt unge mennesker til å prøve narkotika (Vikan, 2014). At markedsplassene på det mørke nettet skal være anonyme

plattformer uten overvåkning kan også friste ungdom til å benytte kryptomarker fremfor andre arenaer for narkotikahandel. Jeg vil i underkapittel 5.3 vise at myndighetene har flere muligheter til å overvåke på det mørke nettet, men på tross av myndighetenes tilstedeværelse på kryptomarkedene er det flere som ikke føler seg truet av myndighetenes overvåkning og styring. Kontrolløren Kjetil er bekymret over denne nye brukergruppen som det mørke nettet legger til rette for:

> Det gjør det kanskje litt lettere for de som ikke har innpass i miljøer, eller der det er lett å få tak i narkotika. Det mørke nettet gjør det veldig tilgjengelig sånn sett, og du slipper å ha noe kontakt med mennesker i utgangspunktet. Det kan jo tenkes at på gata, hvis selgere ser unge mennesker, at de ikke vil selge til dem. Det er sikkert noen som har samvittighet der og. Den samvittigheten er ikke til stede på det mørke nettet i det hele tatt.

Distribusjonen på det mørke nettet kan oppleves som tryggere for kjøperen sammenlignet med å handle på gata, men i realiteten er det ikke nødvendigvis slik. Informanten mener at det er en mulighet for at ved handel ansikt til ansikt, kan selgere kvie seg for å selge til veldig unge personer, mens på det mørke nettet vil den fysiske avstanden skape en distanse hvor selgere ikke vil ha samme type samvittighet. I likhet med kontrolløren Kjetil, er kontrolløren Ole også bekymret over at det mørke nettet legger til rette for økt tilgjengelighet og økt tilbøyelighet for unge personer til å handle narkotika: ”Det er svært bekymringsverdig det der med at flere unge med litt mer teknisk kompetanse velger å prøve narkotika fordi tilgjengeligheten er større. […]”. De som vanligvis ikke ville oppsøkt et miljø for å handle narkotika, vil ifølge kontrolløren Ole muligens handle narkotika fordi de har teknologisk kompetanse til å gjøre det på det mørke nettet. Dette forklares videre i rapporten ”Trusler og utfordringer innen IKT-kriminalitet” (Politidirektoratet, 2017, s. 27):

> Internettfora kan bidra til å normalisere og rettferdiggjøre kriminell atferd. For personer med kriminelle hensikter er de ulike internettforaene en mulighet til å finne et fellesskap med likesinnede. I slike fora, uten deltakere med kritiske motforestillinger, kan medlemmene forsterke hverandres holdninger og meninger. En alle-gjør-det mentalitet kan skape normative grensedragninger slik at hva som er akseptable handlinger avviker fra resten av samfunnet og at flere begår handlinger de ellers ikke ville begått.

I dette utdraget viser Politidirektoratet at de også er bekymret over at internett kan skape nye brukergrupper ved at internettplattformene normaliserer kriminell atferd. Kryptomarkeder kan føre til at veldig potente stoffer blir mer tilgjengelig for kjøpere sammenlignet med tradisjonelle narkotikamarkeder. Når likesinnede samles på en plattform uten forstyrrelser fra folk med kritiske motforestillinger, mener Oslo politistrikt det kan føre til at flere begår handlinger de ellers ikke ville begått. I rapporten "Trender i kriminalitet 2018-2021: Digitale og glokale utfordringer" (Oslo politidistrikt, 2018, s. 89) står det at:

> Kjøp og salg over internett gjør narkotika tilgjengelig for nye brukergrupper. På selgersiden tyder informasjon fra straffesaker på at sosialt integrerte og velfungerende personer med høy sosial kapital, kan tiltrekkes dette markedet. Dette er i kontrast til selgere og distributører på det tradisjonelle, fysiske markedet, som i stor grad består av sosialt ressurssvake personer som er dårlig integrert. Ungdom fristes av status og penger.

Basert på en analyse av dette utdraget, kan en person på det mørke nettet bli påvirket til å tøye sin egen grense, noe som i tillegg til å skape nye brukergrupper også kan føre til at nye selgergrupper etableres. Myndighetene hevder at de som vanligvis selger narkotika på gaten som regel er dårlig integrerte og ressurssvake personer, men på det mørke nettet er dette ofte ressurssterke personer.

Når samfunn skal fordele sine kontrollressurser, utfører myndighetene en vurdering og beregning basert på samfunnsborgernes risiko (Garland, 2013). Det er flere grunner til at myndighetene mener at det er viktig å prioritere noen av sine ressurser til å overvåke narkotikadistribusjonen på det mørke nettet. En viktig faktor, som Politidirektoratet, Oslo politidistrikt og kontrollørene trekker frem, er den økte tilgjengeligheten av farlige og potente stofftyper på kryptomarkedene. De mener at dette gjør denne arenaen for narkotikadistribusjon ekstra bekymringsfull. Myndighetene sikter videre til at det mørke nettet skaper nye brukergrupper ved å gjøre narkotika mer tilgjengelig for personer som ikke ville hatt samme tilgang til narkotika på det tradisjonelle markedet. Politidirektoratet mener også at det mørke nettet har skapt en ny gruppe av narkotikaselgere. De som vanligvis selger narkotika på det tradisjonelle narkotikamarkedet anses ofte som ressurssvake personer, men på det mørke nettet har det vist seg at dette ofte er personer med høy sosial kapital. Myndighetene mener tilgjengeligheten av de farlige narkotiske stoffene på det mørke nettet

er svært bekymringsfullt. Det er imidlertid de samfunnsmessige konsekvensene som følger med narkotikadistribusjonen på kryptomarkeder myndighetene mener er det mest urovekkende, og som anses å være den viktigste faktoren for hvorfor de skal overvåke markedsplassene.

5.2.3 Andre samfunnsmessige konsekvenser som følger av narkotikadistribusjon på kryptomarkeder

Myndighetenes bekymringer om narkotikadistribusjonen på det mørke nettet vil påvirke hvordan de vil rette sin styring og overvåkning av disse plattformene. De vil rasjonalisere sin styring og overvåkning for å guide samfunnsborgernes liv (Lyon, 2007). Myndighetene er bekymret over at det foregår digital vold på det mørke nettet og at kryptomarkeder legger til rette for økt tilgjengelighet av farlige narkotiske stoffer. Det som likevel veier tyngst hos myndighetene, og som er hovedårsaken bak deres rasjonalisering av ressursbruk på styring og overvåkning rettet mot narkotika på det mørke nettet, er de andre samfunnsmessige konsekvensene som følger av narkotikadistribusjonen. Rapporten "EU Drug Markets Report" (EMCDDA, 2019, s. 24) skisserer dette på følgende måte:

> Illicit drug markets have both direct and indirect impacts on society that go far beyond the harms caused by the use of drugs themselves. These include the links that exist with wider criminal activities and terrorism; the negative impact on the legal economy and communities; and the increasingly important issue of how the drug market can fuel corruption and undermine governance.

Myndighetene fra EU hevder at det både er direkte og indirekte konsekvenser som følger av narkotikadistribusjonen utover at det er skadelig for brukerne. De ramser opp ulike effekter, som blant annet innebærer organisert kriminalitet og terrorisme, ulovlig økonomi, samt korrupsjon. Disse synspunktene som myndighetene innehar, vil påvirke deres prioriteringer av ressurser i forbindelse med styring og overvåkning av kryptomarkeder. Kontrolløren Ole mener at myndighetene ikke hadde brukt så mye ressurser på å møte narkotikakriminalitet om det ikke hadde vært for de andre samfunnsmessige konsekvensene som følger av narkotikakriminaliteten:

> Vi er veldig interessert i kriminalitet som følger av narkotikakriminalitet. Det narkotikadistribusjonskjeden fører med seg er jo veldig bekymringsfullt. […] At Bønna røyker hasj er på en måte ikke et samfunnsmessig problem. Det er et problem for Bønna, og Bønna får det ikke noe bedre av det. Men i det store og hele, hvis problemet utelukkende hadde vært at folk brukte narkotika, så tror jeg ikke vi hadde brukt så mye tid som vi gjør på det.

Med dette sitatet mener informanten at hovedårsaken til at myndighetene prioriterer sine ressurser på dette området er de negative konsekvensene som følger av narkotikakriminaliteten. Å se narkotikadistribusjonen på det mørke nettet i et større bilde enn selve narkotikakriminaliteten, er et viktig argument for myndighetene vedrørende hvorfor de skal bruke ressurser på kontroll av kryptomarkeder. Som nevnt i forrige underkapittel, fører det mørke nettet til en økt tilgjengelighet av farlige narkotiske stoffer, noe som myndighetene anså som svært bekymringsfullt. I tillegg til at disse stoffene er farlig å bruke, kan produksjonen av disse føre med seg andre samfunnsmessige konsekvenser utover at det er skadelig for brukeren:

> Drug production, both within the EU and in other countries to produce drugs sold on the EU market, results in health and safety risks and environmental damage. The EU is a significant production area for synthetic drugs and cannabis, resulting in damage to the environment through the dumping of chemical waste and creating risks both to those involved and to the communities where production is located (EMCDDA, 2019, s. 24).

Dette utdraget er fra ”EU Drug Markets Report” (EMCDDA, 2019) og jeg tolker at myndighetene fra EU mener de kjemiske stoffene, og prosessene som benyttes for å lage dem, kan være veldig farlige både for de som produserer det og for samfunnet for øvrig. De hevder videre at avfallet fra denne produksjonen dumpes, noe som kan føre til skade på miljøet og skape en risiko for folkehelsen. Disse miljøkonsekvensene er en annen samfunnsmessig konsekvens som følger av narkotikaproduksjon, og jeg har tidligere forklart at det mørke nettet øker tilgjengeligheten av slike syntetiske stoffer. Dette kan være en av flere årsaker som kan påvirke myndighetenes styring og overvåkning rettet mot narkotikadistribusjonen på kryptomarkeder.

Selv om syntetisk narkotika kan føre til skade på miljø og folkehelsen, er det likevel de samfunnsmessige konsekvensene som er knyttet til organisert kriminalitet som er mest urovekkende for myndighetene, og som kan være en av hovedårsakene til deres rasjonalisering av styring og overvåkning på kryptomarkedene. Mye av narkotikasalget på det mørke nettet gjøres av enkeltindivider, men basert på rapporten "Drugs and the darknet: Perspectives for enforcement, research and policy (EMCDDA, 2017) fremkommer det i min analyse at myndighetene beretter at de er bekymret over at de organiserte gjengene også skal øke bruken av det mørke nettet som distribusjonssted. Dette forklares videre i rapporten "Internet Organised Crime Threat Assessment" (Europol, 2019), hvor Europol belyser hvordan noen kriminelle gjenger forsøker å gjemme seg bak flere forskjellige nettprofiler fordelt på ulike markedsplasser på det mørke nettet. På denne måten vil organiserte gjenger fungere som enkeltindivider fremfor en stor organisert gruppe på kryptomarkedene. I noen tilfeller vil personer som er klar over myndighetenes overvåkning, etterstrebe å motsette seg denne overvåkningen (Lyon, 2007). De organiserte gjengene er klar over myndighetenes tilstedeværelse på det mørke nettet, men de disiplineres til å benytte ulike brukerprofiler for å forsøke å holde seg under radaren for myndighetenes overvåkning, noe som gjør det mer utfordrende for kontrollørene å overvåke de organiserte kriminelle gruppene som opererer på kryptomarkedene. Jeg vil gå nærmere inn på overvåkning, motstand til overvåkning og disiplin i underkapittel 5.3.

I forbindelse med organiserte grupper, står det i rapporten "Drugs and the darknet: Perspectives for enforcement, research and polity" (EMCDDA, 2017) at myndighetene fra EU mener det mørke nettet legger til rette for polykriminelle miljøer. Det kan for eksempel være at noen som selger narkotika på det mørke nettet også er aktive innenfor annen kriminalitet. Eksempelvis kan noen som selger narkotika, også selge andre ulovlige varer på det mørke nettet. De polykriminelle organisasjonene som myndighetene kanskje frykter aller mest er terrororganisasjoner. Dette er en av de viktigste grunnene til at styring og overvåkning rettet mot organisert kriminalitet er satsningsområder i politikken. Myndighetene kan rasjonalisere sin overvåkning med at det er en metode som må benyttes i deres kamp mot terrorisme (Lyon, 2007). Ifølge rapporten "EU Drug Markets report" (EMCDDA, 2019, s. 24) er narkotikamarkeder en av hovedkildene til inntekt for organiserte kriminelle grupper og terrororganisasjoner:

> Globally, involvement in drug production and trafficking, either directly or indirectly,

> is an important source of funds for terrorist activities, although only one of many sources. In Europe, currently there appear to be no strong, systematic links between drug markets and terrorism beyond those arising from shared underlying factors or situations. Links to jihadist terrorism in the EU usually result from individuals' previous involvement in the lower levels of the drug market or in using drugs, which may then continue after their radicalisation.

Myndighetene fra EU forklarer at narkotika er en viktig inntektskilde for terroraktiviteter, selv om de ikke har funnet en sterk systematisk kobling i Europa mellom narkotikamarkeder og terrorisme. I Europa er vanligvis koblingen mellom narkotika og terrorisme et resultat av individer som bruker narkotika eller tidligere har vært involvert i lavere nivåer av narkotikadistribusjon, og i noen tilfeller fortsetter de med dette etter at de blir medlem i terrororganisasjoner. Selv om en av grunnene til at myndighetene trolig prioriterer sine ressurser rettet mot styring og overvåkning narkotikadistribusjon på det mørke nettet på bakgrunn av terrorfinansiering, er det ingen forskning som viser en direkte kobling mellom disse i Europa.

Det er flere aspekter ved kryptomarkeder som myndighetene er bekymret over, og som legger grunnlaget for de rasjonelle prinsippene for styring rettet mot narkotikadistribusjonen på det mørke nettet (Neumann, 2003). Det som likevel betraktes som de aller viktigste årsakene bak myndighetenes styring og overvåkning av kryptomarkeder, er de mer overordnede samfunnsmessige konsekvensene som følger av narkotikadistribusjonen. Det som myndighetene er mest bekymret over, er koblingen mellom narkotikadistribusjon på det mørke nettet og organiserte kriminelle gjenger. Et tiltak som kriminelle organisasjoner utfører på det mørke nettet med mål om å motsette seg myndighetenes overvåkning, er at de fremstår som enkeltindivider. Dette gjør det mer utfordrende for myndighetene å oppdage at det er organiserte organisasjoner som står bak narkotikadistribusjonen.

Organisasjonene som myndighetene frykter mest er terrororganisasjoner. Myndighetene mener at det eksister en sammenheng mellom narkotikakriminalitet og terrorfinansiering, selv om det per i dag ikke foreligger forskning som kan bevise en sterk systematisk link mellom disse i Europa (EMCDDA, 2019). Myndighetene bruker ressurser på styring og overvåkning, og de gjør det med formål om å beskytte samfunnsborgerne fra alt det urovekkende som skjer

på det mørke nettet. Det mørke nettet gjør myndighetenes styring mer utfordrende, men det er ikke helt umulig å overvåke kryptomarkeder.

5.3 ”Det mørke nettet, jeg veit ikke om det faktisk er så veldig mørkt”: Overvåkningsdynamikker på det mørke nettet

Frem til nå har jeg vist hva som kan ligge bak myndighetenes rasjonalisering av deres styring og overvåkning på det mørke nettet. Hvordan deres overvåkning foregår på det mørke nettet, vil presenteres i dette underkapittelet. Det er også andre overvåkningsdynamikker som foregår på kryptomarkedene, og alle disse vil kartlegges i dette underkapittelet. Overvåkningens historie går like langt tilbake i tid som menneskets eksistens, men overvåkning i senmoderne tid har blitt påvirket av digitalisering og teknologisk utvikling (Lyon, Haggerty og Ball, 2012; Salter, 2010). Krypterte nettverk skal fungere som frie plattformer hvor man kan opptre anonymt, men anonymiteten det mørke nettet tilbyr kan likevel være noe begrenset.

I det følgende vil jeg vise at det foregår flere former for overvåkning på kryptomarkeder. Dette innbefatter overvåkning fra myndighetene rettet mot administratorer, kjøpere og selgere for markedsplasser med narkotikahandel. Denne overvåkningen er gjensidig, noe som betyr at administratorer, kjøpere og selgere på markedsplasser med narkotikahandel også overvåker myndighetene. I tillegg til dette overvåker kjøpere og selgere hverandre internt på kryptomarkedene. Det er viktig å se på overvåkningsdynamikkene som foregår på det mørke nettet fordi det vil bidra til økt kunnskap om sammenhengen mellom digitalisering, overvåkning og styring. Jeg vil også vise at det ikke bare er myndighetenes synspunkter om det mørke nettet som kan ha effekt på deres overvåkning og styring, men at overvåkningsdynamikkene på det mørke nettet også kan påvirke myndighetenes fremtidige overvåkning.

5.3.1 Panoptisk overvåkning på kryptomarkeder

Selv om overvåkning er noe som har foregått like lenge som vi mennesker har vært til, vil personer i noen tilfeller forsøke å unngå å bli overvåket. De som er subjekt til myndighetenes overvåkning vil noen ganger etterstrebe å motsette seg denne overvåkingen (Lyon, 2007). En

metode for å motsette seg myndighetenes overvåkning, og å kunne fremstå anonym, er å bruke det mørke nettet. Likevel er ikke det mørke nettet helt anonymt, og det står følgende i rapporten "Drugs and the darknet: Perspectives for enforcement research and policy" (EMCDDA, 2017, s. 60-61):

> Law enforcement authorities in the EU actively monitor online marketplaces to identify trends, such as the most popular darknet markets, the substances traded, the most prolific vendors active on specific darknet markets, price developments, the flow of virtual currencies and other innovations in this area. The regular monitoring of darknet markets yields intelligence on top vendors, prices, available substances and other trends.

Selv om det mørke nettet skal være en trygg plattform for å kommunisere anonymt, viser min analyse at myndighetene fra EU hevder de overvåker det mørke nettet for å blant annet identifisere narkotikatrender og de mest produktive narkotikaselgerne. Ofte har overvåkningsprosesser blitt forklart med Foucaults panoptikon, som er basert på Benthams fengselsarkitektur (Foucault, 1979). Til en viss grad kan denne panoptikonstrukturen illustrere noen av overvåkningsprosessene på det mørke nettet. I Foucaults panoptikonmodell kan fangevokterne se fangene i fengslene, men fangene er uvitende om de blir overvåket eller ikke. Resultatet er det Foucault (1979) anser som en perfekt maktoperasjon hvor få ser mange. Som det fremkommer i utdraget fra rapporten publisert av EMCDDA (2017), blir markedsplassene på det mørke nettet overvåket av myndighetene. Kontrolløren Kjetil trekker frem et eksempel på en kjøper på det mørke nettet som er klar over myndighetenes overvåkning, uten å vite når han eller hun blir overvåket:

> Selv om de beskriver det som risikofritt, så er det fortsatt litt noia der. Også er de jo rusmisbrukere og derfor er de kanskje litt ekstra "sånn". Du ser med en gang om en pakke er en uke eller to forsinka. "Å rydde hjemme" er et begrep da. "Å, må jeg rydde hjemme" liksom. Også skjønner de jo ikke metodebruken heller. De tror at de er litt viktigere enn dem er. "Ja, nå overvåker dem posten min, nå er jeg avlytta" med en gang det er litt forsinkelser liksom. […]

Med dette utsagnet som eksempel, kan overvåkningen på det mørke nettet til en viss grad sammenlignes med Foucaults (1979) panoptikonmodell. Myndighetenes overvåkning på

kryptomarkedene kan ligne på overvåkningen som foregår i fengslene ved at kjøpere og selgere er klar over at myndighetenes tilstedeværelse, men de er aldri sikre på når de blir utsatt for kontrollørenes overvåkning. I noen tilfeller skaper dette en paranoia og selvdisiplin hos kjøpere på kryptomarkeder hvor de tror at de blir overvåket mer enn hva de kanskje egentlig blir. Selvdisiplinen innebærer at de spør om råd og lurer på om de må forberede seg på at de har blitt avslørt av myndighetene. De disiplineres også til å tilpasse seg myndighetenes overvåkning og foretar seg ekstra tiltak for å ikke bli avslørt. I rapporten "Internet Organised Crime Threat Assessment" (Europol, 2020, s. 57) står det følgende:

> Furthermore, Darkweb administrators have been observed pulling together and showing a collaborative spirit to maintain the environment under challenging circumstances. When faced with similar challenges, forum and service administrators have been seen working more closely together over sharing code and security methodologies.

I min analyse av denne rapporten fremkommer det at Europol har observert at administratorene på det mørke nettet har begynt å samarbeide med hverandre for å møte utfordringer sammen og ivareta miljøet på det mørke nettet. Utfordringene de står overfor refereres blant annet til myndighetenes overvåkning. Tilpasningene på bakgrunn av myndighetenes overvåkning viser hvordan subjekter til overvåkning vil samhandle med overvåkningssystemene (Martin, van Brakel og Bernhard, 2009). Dette kan forklares nærmere med governmentalityteori ved at myndighetenes styring disiplinerer aktørene på det mørke nettet (Foucault, 1991). Myndighetene disiplinerer administratorer, kjøpere og selgere av narkotika på det mørke nettet til å øke sin kompetanse på kryptering for å unngå myndighetenes overvåkning. Ut fra dette ser vi at myndighetene overvåker kryptomarkeder, men at kjøpere og selgere på kryptomarkedene også overvåker myndighetene. Mange overvåkningsprosesser krever involvering av de som overvåkes (Lyon, 2007). Samtidig kan teknologien i dag ses som en mekanisme som kan hjelpe til å formilde asymmetrien mellom myndighetene og de som overvåkes (Mann og Ferenbok, 2013). På bakgrunn av dette kan det argumenteres for at Foucaults panoptikonmodell er for snever til å forklare overvåkningen som foregår på det mørke nettet. Derfor skal jeg se nærmere på andre modeller som kan illustrere overvåkningsdynamikkene på kryptomarkedene bedre.

Panoptikonmodellen baseres på at få overvåker mange. Imidlertid presenterte Mathiesen (1997) modellen synoptikon som innebærer at mange kan overvåke få, for å blant annet forklare hvordan massemedienes inntog har påvirket samfunnets overvåkning. Han mente at overvåkning i det moderne samfunnet kan forklares ved å kombinere panoptikon med synoptikon. Myndighetenes overvåkning på det mørke nettet vil disiplinere kjøpere og selgere til å overvåke myndighetene tilbake. Synoptikon og panoptikon vil samlet illustrere at mange ser få, og få ser mange. Et annet overvåkningsperspektiv, som kan være med på å demonstrere hvordan overvåkning kan foregå nedenfra og opp, er sousveillance (Mann og Ferenbok, 2013). Den baseres på at det er flere "våkninger" samtidig, hvor det er mange involverte i overvåkningsprosessene. Selv om sousveillance betyr overvåkning nedenfra og opp, innebærer modellen at det også er andre måter å overvåke på. Vi lever i en tid hvor mennesker kan og vil se tilbake på myndighetene, noe som potensielt kan drive sosial og politisk ending. Basert på informasjon kjøpere og selgere på kryptomarkeder får fra å overvåke myndighetene, tilpasser de sin tilstedeværelse på det mørke nettet med å bedre krypteringen. Dette fører videre til at myndighetene også må bedre sin teknologiske kompetanse. Kontrolløren Peder forklarer hvordan kommunikasjon på det mørke nettet har blitt mer kryptert:

> Utfordringa er jo at det mørke nettet også er i en utvikling. Hvis vi ser tilbake på materiale fra Silk Road fra 2013 så kommuniserer folk åpent og man sender adressen sin ukryptert, mens i dag så er det få som gjør det. Folk har blitt sikrere og folk har begynt å bruke VPN før TOR for å sikre IP-adressen sin der. Det er også mer bruk av kryptert mail. Det er sånn at alle har vært nye en gang. Så selv om du er ekspert i 2020 så var du ikke ekspert da du begynte kanskje i 2014, og på nettet så ligger jo spora lagra. Så det er nok at du gjorde feil i 2014 så kan det være akkurat den lille biten politiet eller toll trenger for å identifisere deg. Sånn sett så er det spor å finne selv om folk er veldig flinke i dag.

Informanten mener at det har oppstått et skifte i hvor mange tiltak kjøpere og selgere på kryptomarkeder foretar seg i dag sammenlignet med oppstartsfasen av krypterte markedsplasser. Tidligere kommuniserte folk mer åpent på det mørke nettet, mens i dag er det flere som benytter seg av VPN før de bruker programvaren TOR, og myndighetene ser en økning i bruk av krypterte e-postadresser. VPN står for virtuelt privat nettverk, og er en datakobling som finner et sted mellom dataenheten og VPN serveren man kobler seg opp til.

All datatrafikken vil gå gjennom en ekstern server, og IP-adressen, identifikasjon av dataenhetens lokasjon, vil være en annen enn det egentlig er. Dette gjør det vanskeligere for myndighetene å spore brukeres lokasjon (VPN, 2020; Ulseth, Bothner-By og Nordal, 2019). Når myndighetene viser at de kan overvåke på det mørke nettet, vil brukerne svare med å utføre enda flere krypteringstiltak. De ekstra tiltakene vil ikke nødvendigvis hjelpe dersom personene har lagt igjen digitale spor på internett tidligere i livet, slik som kontrolløren Peder forteller.

Det er ikke bare TOR og andre lignende programvarer som skal forsøke å sikre anonymiteten til kjøpere og selgere på kryptomarkeder. Kryptert valuta, som for eksempel bitcoin, legger også til rette for anonym narkotikahandel på det mørke nettet (Tzanetakis, 2018). På den måten kan kjøpere betale for narkotikaen uten at overførselen identifiseres og overvåkes av myndighetene. Det fremkommer i min analyse av rapporten ”Drugs and the darknet: Perspectives for enforcement, research and policy” (EMCDDA, 2017, s. 56) at myndighetene har diverse analytiske metoder for å kunne identifisere brukere av det mørke nettet gjennom disse krypterte valutatransaksjonene:

> In February 2017, the Danish National Police Cyber Crime Center (NC3) announced a breakthrough in using new methods to track and identify darknet users. This new technique, which relies on bitcoin transaction analysis, has already been used in practice to identify individuals and help prosecute darknet traders.

Dette utdraget viser at myndighetene bruker teknikker basert på bitcoin transaksjonsanalyser for å identifisere selgere og kjøpere på kryptomarkeder. Dette kan tolkes som om at myndighetene også disiplineres til å forbedre sin kompetanse på kryptering. Når administratorer, selgere og kjøpere på kryptomarkeder overvåkes på det mørke nettet vil de utføre tiltak for å beskytte seg mer og skjule seg bedre. Deres gjensidige overvåkning av kontrollørene vil disiplinere myndighetene til å øke sin teknologiske kompetanse:

> […] Vi må finne den riktige arbeidsmetodikken for å kunne angripe problemstillingene. De vet å beskytte seg der ute, og ofte har folk som er på de stedene her veldig høy teknologisk kompetanse og vet og skjule seg godt. Da må vi utvikle en arbeidsmetodikk som kan nå frem der allikevel da.

Dette sitatet er fra kontrolløren Jan, og med dette mener han at myndighetene må tilpasse seg den teknologiske kompetansen administratorer, kjøpere og selgere har på det mørke nettet. Myndighetene overvåker på kryptomarkeder, og det kan anses for å være en form for indirekte styring i governmentalityteorien (Foucault, 1991). Deres overvåkning fører til at de disiplinerer kjøpere og selgere av narkotika på kryptomarkeder til selvdisiplin, som i denne settingen vil være å utføre ekstra tiltak for å forsøke å motsette seg myndighetenes styring (Garland, 1999). Disse ekstra tiltakene er basert på at de overvåker myndighetene tilbake, og myndighetenes svar på deres overvåkning er å selv også disiplineres til å forbedre sin kompetanse og kunnskap. Her oppstår det en overvåkningsdynamikk som ikke bare baserer seg på overvåkning ovenfra myndighetene og ned på kjøpere og selgere av narkotika på det mørke nettet. Overvåkningsdynamikken innebærer også en overvåkning nedenfra kjøpere og selgere på det mørke nettet og opp mot myndighetene. Dette fører til at myndighetene også disiplinerer seg selv til å endre sine styringstiltak på kryptomarkedene.

Myndighetene kan innhente informasjon fra det mørke nettet, og de kan ved hjelp av ulike teknikker også identifisere kjøpere og selgere på kryptomarkeder. Kryptomarkeder baserer seg på å tilby anonymitet og frie plattformer sammenlignet med det tradisjonelle narkotikamarkedet. På den andre siden vil det mørke nettet gi myndighetene en tilgang til å overvåke narkotikadistribusjon. Kjøpere og selgere på kryptomarkeder blir overvåket av myndighetene, men vet ikke når dette skjer. Denne uvitenheten om når de overvåkes og ikke, kan skape en nervøsitet og paranoia hos kjøpere og selgere på det mørke nettet. Denne overvåkningsdynamikken kan forklares med panoptisk tilnærming, da kjøpere og selgere disiplineres til å samarbeide om å bedre sin kompetanse på kryptering for å motstå myndighetenes overvåkning (Foucault, 1979; Martin, van Brakel og Bernhard, 2009). Myndighetenes indirekte styring gjennom overvåkning, fører dermed til en selvdisiplin hos administratorer, kjøpere og selgere på kryptomarkedene (Foucault, 1991; Garland, 1999).

Foucault sin panoptikonmodell er imidlertid ikke tilstrekkelig til å forklare dagens overvåkningspraksiser. Overvåkningsdynamikken som hittil er skissert, går begge veier og illustrerer en overvåkning som kan forklares som en kombinasjon av panoptisk og synoptisk overvåkning (Mathiesen, 1997). Det vil si at på det mørke nettet er det både overvåkning hvor få ser mange, men også mange som ser få. En annen måte å forklare denne overvåkningsdynamikken på det mørke nettet er sousveillance. Sousveillance forklarer hvordan overvåkning kan foregå nedenfra og opp, i tillegg til andre måter å overvåke på

(Mann og Ferenbok, 2013). Basert på overvåkningen kjøpere og selgere på kryptomarkeder retter mot myndighetene, gjør at myndighetene også disiplineres til å øke sin kompetanse på kryptering for å tilpasse seg de ekstra sikkerhetstiltakene kjøpere og selgere på det mørke nettet forsøker å innføre (Foucault, 1991). Foucaults panoptikonmodell må suppleres med andre modeller for å forklare hvordan overvåkning foregår på kryptomarkedene. Følgende vil jeg hevde at surveillant assemblage kan tilby en mer samlet modell til å forklare overvåkningsdynamikkene på det mørke nettet.

5.3.2 Overvåkningsdynamikker på det mørke nettet i lys av surveillant assemblage

Overvåkning i det postmoderne samfunnet kjennetegnes ved at det ikke bare er myndighetene som overvåker samfunnsborgere, men at det går flere veier (Walby, 2005). Jeg har allerede presentert hvordan myndighetene overvåker administratorer, kjøpere og selgere på kryptomarkeder, og hvordan denne overvåkningen er gjensidig. Dupont (2008) mener at overvåkningsmiljøet på internett er basert på en anti-panoptisk arkitektur. Det vil si at det ikke bare er myndighetene som overvåker samfunnsborgere og motsatt, men at samfunnsborgerne også overvåker hverandre. Kjøpere og selgere på kryptomarkeder har egne mekanismer for å overvåke hverandre, som for eksempel gjennom en tilbakemeldingsfunksjon. Selgere av narkotika på det mørke nettet er avhengig av gode tilbakemeldinger for å kunne selge produkter, og ærlige selgere bygger sin tillit basert på et såkalt internettomdømme (Espinosa, 2019). På denne måten kan en person som ønsker å kjøpe narkotika på det mørke nettet overvåke ulike leverandører gjennom tilbakemeldinger andre kjøpere har gitt. Dette kan være en fordel for kjøper som kan bli kvitt useriøse selgere, beretter kontrolløren Ole:

> Det er jo positivt i den form at vi blir kvitt useriøse selgere da. Vi ser jo at det er denne markedsmodellen som brukes på alt, den vanlige tillitsbaserte kjøpsmodellen. Selgere er avhengig av å gjøre en god handel, ellers får de dårlige tilbakemeldinger. Det vil jo påvirke salget hvis man får mye dårlige tilbakemeldinger. […] Det her er jo distribuering hvor det eneste du har er et navn. Det her er ikke kompisen til kompisen som distribuerer på en måte. Det her er et navn, som gjerne er et nick, som du har brukt ganske lang tid på å bygge deg opp. Det å bare miste det med en gang, er jo på en måte å starte fra scratch da. Dette kan kanskje være positivt for kjøpere, fordi

> selgere som for eksempel selger bøffestoff muligens lukes vekk. […] Det er definitivt noen positive ting ved kjøpsmodellen, og derfor brukes lignende modeller av nettsider hvor man ellers handler lovlige varer.

Denne informanten mener at det er positive sider ved kjøpsmodellen spesielt fordi en selger av narkotika som har gode tilbakemeldinger, har brukt ganske lang tid på å bygge seg opp og bli anerkjent. Det kan derfor ha store konsekvenser for en selger dersom han eller hun mister denne anerkjennelsen ved å få negative tilbakemeldinger dersom vedkommende ikke leverer som forventet. Kjøpsmodellen og tilbakemeldingsfunksjonen på det mørke nettet kan forstås som en digital form for overvåkning hvor kjøpere kan overvåke selgere. Dette er et eksempel som viser at overvåkningsdynamikkene på det mørke nettet er ikke like ensidig som Foucaults (1979) panoptikonmodell illustrerer. Det er heller ikke tilstrekkelig å supplere med modeller som bygger på panoptikon for å forklare hvordan overvåkning foregår på det mørke nettet. Lyon (2007) mener at panoptikonmodellen har hjelpsomme funksjoner, og at den fungerer som en metafor for total makt over hjelpeløse ofre. Samtidig mener han at vi må forlate denne modellen når det kommer til å forklare dagens overvåkningspraksiser, og at det finnes bedre måter å forstå overvåkning.

En modell for å forklare overvåkningen som skjer internt mellom kjøpere og selgere på det mørke nettet er lateral surveillance, oversatt til lateral overvåkning. Lateral overvåkning innebærer samfunnsborgeres overvåkning av andre samfunnsborgere basert på ulike risikovurderinger (Andrejevic, 2005). Tilbakemeldingsfunksjonen på kryptomarkedene fungerer som en teknologi for kjøpernes beregning av risiko. Det mørke nettet er bygget opp ganske likt som en vanlig nettside hvor man kan handle varer, og noen refererer til kryptomarkeder som eBay for narkotiske stoffer (Martin, 2014). De profesjonaliserte og brukervennlige funksjonene som er på kryptomarkeder gjør at det kan sammenlignes med legale markedsplattformer på internett. Et eksempel på hvordan den laterale overvåkningen foregår, forklares på følgende måte av kontrolløren Peder:

> Det er jo på en måte en form for god kundeservice ovenfor kunden. At du må opptre på en god måte som selger for å få god feedback, du må ha et godt produkt, og du må være i stand til å sende det på en trygg og forsvarlig måte. Det gjør jo at det blir færre eksempler på svindel da. Det blir vanskelig å drive utstrakt svindel, eller ”scamming” som vi kaller det. Du kan kanskje lure ti kunder, så må du stenge kontoen din fordi du

> blir avslørt. Det at de trenger gode tilbakemeldinger, gjør at det er de seriøse selgerne som blir igjen. På godt og vondt.

Basert på kontrolløren sitt utsagn kan det tolkes at tilbakemeldingsfunksjonene tilhørende markedsplassene på det mørke nettet gjør at det blir vanskelig å drive svindel i stor skala. Det er en viss risiko for å bli svindlet, men det er utfordrende for selgere å svindle mange før noen kjøpere vil skrive det i tilbakemeldingsfunksjonen. Formålet med tilbakemeldingsfunksjonen er å oppnå en trygghet for kjøperen og for at de skal unngå å bli svindlet (Tzanetakis, m.fl., 2015; Bakken og Demant, 2019). Kjøpere foretar digital overvåkning ved hjelp av tilbakemeldingsfunksjonene for å vurdere om selgeren er til å stole på. Kryptomarkeder er basert på tilbakemeldingsfunksjonene, og markedsplassene på det mørke nettet er helt avhengige av denne overvåkningen for å fungere. Kontrolløren Peder mener at tilbakemeldingsfunksjonene på det mørke nettet legger til rette for at det kun er seriøse selgere som kan bli igjen på plattformene, og dette kan anses som både ”godt og vondt”.

Tilbakemeldingsfunksjonen sitt formål er å skape en trygghet til seriøse selgere, men den kan også gi en falsk trygghet hos kjøperne. I underkapittel 5.2.1 forklarte jeg at det foregår flere former for digital vold, blant annet svindel, på det mørke nettet. Tilbakemeldingsfunksjonen sitt formål er å forebygge denne formen for digital vold, likevel kan den også misbrukes. En selger kan for eksempel kjøpe stoffer av seg selv og gi positive tilbakemeldinger på sin egen profil på det mørke nettet. En selger kan også bygge opp et godt omdømme som tilsier at vedkommende er til å stole på, for så å plutselig endre væremåte og svindle folk for penger (EMCDDA, 2016). Utfordringen med det digitale er at man ikke alltid kan stole blindt på sporene som legges igjen på internett. Kontrolløren Tore forklarer utfordringene med tilbakemeldingsfunksjonen på det mørke nettet:

> Det blir jo litt som om jeg skal kjøpe noe på Finn. Der ser jeg at selgeren har en rating. Så det gir meg en følelse av at andre har vært fornøyd med det de kjøpte av han. Men problemet er at dette her kan manipuleres, dras og ordnes. Det opprettes nye profiler og de kan være falske. Hvis du får alle vennene dine til å gi deg en god feedback så har du plutselig fått en god score.

Informanten mener at tilbakemeldingsfunksjonen som brukes for at kjøpere skal overvåke selgere med mål om en vellykket handel, kan manipuleres på flere måter av selgerne. Noen selgere utnytter denne tilbakemeldingsfunksjonen som skal fungere som en overvåkningsmekanisme. Disse utfordringene fører til at kontrolløren Jan ikke ser noen fordeler ved markedsmodellen for kjøp og salg av narkotika på det mørke nettet:

> Jeg klarer ikke å se at det er noe positivt i det hele tatt. Jeg klarer det ikke. For det er en kjensgjerning at dette faker de til. De oppretter profiler, kjøper av seg sjøl, legger ut egne reviews, og får ufortjent kudos for salg de har gjort. Så det er ikke noe du kan stole på. Det er heller noe som ikke er bra. […] En falsk trygghet, ja. Dette er noe vi har erfart i saker. At det her gjør dem for å på en måte bygge opp sin egen legende.

I dette sitatet forteller informanten at de som myndighetspersoner har sett eksempler i saker hvor selgere har hatt tilbakemeldinger om seg selv som er falske. Dette gjør at de kan bygge opp sitt eget repertoar basert på falskhet, noe som videre skaper en falsk trygghet hos kjøper. Kjøper tror at selger er til å stole på basert på tilbakemeldingene på selgers profil, men det er ikke alltid de er basert på sannheten. Kjøpernes overvåkning av selgere på kryptomarkeder gjennom tilbakemeldingsfunksjonene vil ikke alltid føre til at de ser det sanne bildet.

Som allerede beskrevet, kan lateral overvåkning forklare overvåkningen som foregår mellom kjøpere og selgere på kryptomarkeder. Modellen inkluderer ikke alle de andre overvåkningsprosessene som foregår på det mørke nettet. Lyon og Bauman (2013) anser overvåkning i det moderne samfunnet som ”liquid”, altså flytende. Overvåkningsdynamikkene på det mørke nettet kan også anses for å være flytende, som vil si at overvåkning skjer fra alle kanter og er mindre sentralisert sammenlignet med panoptikon. Jeg har tidligere forklart at Foucaults (1979) panoptikonmodell har blitt møtt med mye kritikk fra andre forskere, og at jeg også mener at den ikke er en tilstrekkelig modell til å forklare overvåkningen som foregår på krypterte nettverksplattformer.

En modell som kan forklare overvåkningspraksisene på det mørke nettet på en mer helhetlig måte er surveillant assemblage (Haggerty og Ericson, 2000). Dette overvåkningsperspektivet innebærer konseptuelle verktøy som belyser hvordan overvåkningssystemer fungerer og knyttes sammen (Haggerty og Ericson, 2000). For å forklare surveillant assemblage kan man se for seg en plante, en jordstengel (rhizome), som sender ut planteskudd i ulike retninger

hvor hver av de har sin egen rot (Lyon, 2007). Surveillant assemblage tar høyde for et hierarki, men i en form der alt er tilkoblet hverandre og vokser på ulike nivåer i planten (Haggerty og Ericson, 2000). Anvendt til overvåkningsdynamikkene på det mørke nettet vil alle som er på det mørke nettet ha sin egen rot i jordstengelplanten, og vil derfor ha muligheten til å overvåke og bli overvåket. De vil kanskje befinne seg på ulike nivåer i et hierarki, men de vil overvåke i forskjellige retninger. Kjøpere og selgere av narkotika på de krypterte markedsplassene vil for eksempel sende ut skudd fra røttene sine rettet mot både hverandre og myndighetene. I dag er overvåkning og styring noe som ikke bare myndighetene er involvert i (Lyon, 2007). Dette gjelder også på det mørke nettet, for som tidligere nevnt, vil kjøpere og selgere på krypterte markedsplasser i tillegg til å overvåke tilbake på myndighetene, også overvåke hverandre. Surveillant assemblage vil derfor være en bedre rustet modell sammenlignet med Foucaults panoptikonmodell til å forklare hvordan overvåkningsdynamikken foregår på kryptomarkeder.

Surveillant assemblage-modellen vil også være mer relevant til å forklare hvordan alle som har nok teknologisk kompetanse til å få tilgang til det mørke nettet, kan overvåke og bli overvåket der. Et eksempel er fra Adresseavisen i en artikkel kalt ”Teppefall” som er skrevet av journalisten Jonas Vikan (2015). I artikkelen forteller Vikan om hvordan han klarte å identifisere en stor norsk narkotikaselger på det mørke nettet som senere fikk fengselsstraff for dette. Vedkommende var i utgangspunktet helt anonym på det mørke nettet under pseudonymene ”Kvalitetsbevisst” og ”Alfa&Omega”. Kommunikasjon mellom selgeren og kundene hans foregikk over kryptert e-post, men denne krypterte e-postadressen hadde lignende navn som en annen e-postadresse som kunne kobles til et finansforum på det åpne nettet fra noen år tilbake i tid. Ut ifra disse små kjennetegnende klarte journalisten Vikan å identifisere en stor norsk leverandør på det mørke nettet. Dette eksempelet viser hvordan alle som har nok teknologisk kompetanse til å få tilgang til kryptomarkedene har mulighet til å overvåke der. Med alle disse forskjellige overvåkningsdynamikkene, stiller kontrolløren Arne seg spørsmålet om hvorvidt det mørke nettet egentlig er så mørkt:

> […] Vi kan være flue på veggen på narkotikamarkedet og det var jo utenkelig før. Det er ikke svart lenger. Det mørke nettet, jeg veit ikke om det faktisk er så veldig mørkt, når vi sammenligner med salg av narkotika på gata. Det er ekstremt mye spor i det mørke nettet, og det er veldig nyttig for oss.

Informanten ser det mørke nettet som nyttig for myndighetene, nettopp fordi det kan overvåkes. Kryptomarkeder kan gi myndighetene innsyn i narkotikadistribusjon på en måte de aldri hadde fått på narkotikahandelen på gaten. Myndighetene kan innhente informasjon på det mørke nettet og slik som kontrolløren Arne sier, kan myndighetene være flue på veggen på et narkotikamarked. På bakgrunn av alle disse overvåkningsdynamikkene som foregår på kryptomarkedene kan det argumenteres for at det mørke nettet ikke er så "mørkt". Jeg har tidligere forklart at "darknet"-begrepet har mystiske, kriminelle og truende assosiasjoner (Tzanetakis, 2017). Mirea, Wang og Jung (2019) har konkludert sin forskning med at det mørke nettet ikke bare er "mørkt" på bakgrunn av at det er flere personer som benytter seg av det mørke nettet for lovlige handlinger. Jeg vil bygge videre på dette og argumentere for at det mørke nettet ikke er så "mørkt" fordi det ikke er så usynlig og mystisk som det kan se ut til med første øyekast. Det er ikke helt sikkert at man klarer å gjemme seg i mørket fordi man er sårbar for overvåkning på kryptomarkedene.

Markedsplassene på det mørke nettet er avhengig av overvåkning. Tilbakemeldings-funksjonen på kryptomarkeder fungerer som en overvåkningsmekanisme hvor kjøpere kan overvåke selgere, og basert på dette kan de velge å handle av de som har fått gode tilbakemeldinger fra tidligere kjøpere. Denne overvåkningsprosessen kan forklares som lateral overvåkning (Andrejevic, 2005). Tilbakemeldingsfunksjonen er ikke alltid til å stole på, og ifølge informantene finnes det flere eksempler på tilfeller hvor disse manipuleres. Krypterte nettverk er utviklet for å legge til rette for anonymitet, men samtidig gir det myndighetene en direkte tilgang til å overvåke narkotikadistribusjonen der. På bakgrunn av den flytende overvåkningsdynamikken, blir panoptikonmodellen til Foucault (1979) for snever alene til å forklare overvåkning på det mørke nettet (Lyon og Bauman, 2013).

Overvåkningspraksisene på det mørke nettet kan bedre belyses ved å supplere Foucaults (1979) panoptikonmodell med andre overvåkningsperspektiver, inkludert surveillant assemblage (Haggerty og Ericson, 2000). Dette gir en bedre forståelse av at det er flere enn myndighetspersoner som overvåker på det mørke nettet. At det foregår overvåkning på det mørke nettet er det ingen tvil om, og basert på denne kartleggingen av overvåkningsdynamikkene på det mørke nettet mener jeg at det mørke nettet ikke er så "mørkt". Krypterte nettverk er åpent for alle som har nok teknologisk kompetanse for å ta seg inn, og det foregår overvåkning i alle retninger selv om de har en kryptert form. Krypterte nettverksplattformer forsøker å legge til rette for anonymitet, men gjentatte ganger innfris

ikke dette. Hvis man ønsker å handle narkotika på det mørke nettet innebærer det en risiko for å kunne bli identifisert av myndighetene.

5.3.3 Panspektrisk overvåkning og datadoubles på det mørke nettet

Jeg har allerede presentert en kartlegging av overvåkningsdynamikkene på det mørke nettet og på bakgrunn av dette argumentert for at det mørke nettet ikke er så "mørkt". Jeg har også beskrevet et eksempel på hvordan journalisten Vikan (2015) klarte å identifisere en stor norsk narkotikaselger på det mørke nettet. Mesteparten av overvåkning krever en form for identifikasjonsprosess (Lyon, 2007). I tillegg til å samle inn etterretningsinformasjon kan myndighetspersonene som jobber med å kontrollere det mørke nettet også lete etter identitetsmarkører for å identifisere kjøpere og selgere på kryptomarkedene:

> […] Men det jeg gjør er egentlig å jakte på identitetsmarkører, altså små puslespillbriller som kan være med å identifisere. Så prøver jeg å danne et bilde av hvem som gjemmer seg bak profilen. Og da kan jeg bruke ting jeg finner andre steder på nettet, fra postpakker eller fra annen etterretning.

Dette sitatet er fra kontrolløren Peder som forklarer hvordan han forsøker å identifisere personene som gjemmer seg bak profilene på det mørke nettets markedsplasser. Han belyser videre hvordan han blant annet finner informasjon som ligger lagret på internett til å komme frem til hvem som står bak de ulike brukerprofilene på det mørke nettet. Denne formen for overvåkning som kontrolløren Peder forteller om kan relateres til dataveillance, også kalt panspektrisk overvåkning. Det innebærer at man overvåker uten å bruke synet direkte, men baseres på en innsamling av detaljert informasjon for å skape en profil som ligner på de som blir sett (Lupton, 2015). Panspektrisk overvåkning vil ta utgangspunkt i personers aktiviteter og kommunikasjon digitalt (Lyon, 2007). Internett sin lagringsegenskap gjør at digital informasjon er søkbar og sporbar, noe som danner grunnlag for en større tilgjengelighet og skaper en ny relasjon mellom fortid, nåtid og fremtid (Kaufmann og Jeandesboz, 2016). Myndighetene finner informasjon om personer på internett som i utgangspunktet ble publisert for andre formål enn at myndighetene i fremtiden skulle bruke det til å identifisere kjøpere og selgere på kryptomarkeder.

For å overvåke på det mørke nettet må myndighetene selv laste ned en krypterings-programvare, som for eksempel TOR, for å få tilgang. De vil benytte seg av et bredt spekter av teknologi og håndtere store mengder med digital data i forbindelse med overvåkning av kryptomarkeder. Myndighetenes overvåkning på internett påvirkes av de store mengdene med digital data som ligger lagret på internett, noe som har resultert i økt strategisk og fremtidsrettet fokus i myndighetenes overvåkningspraksiser (Lupton, 2015). På bakgrunn av internettutviklingen er det ikke nødvendigvis bare fysiske kropper som overvåkes. Personer overvåkes også som abstrakte kropper på internett (Lyon, 2007). For eksempel kan en person ha mange ulike brukerprofiler på diverse nettsider på internett. De abstrakte kroppene overvåkes, som for eksempel brukerprofilene på det mørke nettet. En person kan inneha flere "personer" ut ifra hvordan overvåkeren tolker vedkommende basert på ulike karakteristika som overvåker mener kan passe til forskjellige grupper (Haggerty og Ericson, 2000). En person kan for eksempel ha en brukerprofil på Facebook og en helt annen type brukerprofil som selger på det mørke nettet.

Våre digitale data er i mindre grad knyttet til den fysiske kroppen vår (Lyon, 2007). Vi blir målt og overvåket av myndighetene uten å snakke ansikt til ansikt som tidligere, og man blir koblet fra sin egen kropp for byråkratiske formål. Ved å abstrahere menneskelige kropper fra deres opprinnelige kontekst lages det som Haggerty og Ericson (2000) kaller datadoubles. Fraværet av fysisk kontroll og tilstedeværelse er erstattet med et vidt spekter av databaser og fjernkontroll (Salter, 2010). Når myndighetene overvåker markedsplassene på det mørke nettet, og forsøker å identifisere de som kjøper og selger narkotika på kryptomarkeder, blir ikke individene sett på som enkeltpersoner. De kobles fra sine fysiske kropper, blir sett på som brukernavn i de tilhørende digitale profilene og plasseres i kategoriserte grupper som for eksempel kjøpere eller selgere av narkotika på internett. I underkapittel 5.2.1 beskrev jeg hvordan andres misbruk av våre datadoubles kan kjennes fysisk i kroppen vår. Når vår digitale data utnyttes av andre, vil den som dataene stammer fra føle dette i kroppen sin.

Jeg vil i det følgende belyse hvordan datadoubles kan utvides til å forklare hva som skjer når myndighetene bruker digital data til å identifisere tilbake til fysiske personer. Datadoubles som kjøpere og selgere på det mørke nettet legger igjen på internett kan gjøre det mulig for myndighetene å identifisere personene bak brukerprofilene. De som benytter seg av kryptering utsetter seg for en større risiko for å bli identifisert sammenlignet med de som kjøper eller selger narkotika i det fysiske livet utenfor internett. Dette er på bakgrunn av at all

informasjon på internett er sporbar på en helt annen måte enn informasjon i verden utenfor internett. Det er vanskelig å slette digital informasjon på internett, og det vil alltid ligge igjen spor som lagres (Kaufmann og Jeandesboz, 2016). Myndighetspersonene som kontrollerer det mørke nettet søker etter informasjon som ligger lagret på internett for å finne ut hvem som selger og kjøper narkotika på kryptomarkeder. Kontrolløren Kjetil forteller at det er ulike identifikasjonsspor myndighetene leter etter når de skal forsøke å identifisere kjøpere og selgere på det mørke nettet:

> Det er det med å skaffe en inngang. Det er det som er vanskelig. Den første inngangen, så du kommer i posisjon til å ta noen. Det er gjerne det å lete etter noen feil de har gjort, eller prøve å finne andre innfallsvinkler som gjør at man kan identifisere de som sitter bak. Det er det som er den tunge biten.

Informanten forklarer at det kan være utfordrende å identifisere brukerne på det mørke nettet. Myndighetene må lete etter feil knyttet til kryptering og anonymiseringen som personer har gjort for å avsløre dem. Basert på utsagnene til kontrolløren Peder og kontrolløren Kjetil tolker jeg at datadoubles vi har på internett kan benyttes til å identifisere tilbake til de fysiske kroppene som står bak de digitale brukerprofilene. De digitale sporene som myndighetspersonene bruker til å identifisere personer gjør at de abstrakte kroppene kan kobles tilbake til de fysiske kroppene. Med datadoubles kobles individer fra sine kropper, men med overvåkningen og identifiseringen myndighetspersoner foretar seg på det mørke nettet, kan det være mulig å koble kjøpere og selgere bak de krypterte brukerprofilene tilbake til sin opprinnelige identitet og fysiske kropp.

Myndighetenes overvåkning på det mørke nettet kan anses som panspektrisk overvåkning. De bruker et bredt spekter av teknologi til å overvåke og samle inn store mengder med digital data. Den digitale informasjonen som samles inn brukes blant annet til å forsøke å identifisere de personene som er bak de anonyme brukerne på det mørke nettet. Sporene som ligger lagret om personer på internett kan refereres til som datadoubles. Haggerty og Ericsson (2000) mener at med datadoubles kobles individet fra sin fysiske kropp til mange små digitale biter. Jeg har i dette delkapittelet forklart at dette datadoublesperspektivet kan tas et steg videre. Når myndighetene bruker personers datadoubles på internett til å identifisere hvem som står bak brukerprofilene på det mørke nettet, er det datadoubles er årsaken til at de kan identifiseres tilbake til en persons fysiske kropp. Selv om det mørke nettet skal være

anonyme plattformer, finnes det overvåkningspraksiser der som brukes til å identifisere hvem som står bak de anonyme brukerprofilene. Overvåkningsdynamikkene på det mørke nettet påvirker myndighetenes konkrete tiltak rettet mot styring av narkotikadistribusjonen på det mørke nettet. Jeg vil illustrere dette videre i neste underkapittel ned blant annet at det viktigste for myndighetene er å forebygge samfunnsborgerne fra å gå inn på krypterte markedsplasser.

5.4 "Det må føles usikkert, så dem kanskje avstår": Forebygging og nedstenging av markedsplassene

Myndighetenes syn på det mørke nettet, og utfordringene knyttet til kryptomarkeder, vil være med på å utforme deres holdninger til styring rettet mot denne formen for markedskriminalitet. I dette underkapittelet vil jeg forklare hvordan myndighetenes styring og overvåkning utføres med et forebyggende formål. Forebyggende tiltak er å anses som forebyggende om de avverger eller reduserer det myndighetene definerer som risiko for skade (Ashwort og Zedner, 2014). Jeg vil med utgangspunkt i governmentalityteori, uttrykke at myndighetenes styring på kryptomarkeder har et forebyggende formål. Med forebyggende styring ønsker myndighetene å styre samfunnsborgerne til å styre seg selv (Garland, 1999).

En styringsmekanisme som myndighetene gjør med forebyggende formål, er nedstenging av markedsplassene på det mørke nettet. Myndighetenes nedstenging av de store kryptomarkedene vil føre til en økning i den følte oppdagelsesrisikoen. Dette kan ha en avskrekkende effekt, og forebygge at folk velger å benytte seg av kryptomarkeder for kjøp og salg av narkotika. Avskrekking vil være et middel myndighetene bruker i forsøk på å beskytte samfunnet (Salter, 2010). Nedstenging av markedsplasser på det mørke nettet kan illustreres som en modell for å forebygge samfunnsborgernes ulovlige aktiviteter (Lyon, 2007). Jeg vil diskutere myndighetenes nedstenging av markedsplassene, som en styringsmekanisme som anses for å være både direkte og indirekte. Videre vil jeg vise at overvåkning og styring som myndighetene foretar seg for å beskytte samfunnsborgerne, og få samfunnsborgerne til å styre seg selv til å motstå kryptomarkeder, kan føre til at myndighetenes overvåkning blir vanskeligere i fremtiden.

5.4.1 Myndighetenes holdninger til forebygging på det mørke nettet

Når det kommer til hvordan det mørke nettet skal styres, er *forebygging* et viktig nøkkelbegrep som trekkes frem av myndighetene. I det senmoderne samfunnet kjennetegnes myndighetenes styring med at det er større fokus på forebygging av kriminalitet fremfor etterforskning og straff etter at de ulovlige handlinger er begått (Lomell, 2012). Jeg har tidligere forklart at Foucaults panoptikonmodellen kan være en metafor til å forklare myndighetenes maktposisjon i overvåkningsprosesser (Foucault, 1979; Lyon, 2007). Hovedformålet med myndighetenes overvåkning av kryptomarkeder er at samfunnsborgerne disiplinerer seg selv til å la vær å oppsøke det mørke nettet for kjøp og salg av narkotika. Generelt er overvåkningens funksjon å få folk til å styre seg selv, som igjen knyttes til risikohåndtering i styringsprosessene som Garland (1999) tar for seg. Dette kan forklares med et utdrag fra rapporten "Internet Organised Crime Threat Assessment" (Europol, 2019, s. 7) hvor det står:

> […] More coordinated investigation and prevention actions targeting the phenomenon are required, demonstrating the ability of law enforcement to have a lasting impact and deterring users from illcit activity on the dark web.

I dette utdraget belyses myndighetenes forebyggende rolle i forbindelse med narkotikadistribusjonen på det mørke nettet. Dette sitatet illustrerer ulike anbefalinger om hvordan myndighetene burde styre det mørke nettet. Det interessante med dette sitatet fra denne IOCTA (2019) rapporten, er det forebyggende perspektivet i Europol sine råd. De mener at det er nødvendig at myndighetene får en mer koordinert etterforskning og forebyggende aksjoner på det mørke nettet. De anbefaler at dette gjøres for å demonstrere hvilke muligheter myndighetene har på styring på kryptomarkeder slik at det kan ha en langsiktig påvirkning på ulovlige aktiviteter på det mørke nettet. Europol forklarer hvordan myndighetene kan forebygge brukere til å utføre ulovlige aktiviteter på krypterte markedsplasser ved å vise frem hva slags styringsmekanismer de har på det mørke nettet.

Det var flere av informantene som trakk frem forebygging av kriminalitet som et viktig fokus i myndighetenes styring av narkotikadistribusjonen på det mørke nettet. Kontrolløren Ole sier at: "[…] Det er et av myndighetenes samfunnsoppdrag å forebygge kriminalitet der kriminalitet skjer. Om kriminalitet kun hadde vært analog på gata, så skulle ikke vi vært på

internett. Men siden kriminalitet skjer på internett må vi være der og". Det er to viktige momenter med dette sitatet. For det første trekker han frem at det er myndighetenes samfunnsoppdrag å forebygge kriminalitet. Med dette kan det tolkes at forebygging er å anse som en viktig drivkraft bak myndighetenes styring. Det andre momentet i det informanten skisserer, er at myndighetene ikke hadde vært til stede på internett om det ikke hadde vært for at det foregikk kriminalitet der. Myndighetene har et ansvar for å overvåke der kriminalitet skjer, også på internett, for å forebygge ulovlige handlinger.

Forskere som har utført kvalitative intervjuer med personer som kjøper narkotika på det mørke nettet, og som har analysert ulike nettforum, har konkludert med at hovedårsakene til at personer velger å handle narkotika på det mørke nettet er større tilgjengelighet av rusmidler, kvaliteten på stoffene man kan få tak i, samt lav oppdagelsesrisiko (Barratt, Ferris, og Winstock, 2014; Bakken og Bosnes, 2015; Bancroft og Reid, 2016). Analysen har allerede diskutert hva myndighetene tenker angående den økte tilgjengeligheten av narkotiske stoffer på det mørke nettet i underkapittel 5.2.2. Den andre viktige hovedårsaken til at personer velger å handle narkotika på det mørke nettet er den lave opplevde oppdagelsesrisikoen. Kontrolløren Jan mener at det burde være like stor oppdagelsesrisiko knyttet til narkotikadistribusjon uavhengig av hvilken arena det foregår på:

> […] Det må forbindes med like stor oppdagelsesrisiko å drive narkotikavirksomhet på nett som det gjør i det virkelige liv. Så det skal være relativ like stor sjanse for å bli tatt som narkotikaselger om du operer på nett, om du står langs Akerselva, eller om du står på plata. […]

Dersom myndighetene gjennom sin overvåkning på det mørke nettet kan skape en følelse av at det er en risiko for å bli oppdaget når man kjøper og selger narkotika, vil det forebygge at personer oppsøker kryptomarkeder. Kontrolløren Tore mener at de fra myndighetenes ståsted ikke gjør nok i dag når den følte oppdagelsesrisikoen blant kjøpere og selgere på kryptomarkeder er lav:

> Vi må øke den følte oppdagelsesrisikoen, for vi ser inne i noen forumer nå at dem sier det er lav risiko. Den er lik null, både for kjøp, betaling og forsendelse. Da gjør vi ikke nok. Det er klart det er litt den følelsen i den fysiske verden også, men den er ikke helt lik null, selv om den ikke er langt unna der heller. Det er ikke noe vanskelig

> å kjøpe fem gram hasj i Oslo uten å bli tatt fra politiet, men det er tilnærmet helt risikofritt på nettet. Det må føles usikkert, slik at de kanskje avstår tenker jeg.

Denne uttalelsen indikerer at informanten mener det er myndighetenes oppgave å ta ansvar for å øke den opplevde oppdagelsesrisikoen på det mørke nettet med formål om at noen avstår fra å benytte seg av kryptomarkeder for kjøp og salg av narkotika. Den følte oppdagelsesrisikoen er relativt lav i forbindelse med narkotikadistribusjon generelt sett, men på det mørke nettet er den mer eller mindre lik null ifølge kontrolløren Tore. Kontrollørene mener at det kan være en viktig forebyggende effekt å øke den opplevde oppdagelsesrisikoen på kryptomarkeder. Dette kan kobles til governmentalityteori, hvor hovedprinsippet er at samfunnsborgerne er ansvarlig for egne valg, men myndighetene skal gjøre det de kan for at samfunnsborgerne disiplineres (Foucault, 1991). Dersom myndighetene kan øke den følte oppdagelsesrisikoen for kjøp og salg av narkotika på det mørke nettet, kan de på den måten styre personer til å selv ta valget om å avstå fra å bruke kryptomarkeder. Når det mørke nettet føles usikkert, mener kontrolløren Tore at personer vil avstå fra krypterte markedsplasser. På denne måten kan myndighetene styre samfunnsborgerne til å styre seg selv (Garland, 1999).

Sentralt for styring i senmoderne samfunn er at myndighetene skal styre samfunnsborgernes sjel gjennom å skape frie subjekter som er ansvarlige for egne liv (Rose og O´Malley, 2006). Hvis myndighetene kan påvirke den opplevde oppdagelsesrisikoen på kryptomarkeder, og dette fører til at kjøpere og selgere avstår fra handel på det mørke nettet, er dette et eksempel på hvordan myndighetene kan påvirke samfunnsborgerne til å ta de beste valgene for seg selv. Myndighetene vil gjennom sine styringsmekanismer forsøke å få de aktive subjektene til å frastå fra å bruke det mørke nettet for kjøp og salg av narkotika ved å øke den opplevde oppdagelsesrisikoen. For å gjennomføre dette mener kontrolløren Jan at: ”Vi burde på bakgrunn av det forebyggende perspektivet kanskje hatt mer muligheter til å ha kontrollfunksjoner på nettmarkedene”. Med dette sitatet forteller informanten at de som myndighetspersoner burde hatt flere styringsmuligheter på det mørke nettet på bakgrunn av det forebyggende perspektivet. Mens noen mener at myndighetene burde ha flere muligheter til å overvåke på det mørke nettet, mener andre at det ikke ville vært nok å ha flere kontrollfunksjoner så lenge sakene ikke følges opp. Kontrolløren Kjetil forteller at noen er kritiske til at myndighetene ikke har fokusert på å berøre narkotikakjøpere på det mørke nettet:

> Det har vært en tradisjon at myndighetene går etter selgere og ikke kjøpere, som noen kanskje kritiserer nettopp på grunn av den forebyggende effekten. Så lenge du bare kjøper så er du trygg, og det er selgerne som løper all risikoen. Det er noe av kritikken som man ser fra toll mot politiet for eksempel. Alt som tas i beslag i post av toll, blir bare henlagt. Det samme gjelder alle disse store sakene vi har hatt på markedsplassene, hvor det er sjeldent man har berørt noen kjøpere i det hele tatt. Det har vært et par kjøpere som har ryki for å lage et komplett bilde av saken når man går til retten, men da har det vært storkjøpere som har drevet videresalg kanskje i den fysiske verden. Ellers har man lagt vekk alt som heter kjøpere selv om man har hatt masse navn og adresser. Kanskje det er fornuftig, og kanskje ikke. […]

Det er flere elementer ved dette sitatet som kan tolkes som kritikk mot myndighetenes forebyggende arbeid i forbindelse med narkotikadistribusjonen på det mørke nettet. Utsagnet indikerer at myndighetene i hovedsak har vært ute etter å straffe selgere og ikke kjøpere på de krypterte markedsplassene. Dette vil trolig ha minimal forebyggende effekt på de som handler narkotika på det mørke nettet. Kontrolløren Kjetil trekker også frem at Tolletaten kritiserer politiet for å henlegge postbeslagene de har tatt som kan knyttes til narkotikadistribusjonen på det mørke nettet. Å straffeforfølge selgere og administratorer på det mørke nettet vil trolig øke den opplevde oppdagelsesrisikoen for dem, men det vil ha liten forebyggende effekt for de som vil kjøpe narkotika på det mørke nettet. Informanten mener at myndighetenes mangel på ressurser fører til at de ikke prioriterer å straffe kjøpere av narkotika på det mørke nettet selv om de har identifisert dem. Selv er han usikker på om disse prioriteringene er fornuftig eller ikke.

Forebygging har fått et gradvis større fokus i forbindelse med hvordan myndighetene møter utfordringer knyttet til kriminalitet (Lomell, 2012). Først og fremst ønsker myndighetene å forebygge at personer skal oppsøke det mørke nettet for kjøp og salg av narkotika. For å gjøre dette mener kontrollørene at myndighetene er nødt til å øke den følte oppdagelsesrisikoen. Myndighetenes overvåkning med formål om å forebygge og øke den opplevde oppdagelsesrisikoen på det mørke nettet kan kobles til governmentalityteorien, hvor hovedprinsippet er at samfunnsborgerne er ansvarlig for egne valg, men myndighetene skal gjøre det de kan for at samfunnsborgerne disiplineres (Foucault, 1991). Dersom myndighetene kan øke den følte oppdagelsesrisikoen for kjøp og salg av narkotika på det mørke nettet, kan de på den måten styre personer til å selv ta valget om å avstå fra å bruke

kryptomarkeder. På denne måten kan myndighetene indirekte styre samfunnsborgerne til å styre seg selv (Garland, 1999).

Frem til i dag har myndighetene hovedsakelig basert sitt forebyggende arbeid på det mørke nettet ved å fokusere på å avskrekke gjennom å straffe administratorer og selgere på kryptomarkeder. Noen av kontrollørene mener at dette kan påvirke folk til å avstå fra narkotikamarkedet på det mørke nettet, fordi de ser at myndigheten er til stede, mens andre mener at myndighetene også må rette søkelyset mot kjøperne på kryptomarkeder for å oppnå en større forebyggende effekt. En direkte form for styring myndighetene foretar seg på det mørke nettet med forebyggende formål er å stenge ned de store krypterte markedsplassene. Ved å stenge ned store kryptomarkeder vil myndighetene først og fremst disiplinere direkte ved å fjerne muligheten til samfunnsborgerne til å handle narkotika på disse plattformene (Foucault, 1991). Samtidig vil nedstenging av store kryptomarkeder øke den opplevde oppdagelsesrisikoen, og ifølge myndighetene også være en indirekte form for styring med mål om å forebygge (Garland, 1999).

5.4.2 Myndighetenes syn på nedstenging av markedsplasser på det mørke nettet

Forebygging var et nøkkelbegrep hos alle kontrollørene når de snakket om styring rettet mot narkotikadistribusjonen på det mørke nettet. Det er flere ulike teknikker som myndighetene kan benytte seg av som sikter på å forebygge lovbrudd som kan skje i fremtiden (Ashwort og Zedner, 2014). En slik form for teknikk, eller styringsmekanisme, som myndighetene har anvendt på narkotikadistribusjonen på kryptomarkeder, er å stenge ned de største markedsplassene. For eksempel ble det sommeren 2017 utført en internasjonal samarbeidsaksjon ledet av FBI og DEA og nederlandsk politi med støtte fra Europol. Aksjonen resulterte i at to av datidens største markedsplasser på det mørke nettet, Alphabay og Hansa Market, ble stengt. Rett før nettverkene ble lagt ned, fikk det nederlandske politiet, med hjelp fra tysk og litauisk politi, kontroll over Hansa Markedet i omtrent en måned. På bakgrunn av denne aksjonen fikk myndighetene stengt to store markedsplasser, arrestert mange store aktører og samlet inn store mengder med etterretningsinformasjon (Europol, 2017). Kontrolløren Kjetil mener at slik nedstenging av markedsplasser på det mørke nettet kan ha en forebyggende effekt:

> Jeg tenker at det først og fremst er forebyggende. Det er for å statuere eksempelet at det er ikke et fristed, men at det har konsekvenser og at du blir tatt her også. For det er den oppfattelsen mange har hatt, at det er et fristed. Det er først og fremst forebyggende, tenker jeg. Mange av dem som driver markedsplassene får store straffer.

Med denne uttalelsen adresserer informanten hvilken forebyggende virkning som kan oppstå ved å legge ned de store markedsplassene. Først og fremst kan det være forebyggende ved at myndighetene viser at det mørke nettet ikke fungerer som et anarki, men at ulovlige handlinger på kryptomarkeder kan få konsekvenser. Videre fremkommer det i sitatet at nedstenging av kryptomarkeder kan være forebyggende fordi administratorene på markedsplassene får store straffer, og det kan gjøre det mer utfordrende for dem å starte opp nye plattformer. Kontrolløren Jan er også positiv til at myndighetene legger ned de store kryptomarkedene: ”Da slår du hvert fall selgerne tilbake, som må starte på nytt igjen med en ny profil. Mange blir pågrepet og blir satt lagt tilbake. Oppdagelsesrisikoen mener jeg er viktig at er der ute”. Informanten mener at når myndighetene legger ned de store markedsplassene vil resultatet være at mange blir pågrepet, og de må starte opp på nytt igjen med nye brukerprofiler. Videre uttrykker han at det er viktig at oppdagelsesrisikoen er til stede på det mørke nettet, og nedstenging av markedsplasser kan være med på å øke den. Kontrolløren Peder sier at myndighetenes nedstenging av markedsplasser kan forebygge noen fra å gå inn å det mørke nettet:

> Du skaper uro i miljøet ved å gjøre det. Du samler og sikrer mye informasjon om både selgerne og kjøperne, og du kan straffeforfølge en del. Alt det her ser jeg på som positive sider. Du kan kanskje forebygge noen fra å fortsette å gå inn på det mørke nettet, ved at de tenker: ”Oi, nå var myndighetene her og stengte det. Kanskje jeg må tenke meg litt om før jeg gjør mer her på det mørke nettet”.

Ut ifra dette sitatet kan det tolkes at informanten mener det er nyttig å legge ned markedsplasser fordi det skaper en uro i miljøet på det mørke nettet. Ved å legge ned kryptomarkeder kan myndighetene både straffe personer for sine ulovlige handlinger og samtidig innhente mye informasjon. Kontrolløren Peder mener at nedstenging av markedsplasser også kan forebygge noen fra å fortsette å gå inn på det mørke nettet fordi de ser at myndighetene har vært der og stengt det. Dette er et konkret eksempel på hvordan

myndighetenes styring kan påvirke samfunnsborgerne til å styre seg selv slik governmentalityteorien skisserer (Garland, 1999). Når myndighetene gjør forebyggende tiltak som å stenge ned markedsplasser kan det påvirke personene til å ta et valg om å unngå å bruke det mørke nettet. Kontrolløren Ole fremmer at det er viktig at myndighetene gjør mer enn å bare stenge markedsplassene for å oppnå en forebyggende effekt:

> Å rett og slett bare stenge serveren tenker jeg at i utgangspunktet er bra. Vi blir jo kvitt en markedsplass. Hvis det er det eneste som gjøres, så er jeg ikke nødvendigvis sikker på den forebyggende effekten. Hvis vi gjør noe aktivt med spesielt kjøper og selger, så tror jeg fremgangsmåten er god. Metoden er kanskje litt treig, men jeg klarer ikke komme på en annen raskere måte å gjøre det på heller. Hvis du bruker flere år på å ta ned en server og de bruker en uke på å sette det opp igjen, så er kostnytten kanskje ikke høy nok.

Med utgangspunkt i denne uttalelsen vil myndighetene først og fremst fjerne en markedsplass ved nedstengingsaksjoner. Dette vil da være en direkte form for styring som myndighetene utøver for å disiplinere samfunnsborgerne ved at de tvinges til å være føyelige fordi kryptomarkedet ikke lenger er tilgjengelig (Foucault, 1991). Kontrolløren Ole mener samtidig at det er viktig at myndighetene også agerer mot kjøpere og selgere for å oppnå en forebyggende effekt. Det er her myndighetene vil disiplinere samfunnsborgerne til selvdisiplin (Garland, 1999). Informanten er videre usikker på hvor effektiv denne metoden er, fordi myndighetene bruker så mye ressurser på å legge ned en markedsplass som raskt kan bli satt opp på nytt. Administratorer, kjøpere og selgere på kryptomarkeder disiplineres ikke til å frastå markedsplassene, men de disiplineres til å sette opp nye.

Myndighetene forsøker å disiplinere samfunnsborgere ved å stenge ned markedsplasser, noe som i tillegg til å potensielt ha en forebyggende effekt, kan føre til at administratorer og selgere tilpasser seg myndighetenes styringsmekanismer. I rapporten ”Internet Organised Crime Threat Assessment” (Europol, 2019, s. 45) skisseres flere eksempler på tilpasninger som administratorer på kryptomarkedene foretar seg som en konsekvens av myndighetenes styring:

> However, for this market growth has been slow due to continued suspicion over law enforcement involvement. Finally, some markets have changed their policies to

> prohibit the sale of fentanyl and weapons and explosives in an attempt to avoid law enforcement attention. […]

Noen markeder tilpasser sine regler som for eksempel å forby salg av fentanyl, våpen og eksplosiver i et forsøk på å unngå myndighetenes oppmerksomhet. Her har administratorene på markedsplassene overvåket myndighetenes styring og sett at de prioriterer å legge ned nettverker som selger ekstra potente narkotiske stoffer, våpen og eksplosiver, og velger derfor å forby slik aktivitet på sine markedsplasser for å unngå myndighetenes søkelys. Akkurat denne overvåkingsdynamikken har tidligere i analyse- og diskusjonskapittelet blitt referert til som sousveillance (Mann og Ferenbok, 2013). Basert på min analyse av utdraget fra IOCTA (2019) rapporten kan det tolkes at til mer myndighetene overvåker det mørke nettet, desto mer vil administratorene tilpasse seg og gjøre det mer utfordrende for myndighetene å fortsette å overvåke. Myndighetenes nedstenging av kryptomarkeder vil disiplinere administratorer og selgere, men ikke nødvendigvis til at de slutter å distribuere narkotika. De vil disiplineres til å overvåke myndighetene tilbake og basert på det innføre flere tiltak for å motsette seg myndighetenes overvåkning. Imidlertid mener kontrolløren Tore at nedstenging av kryptomarkeder kan være lurt, selv om det bare vil flytte på seg:

> Det tror jeg kan være litt lurt. Men det blir jo som å legge ned plata, det forflytter seg bare. En viss grad av forstyrrelse tenker jeg må til. Noen av markedsplassene er jo reinspikka kriminalitet, og det å bare la de få holde på med det, det tenker jeg er… […] Du kan ikke la de få holde på helt fritt tenker jeg da.

Markedsplassenes forflytting kan føre med seg negative konsekvenser for myndighetenes fremtidige styring og overvåkning. Denne forflyttingen forklares nærmere i et utdrag fra rapporten ”Trusler og utfordringer innen IKT-kriminalitet” (Politidirektoratet, 2017, s. 16): ”Dersom myndighetene stopper et nettverk eller en markedsplass på internett, står som regel andre aktører raskt klare til å ta over narkotikahandelen”. Politidirektoratet beretter at når myndighetene legger ned markedsplasser på internett, vil andre aktører stå klar til å overta narkotikadistribusjonen. Basert på en analyse av dette utsagnet kan det tolkes at myndighetene er klar over at de ikke blir kvitt narkotikadistribusjonen på det mørke nettet ved å stenge ned nettverkene, fordi det vil være andre personer som overtar. Kontrolløren Kjetil er uttrykker dette på følgende måte:

> Ja, det er det som gjøres i stor grad nå. Du ser jo alle disse Europolprosjektene med fellesinnsats som rammer én etter én av disse markedsplassene. Men så åpnes jo nye igjen. Det er jo mange som har blitt stengt ned de senere årene, og jeg tror det bare forflytter seg. Du får jo tatt noen bakmenn da, men så lenge det er penger å tjene så vil det bare flytte seg liksom.

I dette sitatet forklarer informanten at nye aktører vil overta narkotikadistribusjonen på det mørke nettet så lenge det er penger for dem å tjene på det. Han ser det positive i at man får tatt noen bakmenn, men beretter videre at etter man har tatt ned noen markedsplasser vil nye oppstå. Det står skrevet i "EU Drug Markets Report" (EMCDDA, 2017, s. 62) at:

> Takedowns of darknet markets alone result in only short-term gains for law enforcement and that effective disruption strategies require a broad and more integrated approach to monitoring, intervention and investigation.

Myndighetene mener at det mørke nettet er veldig motstandsdyktig fordi administratorer, kjøpere og selgere raskt absorberer myndighetenes aksjoner om nedstenging av markedsplassene. Når myndighetene legger ned en stor markedsplass på det mørke nettet, vil narkotikahandel reduseres for en kort periode, men så vil selgere og kjøpere raskt finne alternative tilgjengelige markedsplasser eller det vil oppstå nye. Kontrolløren Peder forklarer dette på følgende måte: "Det blir som å hugge hodet av et troll, det vokser et nytt opp igjen ifølge eventyrene". Her sammenligner informanten kryptomarkedene med troll i eventyr, hvor myndighetene vil forsøke å hugge hodet av trollet, men det vokser bare opp igjen. På samme måte vil myndighetenes nedstenging av markedsplassene føre til at nye markedsplasser dukker opp istedenfor.

Administratorer på kryptomarkedene vil prøve å tilpasse seg myndighetenes kontroll ved å innføre regler på markedsplassene. Jeg har videre forklart at når myndighetene stenger ned store kryptomarkeder vil noen gå over til andre markedsplasser. Det er ikke alltid kjøpere og selgere velger å gå over til andre store markedsplasser, men noen velger heller å gå over til mindre og regionale kryptomarkeder:

> Samtidig så skaper det en trend som gjør det vanskeligere å kontrollere markedene. Først så hadde man store internasjonale markedsplasser som blant annet Silk Road,

> der hele verden var til stede. Det blir så stort at myndighetene må gjøre noe med det, og man tar de som står bak det, og man tar mange av selgerne og noen kunder. Så skapes det nye markeder og det var jo en voldsom oppblomstring etter Silk Road. Da kom det mange flere mindre markeder som kanskje var mer regionale. […] Som gjør at det blir mange flere markeder å holde følge med og det blir mer ressurskrevende for myndighetene å kontrollere det.

I dette utsagnet fra kontrolløren Peder kan det tolkes at utviklingen i flere regionale plattformer på det mørke nettet resulterer i mer ressurskrevende styring og overvåkning for myndighetene. I rapporten ”Internet Organised Crime Threat Assessment” (Europol, 2018, s. 10) står det at: ”The almost inevitable closure of large, global Darknet marketplaces has led to an increase in the number of smaller vendor shops and secondary markets catering to specific language groups or nationalities ”. Basert på analyse av dette utdraget, tolker jeg at en konsekvens av å stenge ned store globale markedsplasser på det mørke nettet, vil være en økning i mindre markedsplasser som spesifiserer seg på begrensede nasjonaliteter eller språk. Myndighetene har lagt ned de store markedsplassene gjennom internasjonale samarbeidsaksjoner. Når plattformene blir mer nasjonale vil det følgelig utføres færre slike internasjonale samarbeidsaksjoner. Dette er administratorene og selgerne på kryptomarkedene klar over, og derfor gjør de disse tilpasningene. Myndighetenes nedstenging av markedsplassene skulle være med på å forebygge og øke den opplevde oppdagelsesrisikoen knyttet til kryptomarkeder. Konsekvensen ved å gjøre det er heller at markedene blir mindre og mer regionale som videre fører til mer utfordrende overvåkning for myndighetene.

Nedstenging av store markedsplasser på det mørke nettet fører til flere regionale kryptomarkeder, og myndighetenes overvåkning blir mer utfordrende. En annen og mer utfordrende konsekvens fra myndighetenes ståsted er at flere går over til lukkede nettbutikker (EMCDDA, 2017). Myndighetenes samarbeidsaksjoner rettet mot store markedsplasser fører til en oppblomstring av sekundærmarkeder. Veletablerte leverandører på det mørke nettet som har stor tillit kan enkelt sette opp egne små nettbutikker og fortsette sine bedrifter med allerede etablerte kundemarkeder og selge til faste kjøpere (Europol, 2018). Kontrolløren Jan skisserer denne oppblomstringen av nettbutikker:

> Jeg tror vi kommer til å se en dreining mer og mer mot at det går bort ifra

> markedsplasser og at det blir mer selvstendig drevne type nettbutikker uavhengig av markedsplassene. Det er det som er trenden, og det er nok dit det kommer til å gå mer og mer mot, tenker jeg. […] Det blir mer salg én til én hvor de sender e-poster og kommuniserer på krypterte plattformer, og gjør oppgjør via kryptovaluta. Det gjør at dem skjermer seg mye mer enn de har gjort via markedsplassene.

Informanten tror at et resultat av at myndighetene stenger de store markedsplassene, er at flere går over til selvstendige drevne nettbutikker. Dette gjør at de skjermer seg mer for myndighetenes overvåkning. Basert på min analyse av rapporten "EU Drug Markets Report" (EMCDDA, 2019) forventer myndighetene en fragmentering på det mørke nettet. De tror at store markedsplasser muligens vil vedvare, men de regner samtidig med en økning i antall nettbutikker som drives av enkeltindivider. Videre kan det tolkes ut fra rapporten at myndighetene hevder at det vil være like ressurskrevende for dem å slå ned på disse små nettbutikkene som en stor markedsplass. Nedstenging av disse nettbutikkene vil gi dårligere resultat, noe som gjør det mindre sannsynlig at myndighetene vil slå ned på disse. Kontrolløren Peder forklarer nærmere hvordan disse små nettbutikkene vil være mer ressurskrevende for myndighetene:

> […] Noen selgere åpner egne sider der det kun er én selger, og da begynner det å bli så smått at det er for mye ressurser knyttet opp til vinninga ved å gjøre noe med det. Man har liksom sprengt de store, også har det blitt mange små satellitter med sider og selgere. Det siste fenomenet nå er at man har gått ned fra å selge på egen side til å bare selge via mail. Man er inne på et forum og skriver "på denne mailadressen her kan dere bestille, og her er lista over hva man selger". Det blir mindre og mindre og mindre. Det vil kanskje kreve like mye ressurser for å ta den lille som for hele den store. Nå er det tusenvis av små markeder som åpner, og det er den negative siden ved å legge ned de store nettverka. Det at du rett og slett eksploderer alt til å bli tusen biter, men det er fremdeles tusen små velfungerende biter. Du kan kanskje starte etterforskning mot en av dem, men de tretti andre får gå. Hadde du hatt alle samla på et sted så hadde du kanskje hatt bedre kontroll.

Fra dette sitatet kan det tolkes at informanten mener at nedstenging av de store markedsplassene vil føre til åpning av flere mindre nettbutikker som drives av enkeltpersoner. Denne konsekvensen gjør etterforskning for myndighetene mer krevende, og

de får tatt færre sammenlignet med hva de gjorde på de store markedsplassene. Myndighetene ville hatt bedre kontroll ved å ha alt samlet på ett sted. Kontrolløren Arne er generelt kritisk til myndighetenes nedstenging av de store markedsplassene:

> Jeg tror ikke at det er stor gevinst for myndighetene på lang sikt. Jeg er litt usikker på om det er veldig effektivt å skade tillit til nettstedene. Åpne marked er nyttig for oss for å bekjempe kriminalitet. Skal vi ødelegge vår største informasjonskilde som starter etterforskning? Det er en veldig kortsiktig gevinst med en langsiktig ulempe.

I dette utsagnet forteller informanten at fordelen ved å legge ned markedsplassene vil være kortvarig. Han mener at når myndighetene stenger ned store markedsplasser, ødelegger de samtidig for seg selv. Det mørke nettet er en stor informasjonskilde for myndighetene, og dersom nedstenging av markedsplassene fører til små nettbutikker, vil de miste den store informasjonskilden om narkotikadistribusjon og dette vil være deres langsiktige ulempe. Myndighetenes overvåkning og styring av det mørke nettet som skal forebygge samfunnsborgere til å gå på det mørke nettet for å kjøpe narkotika, kan samtidig være ødeleggende etterretningsmessig for myndighetene selv.

Myndighetenes nedstenging av markedsplassene er en form for både indirekte og direkte styring som aktivt brukes i internasjonale samarbeidsaksjoner på tvers av myndigheter. Denne styringen kan derfor kobles til governmentalityteori (Foucault, 1991). Å legge ned de største markedsplassene fungerer som direkte form for styring ved at myndighetene luker vekk de store markedsplassene, og på den måten disiplineres samfunnsborgerne til å ikke ha mulighet til å handle på disse kryptomarkedene (Garland, 1999). Flere av informantene mener at dette kan være en nyttig styringsmekanisme. Ikke bare fordi myndighetene setter narkotikaselgere tilbake og får samlet inn store mengder etterretningsinformasjon, men også fordi nedstengingene kan virke forebyggende på samfunnsborgerne. Nedstenging kan sammen med overvåkning også øke den følte oppdagelsesrisikoen, og på den måten disiplinere samfunnsborgerne til å disiplinere seg selv (Foucault, 1991).

Riktignok kan nedstenging av markedsplasser føre med seg negative konsekvenser, også fra myndighetenes ståsted. Dette gjør at kontrollørene er litt delte i meningene sine om hvor effektiv myndighetenes nedstenging av det mørke nettet er. Det har blitt vist i tidligere aksjoner mot kryptomarkedene at myndighetene både styrer og overvåker på det mørke

nettet. Dette vil kunne forklares med elementer av panoptisk overvåkning, hvor kjøpere og selgere av narkotika ikke er klar over hvor overvåket de blir av myndighetene (Foucault, 1979). Som et resultat av myndighetenes nedstenging av de store kryptomarkedene vil noen administratorer overvåke myndighetene for å finne ut hvilke markeder de prioriterer å stenge ned. Deres sousveillance vil føre til at de innfører egne regler på sine markedsplasser for å unngå å bli tatt ned av myndighetene.

En annen konsekvens av at myndighetene legger ned de store kryptomarkedene er at markedsplassene blir mindre og regionale. Dette vil kreve mer ressurser og fører til færre internasjonale samarbeid for å kunne ta de ned. Myndighetene har også sett at flere narkotikaselgere på det mørke nettet har satt opp egne nettsider eller selger fra kryptert e-post. For kontrollørene vil det være like ressurskrevende å overvåke disse små nettbutikkene som de store markedsplassene, men styringen av disse vil føre til adskillig dårligere resultat for myndighetene. Myndighetene forsøker å disiplinere sine borgere til å avstå fra narkotikadistribusjon på det mørke nettet basert på rasjonelle prinsipper (Neumann, 2003). Spørsmålet er om de skal fortsette å gjøre det til tross for at det er en ulempe for dem selv. Myndighetenes disiplin av administratorer, kjøpere og selgere på kryptomarkeder vil føre til at styring og overvåkning med formål om å forebygge og å øke den følte oppdagelsesrisikoen blir mer utfordrende i fremtiden. Overvåkningsprosessene på det mørke nettet, illustrert ved surveillant assemblage, vil hele tiden føre til mer overvåkning og styring fra alle hold.

6 Avslutning

"Vi kan være flue på veggen på narkotikamarkedet og det var jo utenkelig før […]"
"[…] Skal vi ødelegge vår største informasjonskilde som starter etterforskning? […]"

Begge disse utsagnene er fra intervjuet med kontrolløren Arne. I det første sitatet forteller han at det mørke nettet har gitt myndighetene en helt spesiell mulighet til å kunne overvåke narkotikahandel. I det andre sitatet viser informanten sin skepsis til å legge ned de store kryptomarkedene, for ved å gjøre det kan myndighetene selv påvirke sin egen fremtidige overvåkning og styring i negativ retning. Disse to sitatene uttrykker oppgavens hovedfokus, nemlig myndighetenes syn på narkotikadistribusjonen på det mørke nettet i lys av overvåkning, og hvordan myndighetenes overvåkningsmuligheter på bakgrunn av digitalisering kan bidra til å ødelegge overvåkning og styring i fremtiden.

Teknologi og digitalisering er i stadig endring, og denne oppgaven har utforsket kryptomarkeder som et aspekt ved den digitale utviklingen som påvirker myndighetenes overvåkning og styring. Flere forskere har de senere årene studert det mørke nettet (Décary-Hétu og Dupont, 2013; Martin, 2014; Barratt, Ferris og Winstock, 2014; Bakken og Bosnes, 2015; Tzanetakis m.fl., 2015; Bancroft og Reid, 2016; Broséus m.fl., 2016; Rhumorbarbe m.fl., 2016; Bakken, Møller, og Sandberg, 2017; Bancroft, 2017; Espinosa, 2019; Aldridge og Askew, 2017; Tzanetakis, 2018; Aldridge, 2019). Det foreligger riktignok lite forskning som ser narkotikadistribusjon på kryptomarkeder fra myndighetenes side. I denne oppgaven har jeg vist at det er viktig å forske på deres holdninger om dette temaet fordi det kan gi større innsikt i hva som ligger bak myndighetenes kriminalpolitikk som påvirker styring og overvåkning.

Myndighetenes synspunkter som denne oppgaven bygger på har empirisk forankring i kvalitativ metode. Kvalitativ forskningsmetode har vært hensiktsmessig å bruke til dette masterprosjektet fordi det har gjort det mulig å gå i dybden på de ulike holdningene myndighetene har til narkotikadistribusjonen på det mørke nettet. For å fremme de ulike nyansene av kontrollmyndighetenes meninger om narkotikadistribusjon på det mørke nettet, har denne avhandlingen kombinert kvalitative forskningsintervju og kvalitativ dokumentanalyse. Jeg har intervjuet seks myndighetspersoner som jobber med styring på det mørke nettet, og jeg har analysert offentlige rapporter som er publisert av Politidirektoratet

(2017), Oslo politidistrikt (2018), Europol (2018; 2019; 2020) og EMCDDA (2017; 2019). Jeg har valgt å triangulere transkripsjonene fra de kvalitative intervjuene og utdragene fra de offentlige rapportene til å analysere de samme problemstillingene.

På bakgrunn av det empiriske materialet, har min analyse illustrert myndighetenes nyanserte meninger, og at flere av kontrollørene også opplever en intern spenning i sine egne synspunkter knyttet til de ulike funksjonene ved krypterte nettverk. Et tema som har skapt ekstra spenning i myndighetenes synspunkter er anonymitet og kryptering på det mørke nettet. Jeg har blant annet vist i denne oppgaven at en typisk fremstilling av anonymiteten på det mørke nettet er et samfunnsdilemma med personvern og frihet på den ene siden og samfunnssikkerhet på den andre (Tzanetakis, 2017; Powell, Stratton og Cameron, 2018). Noen av kontrollørene mente i utgangspunktet at det mørke nettet hadde flere legale og positive funksjoner sett fra myndighetenes ståsted, mens andre mente at vi ikke har behov for krypterte nettverk fordi vi burde stå frem med hvem vi er slik vi må i livet utenfor internett. Min analyse viste derfor ingen tydelig og felles holdning blant myndighetspersonene knyttet til dette samfunnsdilemmaet, men jeg har likevel illustrert noen nyanser. Imidlertid er myndighetene nødt til å veie de to sidene opp mot hverandre når de skal prioritere sine ressurser rettet mot styring på det mørke nettet. For selv om krypterte nettverk har legale og positive funksjoner sett fra de norske og europeiske myndighetenes ståsted, mener de likevel at de kan rasjonalisere sin bruk av ressurser rettet mot styring på det mørke nettet med fokus på de som bruker kryptering for illegale hensikter.

Min analyse har presentert flere faktorer med det mørke nettet som myndighetene anser som utfordrende. Elementer ved det mørke nettet som de anser som bekymringsverdig kan være med på å uttrykke hvordan deres overvåkning på kryptomarkeder er rasjonalisert (Neumann, 2003). Når samfunn skal fordele sine kontrollressurser, utfører myndighetene vurderinger og beregninger basert på samfunnsborgernes risiko (Garland, 2013). Min oppgave har blant annet trukket frem tre faktorer som knyttes til samfunnsborgernes risiko ifølge myndighetene: Digital vold, økt tilgjengelighet av farlige narkotiske stoffer og andre samfunnsmessige konsekvenser som oppstår som følger av narkotikadistribusjonen på det mørke nettet. Min oppgave har vist at kontrollørene til en viss grad er enig i forskningen som konkluderer med at det mørke nettet fører til mindre fysisk vold, og anser dette som en positiv effekt (Barratt, Ferris og Winstock, 2016; Martin, 2018). Riktignok trekker de frem at man kan være både heldig og uheldig i forbindelse med narkotikadistribusjon uavhengig om det foregår på det

mørke nettet eller på tradisjonelle narkotikamarkeder. Dessuten har myndighetenes synspunkter vist at den teknologiske og digitale utviklingen har ført til at man kan bli utsatt for digital vold. På det mørke nettet kan digital vold innebære svindel, ID-tyveri og doxing (Martin, 2018). I oppgavens analyse har jeg videre illustrert hvordan digital vold på det mørke nettet også kan anses som fysisk vold, fordi et offer for misbruk av digital data vil kunne føle dette fysisk i kroppen sin. Selv om det er vår digitale data, eller datadoubles som Haggerty og Ericson (2000) referer til, som utnyttes av andre vil vi kjenne på dette fysisk inni oss.

Et annet element jeg har diskutert i denne oppgaven er myndighetenes bekymring om den økte tilgjengeligheten av farlige og potente stofftyper på kryptomarkedene. Myndighetene trekker frem denne tilgjengeligheten som svært urovekkende, både fordi det mørke nettet gjør det enklere å få tak i farlige narkotiske stoffer man sjeldent ser på det tradisjonelle narkotikamarkedet, men også fordi kryptomarkedene skaper nye brukergrupper. Min analyse har vist at myndighetene mener at narkotika blir mer tilgjengelig for personer som muligens ikke ville hatt samme tilgang i miljøet på det tradisjonelle markedet. Jeg har også vist at det mørke nettet kan skape en ny gruppe av narkotikaselgere. De som vanligvis selger narkotika på det tradisjonelle narkotikamarkedet kan som regel betraktes som ressurssvake personer, men på det mørke nettet er det ofte ressurssterke personer som står bak narkotikasalgene. Selv om vold og tilgjengelighet av farlige narkotiske stoffer er viktige faktorer til hvorfor myndighetene skal styre og overvåke på det mørke nettet, er det imidlertid de andre samfunnsmessige konsekvensene som følger med narkotikadistribusjonen på kryptomarkeder som myndighetene mener er det mest urovekkende. Myndighetene er mest bekymret over koblingen mellom narkotikadistribusjon på det mørke nettet og organiserte kriminelle gjenger, og de organisasjonene som myndighetene frykter mest er terrororganisasjoner. Myndighetene bruker ressurser på styring og overvåkning på det mørke nettet, og de gjør det med formål om å beskytte samfunnsborgerne.

I og med at myndighetene anser det mørke nettets eksistens som bekymringsverdig, mener de at de er nødt til å være til stede og overvåke der. Med utgangspunkt i min analyse, argumenterer jeg for at myndighetenes meninger om kryptomarkeder kan påvirke deres styring og overvåkning. Jeg har videre i oppgaven vist at dette fører til mange overvåkningsdynamikker på kryptomarkedene, og forklart at disse også kan være med på å påvirke deres styring. Derfor har jeg som en del av analysen, presentert en kartlegging av

overvåkningsdynamikkene på det mørke nettet. Myndighetenes overvåkning på krypterte nettverk har aspekter av panoptisk tilnærming (Foucault, 1979). Det vil si at kjøpere og selgere av narkotika på kryptomarkedene er klar over myndighetenes overvåkning, men de vet ikke når overvåkningen er rettet mot dem. Jeg har videre begrunnet at dette fører til at de disiplineres til å iverksette ekstra tiltak for å motsette seg myndighetenes overvåkning. Tiltakene baserer seg på informasjon fra deres overvåkning av myndighetene. På bakgrunn av dette kom jeg frem til at den panoptiske modellen ikke var en tilstrekkelig modell til å forklare overvåkningsprosessene på det mørke nettet, og jeg valgte å supplere med andre overvåkningsperspektiver. At administratorer, kjøpere og selgere på kryptomarkedene overvåker myndighetene, kan illustreres med synoptikon, en modell som beskriver at mange overvåker få (Mathiesen, 1997). Videre har jeg uttrykt deres iverksetting av ekstra tiltak for å gjøre overvåkning og styring mer utfordrende for myndighetene som overvåkning nedenfra og opp, som kan beskrives som sousveillance (Mann og Ferenbok, 2013). Min analyse har forklart hvordan dette videre vil disiplinere myndighetene til å også bedre sin teknologiske kompetanse.

Det er ikke bare en gjensidig overvåkning mellom myndighetene og administratorer, kjøpere og selgere på det mørke nettet. Jeg har også presentert en annen overvåkningsdynamikk, nemlig lateral overvåkning (Andrejevic, 2005). Tilbakemeldingsfunksjonen på kryptomarkedene gjør at kjøpere og selgere overvåker hverandre. Denne markedsføringsmekanismen fungerer som en overvåkningsanordning, hvor kjøpere kan overvåke selgere, og basert på dette kan de velge å handle av de som har fått gode tilbakemeldinger fra tidligere kjøpere. Markedsplassene på det mørke nettet er helt avhengig av denne overvåkningsprosessen. Den laterale overvåkningen vil eksempelvis disiplinere selgere til å passe på at det de selger er av bra kvalitet slik at de aktivt bedrer sitt internettomdømme for senere salg (Andrejevic, 2005; Espinosa, 2019). Likevel er tilbakemeldingsfunksjonene ikke alltid til å stole på, og ifølge informantene finnes det flere eksempler på tilfeller hvor disse manipuleres.

På bakgrunn av alle disse dynamikkene, kan overvåkningen på det mørke nettet anses for å være flytende (Lyon og Bauman, 2013). Overvåkningen på kryptomarkedene foregår fra flere kanter og i ulike retninger, og jeg har i min avhandling derfor hevdet at det ligner mer en surveillant assemblage som viser mer konkret hvordan og av hvem kryptomarkeder styres (Haggerty og Ericson, 2000). Surveillant assemblage gir en bedre forståelse av at det er flere

enn myndighetspersoner som overvåker på det mørke nettet. At det foregår overvåkning på krypterte nettverk er det ingen tvil om, og basert på min kartlegging av overvåkningsdynamikkene på det mørke nettet mener jeg at det mørke nettet ikke er så ”mørkt”. Krypterte nettverk er åpne for alle som har nok teknologisk kompetanse til å kunne ta seg inn, og det foregår overvåkning i alle retninger selv om de har en kryptert form. Krypterte nettverksplattformer forsøker å legge til rette for anonymitet, men gjentatte ganger innfris ikke dette. Hvis man ønsker å handle narkotika på det mørke nettet innebærer det en risiko for å kunne bli identifisert av myndighetene.

Dette fører videre til min anvendelse av Haggerty og Ericsons (2000) datadoubles. Lyon (2007) mener at med datadoubles skilles vi fra vår egen kropp til små biter av informasjon om oss på internett. Egenskapene med digital data er at det kan spores og lagres (Kaufmann og Jeandesboz, 2017). Jeg har forklart at det er dette som er grunnlaget for at overvåkning på kryptomarkeder er mulig, og på bakgrunn av dette har jeg videre vist at sporbarheten til disse digitale bitene gjør at myndighetene kan identifisere hvem personene bak disse dataene er. Derfor har jeg konkludert med at datadoubles ikke er så abstrakt som det tidligere har blitt fremstilt, men de kan derimot føres tilbake til en persons fysiske kropp.

I min analyse har jeg forklart at myndighetene styrer og overvåker på det mørke nettet med formål om å beskytte samfunnsborgerne, og med hovedfokus på å forebygge at personer entrer krypterte markedsplasser. Forebygging har fått et større fokus når myndighetene skal møte sine utfordringer knyttet til kriminalitet (Lomell, 2012). For å gjøre dette på det mørke nettet mener kontrollørene at myndighetene er nødt til å øke den følte oppdagelsesrisikoen og disiplineringen. Jeg har vist at dette kan kobles til governmentalityteori, hvor et av hovedprinsippene er at samfunnsborgerne er ansvarlig for egne valg, men myndighetene skal gjøre det de kan for at samfunnsborgerne disiplineres til å ta de riktige valgene (Foucault, 1991). Frem til i dag har myndighetene hovedsakelig basert sitt forebyggende arbeid på det mørke nettet ved å avskrekke gjennom å straffe administratorer og selgere på kryptomarkeder. Noen av kontrollørene mener at dette kan påvirke folk til å avstå fra narkotikamarkedet på det mørke nettet, fordi de ser at myndighetene er til stede, mens andre mener at myndighetene også må rette søkelyset mot kjøperne på kryptomarkeder for å oppnå en større forebyggende effekt.

En form for styring som myndighetene foretar seg på det mørke nettet med forebyggende formål, er å stenge ned de store krypterte markedsplassene. Ved å gjøre dette vil de først og fremst disiplinere direkte ved å fjerne muligheten samfunnsborgerne har til å handle narkotika på disse markedsplassene (Foucault, 1991). Samtidig vil nedstenging av store kryptomarkeder øke den opplevde oppdagelsesrisikoen, og ifølge myndighetene også være en indirekte form for styring med mål om å forebygge (Garland, 1999). Riktignok kan nedstenging av markedsplasser føre med seg negative konsekvenser for myndighetene. Derfor er kontrollørene litt delte i meningene sine om hvor effektivt myndighetenes nedstenging av det mørke nettet er. For som kontrolløren Arne uttrykte i sitatene innledningsvis i dette avslutningskapittelet, kan myndighetenes nedstenging av markedsplasser ha negative konsekvenser for deres fremtidige styring og overvåkning. Som et resultat av myndighetenes nedstenging av de store kryptomarkedene vil noen administratorer overvåke myndighetene for å blant annet finne ut hvilke markeder de prioriterer å stenge ned. Dette har ført til mange har endret markedsplassene til å bli mindre og regionale, noe som vil kreve mer ressurser og føre til færre internasjonale samarbeid for myndighetene. Myndighetene har også sett at flere selgere av narkotika på det mørke nettet har satt opp egne nettsider eller selger fra kryptert e-post. For kontrollørene vil det være like ressurskrevende å overvåke disse små nettbutikkene som de store markedsplassene, men styringen av disse vil føre til adskillig dårligere resultat. Basert på min analyse av dette har jeg kommet frem til at myndighetenes disiplin av administratorer, kjøpere og selgere på kryptomarkeder kan føre til at styring og overvåkning med formål om å forebygge og å øke den følte oppdagelsesrisikoen blir mer utfordrende i fremtiden.

Overvåkningsprosessene på det mørke nettet vil hele tiden føre til mer overvåkning og styring fra alle hold. Min analyse har vist at både myndighetenes synspunkter og overvåkningsdynamikkene på det mørke nettet påvirker myndighetenes styring. Hvis teknologi og digitalisering er i stadig utvikling, gjelder dette også på de krypterte internettplattformene (Sunde og Sunde, 2019). Samtidig som teknologi utvikler seg, vil også overvåkningsdynamikker endre seg. Dette gjør at det mørke nettet er dynamisk og i stadig endring. De gjensidige overvåkningsdynamikkene og disiplinen gjør at det blir mer utfordrende for myndighetene å styre og overvåke narkotikadistribusjonen på internett i fremtiden. De mister også sin største informasjonskilde knyttet til narkotikadistribusjon ved å legge ned de store markedsplassene. Den raske utviklingen for digital narkotikadistribusjon må forskes videre på, for det som er relevant i dag er ikke nødvendigvis det i nær fremtid.

Det eneste som er sikkert er at overvåkingsprosessene og myndighetenes styring i dag vil påvirke myndighetenes fremtidige styring av narkotikadistribusjon på internett.

Antall ord i oppgaven: 38 648

Litteraturliste

Aas, K. F., Gundhus, H. O. og Lomell. H. M. (2009) Introduction: Technologies of (In)security, i Aas, K. F., Gundhus, H. O. og Lomell, H. M. (red.) *Technologies of (In)security: The Surveillance of Everyday Life*. Oxon: Routledge-Cavendish, s. 1-17.

Aldridge, J. (2019) Does online anonymity boost illegal market trading?, *Media, Culture & Society,* 41(4), s. 578-583.

Aldridge, J. og Askew, R. (2017) Delivery dilemmas: How drug cryptomarkets users identify and seek to reduce their risk of detection by law enforcement, *International Journal of Drug Policy,* 41(1), s. 101-109.

AlQahtani, A. og El-Alfy, E. M. (2015) Anonymous connections based on onion routing: A review and a visualization tool*, Procedia Computer Science,* 52(1), s. 121-128.

Andrejevic, M. (2005). The Work of Watching One Another: Lateral Surveillance, Risk, and Government, *Surveillance & Society,* 2(4), s. 479-497.

Andrejevic, M. og Gates, K. (2014) Big Data Surveillance: Introduction, *Surveillance & Society,* 12(2), s. 185-196.

Ashwort, A. og Zedner, L. (2014) *Preventive Justice.* Oxford: Oxford University Press.

Bakken, S. A., Møller, K. og Sandberg, S. (2017) Coordination problems in cryptomarkets: Changes in cooperation, competition and valuation, *European Journal of Criminology,* 15(4), s. 442-460.

Bakken, S. A. og Bosnes, H. (2015) *Narkotikamarkeder på det mørke nettet: En kvalitativ studie av Silk Road 2.0*. SIRUS rapport 7/2015. Oslo: Statens institutt for rusmiddelforskning.

Bakken, S. A. og Demant, J. J. (2019) Sellers´risk perceptions in public and private social media drug markets, *International Journal of Drug Policy,* 73(1), s. 255-262.

Bancroft, A. (2017) Responsible use to responible harm: Illicit drug use and peer harm reduction in a darknet cryptomarket, *Health, risk & society,* 19(1), s. 336-350.

Bancroft, A. (2019) *The Darknet and Smarter Crime: Methods for Investigating Criminal Entrepreneurs and the Illicit Drug Economy.* Cham: Springer International Publishing AG.

Bancroft, A. og Reid, P. S. (2016) Challenging the techno-politics of anonymity: The case of cryptomarket users, *Information, Communication & Society,* 20(4), s. 497-512.

Barratt, M., Ferris, J. og Winstock, A. R. (2014) Use the Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States, *Addiction*, 109(5), s. 774-783.

Barratt, M., Ferris, J. og Winstock, A. R. (2016) Safer scoring? Cryptomarkets, social supply and drug market violence, *International Journal of Drug Policy,* 35(1), s. 24-31.

Barratt, M. og Aldridge, J. (2016) Everything you always wanted to know about drug cryptomarkets (but were afraid to ask), *International Journal of Drug Policy,* 35(1), s. 1-6.

Bellanova, R. (2017) Digital, politics, and algorithms: Governing digital data through the lens of data protection, *European Journal of Social Theory,* 20(3), s. 329-347

Bennett. C. J. og Regan, M. (2004). Editorial: Surveillance and Mobilities, *Surveillance & Society* 1(4), s. 449-455.

Boyd, D. og K. Crawford (2012) Critial Questions for Big Data: Provocations for a cultural, technological and scholarly phenomenon, *Information, Communication and Society,* 15(5), s. 662-679.

Bratberg, Ø. (2018) *Tekstanalyse for samfunnsvitere.* 2. utg. Oslo: Cappelen Damm Akademisk.

Broséus, J., Rhumorbarbe, D., Mireault, C., Ouelette, V., Crispino, F. og Décary-Hétu, D. (2016) Studying illicit drug trafficking on Darknet markets: Structure and organisation from a Canadian perspective, *Forensic Science International,* 264(1), s. 7-14.

Bryman, A. (2012) *Social Research Methods*. 4. utg. Oxford: Oxford University Press.

Bukve, O. (2016) *Forstå, forklare, forandre: Om design av samfunnsvitenskaplege forskningsprosjekt.* Oslo: Universitetsforlaget.

Christie, N. (2000). *Kriminalitetskontroll som industri.* Oslo: Universitetsforlaget AS.

Creswell, J. W. og Poth, N. (2018) *Qualitative Inquiry and Research Design: Choosing Among Five Approaches.* 4. utg. London: SAGE.

Décary-Hétu, D. og Dupont, B. (2013) Reputation in a dark network of online criminals, *Global Crime,* 14(2-3), s. 175-196.

Dupont, B. (2008) Hacking the Panopticon: Distributed Online Surveillance and Resistance, i M. Deflem. (red.) *Surveillance and Governance 10: Sociology of Crime, Law and Deviance,* Esmerald Publishing, s.259-280.

EMCDDA (2016) *European Drug Report 2016: Trends and Developments,* European Monitoring Centre for Drugs and Drug Addiction-Europol Joint Publications, Luxemburg: Office of the European Union.

EMCDDA (2017) *Drugs and the darknet: Perspectives for enforcement research and policy,* European Monitoring Centre for Drugs and Drug Addiction-Europol Joint Publications, Luxemburg: Office of the European Union.

EMCDDA, (2019) *EU Drug Markets Report,* European Monitoring Centre for Drugs and Drug Addiction-Europol Joint Publications, Luxemburg: Office of the European Union.

Espinosa, R. (2019) Scamming and the reputation of drug dealers on Darknet Markets, *International Journal of Industrial Organization,* 67(1), s. 1-26.

Europol (2017) *Internet Organised Crime Threat Assessment* (IOCTA, 2017). Tilgjengelig fra: https://www.europol.europa.eu/iocta/2017/index.html (Hentet: 11.06.2020).

Europol (2018) *Internet Organised Crime Threat Assessment* (IOCTA, 2018). Tilgjengelig fra: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018 (Hentet: 11.06.2020).

Europol (2019) *Internet Organised Crime Threat Assessment* (IOCTA, 2019). Tilgjengelig fra: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019 (Hentet 08.06.2020).

Europol (2020) *Internet Organised Crime Threat Assessment* (IOCTA, 2020). Tilgjengelig fra: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020 (Hentet: 11.10.2020).

Fangen, K. (2004) *Deltagende observasjon.* 2. utg. Oslo: Fagbokforlaget.

Fangen, K. (2011) Deltagende observasjon, i Fangen, K. og Sellerberg, A.-M. (red.) *Mange ulike metoder.* Oslo: Gyldendal Akademisk, s. 37-56.

Finstad, L. (2006) Politisosiologi, i Finstad, L. og Høigård, C. (red.) *Straff og rett.* Oslo: Pax Forlag, s. 49-95.

Foucault, M. (1979) *Discipline and Punish: The Birth of the Prison.* New York: Vintage Books.

Foucault, M. (1991) Governmentality, i Burchell, G., Gordon, C., Miller, P. (red.) *The Foucault Effect: Studies in Governmentality.* Chicago: Chicago University Press, s. 87-104.

Garland, David (1999): 'Governmentality' and the Problem of Crime, i Smandych, R. (red.) *Governable Places: Readings on Governmentality and Crime Control*. Aldershot: Ashgate, s. 15-45.

Garland, D. (2013) Penality and the Penal State, *Criminology,* 51(3), s. 475-516.

Haggerty, K. og Ericson, R. V. (2000) The Surveillant Assemblage, *Journal of Sociology,* 51(4), s. 605-622.

Halvorsen, Knut (2008) *Å forske på samfunnet: En innføring i samfunnsvitenskapelig metode*. 5.utg. Oslo: Cappelen Damm Akademisk.

Kalleberg, R., Malnes, R. og Engelstad, F. (2009) *Samfunnsvitenskapenes oppgaver, arbeidsmåter og grunnlagsproblemer.* 2. utg. Oslo: Gyldendal Akademisk.

Kaufmann, M. og Jeandesboz, J. (2016) Politics and 'the Digital': From Singularity to Specificity, *European Journal of Social Theory,* 20(3), s. 309-328.

Kripos, (2017) *Dom i Kripos første etterforskning på det mørke nettet*. Tilgjengelig fra: https://www.politiet.no/aktuelt-tall-og-fakta/aktuelt/nyheter/2017/11/15/dom-i-kripos-forste-etterforskning-pa-det-morke-nettet/ (Hentet: 02.08.2020).

Kvale, S. og Brinkmann, S. (2019) *Det kvalitative forskningsintervju.* 3. utg. Oslo: Gyldendal

Lacson, W. og Jones, B. (2016) The 21st Century Darknet Market: Lessons from the Fall of Silk Road, *International Journal of Cyber Criminology,* 10(1), s. 40-61.

Letvik, H. (2017) 15-åring funnet død på gutterommet i Oslo – hadde tatt syntetisk dop, *Aftenposten,* 19. april. Tilgjengelig fra: https://www.aftenposten.no/norge/i/5XEm6/15-aring-funnet-dod-pa-gutterommet-i-Oslo--hadde-tatt-syntetisk-dop (Hentet: 08.05.2020).

Lindgren, S. (2011) Tekstanalyse, i Sellerberg, A.-M. og Fangen, K. (red.) *Mange ulike metoder.* Oslo: Gyldendal Akademisk, s. 266-279.

Lomell, H. M. (2012) Punishing the uncommitted crime: Prevention, pre-emption, precaution and the transformation of criminal law, i Hudson, B. og Ugelvik, S. (red.) *Justice and Security in the 21st Century: Risks, rights and the rule of law.* London: Routledge, s. 83-100.

Lupton, D. (2015) Theorising Digital Society, i Lupton, D. (red.) *Digital Sociology.* London/New York: Routledge, s. 20-41.

Lyon, D. (2007) *Surveillance Studies: An Overview.* Cambridge: Polity.

Lyon, D., Haggerty, K. D. og Ball, K. (2012) Introducing Surveillance Studies, i Lyon, D., Haggerty, K. D. og Ball, K. (red.) *Routledge Handbook of Surveillance Studies.* Abingdon/Oxon: Routledge, s. 1-11.

Lyon, D. og Bauman, Z. (2013) Introduction, i Lyon, D. og Bauman, Z. (red.) *Liquid Surveillance*. Cambridge: Polity, s. 1-17.

Mann. S. og Ferenbok, J. (2013) New Media and the Power Politics of Sousveillance in a Surveillance-Dominated World, *Surveillance & Society,* 11(1/2), s. 18-34.

Martin, J. (2014) Lost on the Silk Road: Online drug distribution and the 'cryptomarket', *Criminology & Criminal Justice,* 14(3), s. 351-367.

Martin, J. (2018) Cryptomarkets, systemic violence and the 'gentrification hypothesis'. *Addiciton,* 113(5), s. 797-798.

Martin, A. K., van Brakel R. E. og Bernhard, D. J. (2009) Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework, *Surveillance & Society,* 6(3), s. 213-232.

Masson, K. og Bancroft, A. (2018) 'Nice people doing shady things': Drugs and the morality of exchange in the darknet cryptomarkets, *International Journal of Drug Polity,* 58(2018), s. 78-84.

Materstvedt, L. J. (2018) *Vitenskap, etikk og politikk.* Oslo: Fagbokforlaget.

Mathiesen, T. (1997) The Viewer Society: Michel Foucault´s `Panopticon´ Revisited, *Theoretical Criminology,* 1(2), s. 215-234.

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).

Mehta, M. D. og Darier, E. (1998) Virtual Control and Disciplining on the Internet: Electronic Governmentality in the New Wired World, *The Information Society,* 14(2), s. 107-116.

Mirea, M., Wang, V. og Jung, J. (2019) The not so dark side of the darknet: a qualitative study, *Security Journal,* 32(2), s. 102-118.

Mörch, C.-M., Côte, L.-P., Corthésy-Blondin, L., Plourde-Léveillé L., Dargis, L. og Mishara, B. L. (2018) The Darknet and suicide, *Journal of Affective Disorders,* 241(1), s. 127-132.

Narko på Dark Web (2020) *Insider,* sesong 9, episode 8. Tilgjengelig fra Dplay (Lastet ned: 10.03.2020).

NESH (2016). *Forskningsetiske retningslinjer for samfunnsvitenskap, humaniora, juss og teologi.* Tilgjengelig fra: https://www.etikkom.no/forskningsetiske-retningslinjer/Samfunnsvitenskap-jus-og-humaniora/innledning-formal/ (Hentet: 29.03.2020).

Neumann, I. B. (2003) Innledning: Regjeringsbegreper og regjeringens historiske fremvekst, i Neumann, I. B. og Sending, O. J. (red.) *Regjering i Norge.* Oslo: Pax Forlag, s. 9-43.

Oslo politidistrikt (2018) *Trender i kriminalitet 2018-2021: Digitale og glokale utfordringer.* Tilgjengelig fra: https://kriminalitetsforebygging.no/dokument/trender-i-kriminalitet-2018-2021-digitale-og-globale-utfordringer/ (Hentet: 08.06.2020).

Pergolizzi, J. V., Leguang, J. A., Taylor, R. og Raffa, R. B. (2017) The ”Darknet”: The new street for street drugs, *Journal of Clinical Pharmacy and Therapeutics,* 42(6), s. 790-792.

Politidirektoratet (2017) *Trusler og utfordringer innen IKT-kriminalitet (2017).* Tilgjengelig fra: https://www.politiet.no/globalassets/dokumenter/pod/ikt_krim_pod.pdf (Hentet: 08.06.2020).

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

Regjeringen (2018) *Ny personopplysningslov og EUs personvernforordning.* Tilgjengelig fra: https://www.regjeringen.no/no/tema/lov-og-rett/innsikt/ny-personopplysningslov/id2592984/ (Hentet: 08.05.2020).

Repstad, P. (1987) *Mellom nærhet og distanse: Kvalitative metoder i samfunnsfag*. Oslo: Universitetsforlaget.

Rhumorbarbe, D., Staehli, L., Broséus, J., Rossy, Q. og Esseiva, P. (2016) Buying drugs on a Darknet market: A better deal? Studying the online illicit drug market through the analysis of digital, physical and chemical data, *Forensic Science International*, 267(1), s. 173-182.

Rose, N., O´Malley, P. og Valverde, M. (2006) Governmentality, The *Annual Reviews of Law and Social Science,* 2(1), s. 83-104.

Salter. M. (2010) Surveillance, i Burgess, P. J. (red.) *The Routledge Handbook of New Security Studies.* London/New York: Routledge, s. 187-196.

Sellerberg, A.-M. og Fangen, K. (2011) Innledning, i Sellerberg, A.-M. og Fangen, K. (red.) *Mange ulike metoder*. Oslo: Gyldendal Akademisk, s. 11-13.

Skardhamar, T. og Klemsdal, L. (2019) Digitalisering – en introduksjon, *Norsk sosiologisk tidsskrift,* 3(3), s. 169-172.

Sollund, R. (2007) *Tatt for en annen: En feltstudie av relasjonen mellom etniske minoriteter og politiet.* Oslo: Gyldendal akademisk.

Sunde, I. M. og Sunde, N. (2019) *Det digitale er et hurtigtog!: Vitenskapelige perspektiver på politiarbeid, digitalisering og teknologi.* Bergen: Fagbokforlaget.

Taddicken, M. (2014) The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure, *Journal of Computer-Mediated Communication,* 19(2), s. 248-273.

Thagaard, T. (2011) *Systematikk og innlevelse: En innføring i kvalitativ metode.* 3. utg. Bergen: Fagbokforlaget Vigmostad & Bjørke AS.

Tjora, A. (2017) *Kvalitative forskningsmetoder i praksis.* 3. utg. Oslo: Gyldendal akademisk.

Trædal, (2018) *Nå er Oslo-politiets nettpatrulje til stede i tre sosiale medier: Inntar Snapchat, Instagram og Facebook.* Tilgjengelig fra: https://www.politiforum.no/nettpatruljen-oslo-polidistrikt-sosiale-medier/na-er-oslo-politiets-nettpatrulje-til-stede-i-tre-sosiale-medier/147550 (Hentet: 11.11.2010).

Tzanetakis, M. (2017) The darknet´s anonymity dilemma, *Encore. The Annual Magazine on Internet and Society Research,* s. 118-125.

Tzanetakis, M. (2018) Comparing cryptomarkets for drugs: A characterisation of sellers and buyers over time, *International Journal of Drug Policy,* 56(1), s. 176-186.

Tzanetakis, M., Kamphausen, G., Werse, B og Von Laufenberg, R. (2015) The transparency paradox: Building trust, resolving disputes and optimising logistics on conventional and online drug markets. *International Journal of Drug Policy,* 35(1), s. 58-68.

Ulseth, T., Bothner-By, H. og Nordal, O. (2019) IP-adresse, i *Store norske leksikon.* Tilgjengelig fra: https://snl.no/IP-adresse (Hentet: 10.09.2020).

UNDOC (2019) *World Drug Report 2019.* Wien: United Nations Office on Drugs and Crime.

Vikan, J. A. (2014) Silkeveiene, *Adresseavisa,* 5. november. Tilgjengelig fra: https://www.adressa.no/pluss/2014/11/05/Silkeveiene-10313897.ece (Hentet: 14.09.2020).

Vikan, J. A. (2015) Teppefall, *Adresseavisa,* 18. juni. Tilgjengelig fra: https://www.adressa.no/pluss/magasin/2015/06/18/Teppefall-11219093.ece (Hentet: 14.09.2020).

VPN (2020) i *Store norske leksikon.* Tilgjengelig fra: https://snl.no/VPN (Hentet: 10.09.2020).

Walby, K. T. (2005) Institutional Ethnography and Surveillance Studies: An Outline for Inquiry, *Surveillance and Society,* 3(2/3), s. 158-172.

Vedlegg 1: Informasjonsskriv

Prosjektets tittel: Narkotikabekjempelse på det mørke nettet

Studier av det mørke nettet er relativt nytt i akademia og offentlige rapporter etterlyser mer forskning på temaet. Narkotikadistribusjon på det mørke nettet har ført til nye utfordringer sammenlignet med tradisjonell narkotikahandel. Temaet er komplekst og kan ses fra mange ulike vinkler. Dette er et masterprosjekt som ønsker å se narkotikabekjempelse på det mørke nettet fra kontrollmyndighetenes ståsted.

Mitt navn er Cecilie Nyhus og jeg studerer for en mastergrad i kriminologi på institutt for kriminologi og rettssosiologi på Universitetet i Oslo. Våren og høsten 2020 skal jeg forske på temaet narkotikadistribusjon og narkotikabekjempelse på det mørke nettet. Dette skrivet vil gi informasjon om målene for prosjektet og hva en deltakelse i prosjektet vil innebære. Institutt for kriminologi og rettssosiologi ved juridisk fakultet på Universitetet i Oslo er ansvarlig for masterprosjektet.

Formål

Forskningsprosjektets formål er å undersøke hva slags syn ansatte i Tolletaten og Politiet som jobber med kontroll av narkotikadistribusjonen på det mørke nettet har på denne formen for markedskriminalitet. Spørsmålet som masteroppgaven skal besvare er ”*Hvordan forstår kontrollmyndighetene i Norge narkotikadistribusjon på det mørke nettet?”*

Hvorfor får du spørsmål om å delta?

Temaet om det mørke nettet er komplekst og det finnes mange forskjellige diskurser som kan belyses. Dette masterprosjektet ønsker å se på temaet fra det de norske kontrollmyndighetenes ståsted. Det kan være interessant å se om denne diskursen skiller seg fra andre på for eksempel samfunnsmessig- eller internasjonalt nivå. Du får spørsmål om å delta i dette masterprosjektet da din arbeidsoppgave i toll/politi innebærer kontroll av narkotikadistribusjon på det mørke nettet. For å belyse masterprosjektets tema om det mørke nettet og besvare forskningsspørsmålet vil din deltakelse være veldig relevant. Din deltakelse vil bidra til å øke belysningen av og forskning på temaet om det mørke nettet.

Hva innebærer det for deg å delta?

Hvis du velger å delta i prosjektet innebærer det at du stiller til et intervju. Intervjuet er beregnet til å vare mellom 30-60 minutter og vil bli tatt opp med en båndopptaker. Dette masterprosjektet vil ikke være ute etter taushetsbelagt informasjon.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykke tilbake uten å oppgi noen grunn. Alle opplysninger om deg vil bli anonymisert. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Dine opplysninger vil bare brukes til formålene beskrevet i dette skrivet. Opplysningene dine vil bli behandlet konfidensielt og i samsvar med personvernregelverket. Navnet og kontaktopplysningene dine vil erstattes med en kode som lagres på egen navneliste adskilt fra øvrige data. Kontaktopplysninger og navneliste vil lagres på datamaskin som er tilknyttet Universitetet i Oslo med brukertilgang som krever passord. Båndopptaker vil sikres i et låsbart skap på Universitetet i Oslo som bare jeg, masterstudent Cecilie Nyhus, har tilgang til. Du vil ikke bli gjenkjent i publikasjon.

Hva skjer med opplysningene dine når masterprosjektet avslutter?

Prosjektet skal etter planen avsluttes november 2020. Ved prosjektslutt vil kontaktinformasjon, navneliste og opptak på båndopptaker makuleres. Informasjon som fremkommer i intervju vil bli anonymisert.

Dine rettigheter

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

- Innsyn i hvilke personopplysninger som er registrert om deg
- Få rettet personopplysninger om deg
- Få slettet personopplysninger om deg
- Få utlevert kopi av dine personopplysninger (dataportabilitet)
- Å sende klage til personvernombudet eller 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 ved Universitetet i Oslo har NSD, Norsk senter for forskningsdata AS, vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan du finne ut mer?

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

- Masterstudent Cecilie Nyhus på e-post Cecilie.Nyhus@student.jus.uio.no og telefon 95 14 81 04 eller veileder Mareile Kaufmann på e-post Mareile.Kaufmann@jus.uio.no og telefon 22 85 01 22 ved institutt for kriminologi og rettssosiologi.
- Universitetet i Oslo sitt personvernombud Roger Markgraf-Bye på personvernombud@uio.no.
- NSD – Norsk senter for forskningsdata AS, på e-post personverntjenester@nsd.no eller telefon: 55 58 21 17.

Med vennlig hilsen

Student Cecilie Nyhus

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *"Narkotikabekjempelse på det mørke nettet"* og har fått anledning til å stille spørsmål. Jeg samtykker til å delta i intervju i dette masterprosjektet.

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, ca. november 2020.

(Signatur, dato, sted)

Vedlegg 2: Intervjuguide

Samtykkeerklæring

Har du lest informasjonsskrivet jeg har sendt deg?

Har du forstått informasjonen som fremkommer i informasjonsskrivet om dette masterprosjektet?

Har du noen spørsmål til masterprosjektet?

Samtykker du til å delta i dette masterprosjektet?

Samtykker du til at opplysningene dine behandles frem til prosjektets slutt i november 2020?

Innledning

Kan du tenke deg hvorfor jeg intervjuer deg?

Har du gjort noen forberedelser i forkant av intervjuet?

Hvor lenge har du vært ansatt i toll/politi?

Hvor lenge har du arbeidet med det mørke nettet?

Hvordan er det å jobbe som toller/politi på det mørke nettet?

Hvordan tenker du at denne jobben er annerledes enn å jobbe operativt ute?

Generelt syn på narkotikadistribusjon på det mørke nettet

Hva ville du sagt til en ungdom som tenker å bestille narkotika på det mørke nettet?

Hva anser du som ulemper med at mange unge kjøper og selger narkotika på det mørke nettet? Eventuelt fordeler?

Hva er dine tanker rundt tilgjengeligheten av narkotiske stoffer, og da spesielt tilgjengeligheten av NPS (nye psykoaktive stoffer) på det mørke nettet?

Syn på nye forskningsfunn rundt narkotikadistribusjon på det mørke nettet

På det mørke nettet er selgerne avhengig av gode tilbakemeldinger fra kjøperne for senere salg. På hvilken måte kan dette være positivt?

Forskning på det mørke nettet viser at narkotikadistribusjon på det mørke nettet har lavere risiko for vold sammenlignet med tradisjonell narkotikadistribusjon. Hva er dine tanker rundt dette?

Sett bort ifra narkotikadistribusjon og annen kriminalitet, er det ting du tenker det mørke nettet kan brukes til som er positivt?

Krypterte nettverk åpnes og stenges hele tiden. Hva tenker du om bekjempelse av det mørke nettet ved å legge ned nettverkene?

Overvåkning

Hvorfor er det viktig å ha tjenestepersoner til å jobbe med narkotikadistribusjonen på det mørke nettet?

Hva er dine tanker om kjøp og salg av narkotika på det mørke nettet sammenlignet med gaten?

Hvordan tenker du kontrollen over det mørke nettet skiller seg fra kontrollen av den mer tradisjonelle narkotikahandelen?

Hvordan tenker du internkontrollen blant brukerne på det mørke nettet skiller seg fra internkontrollen selgere og kjøpere har på gata?

Korona

Har du lagt merke til om det har oppstått noe forskjell i markedene på det mørke nettet nå etter koronaen kom? I og med at grensene har blitt stengt.

Avslutning

Har du noe du lurer på eller ønsker å tilføye?

Vedlegg 3: Godkjennelse fra NSD

NSD NORSK SENTER FOR FORSKNINGSDATA

NSD sin vurdering

Prosjekttittel

Narkotikabekjempelse på darknet

Referansenummer

879951

Registrert

18.12.2019 av Cecilie Nyhus - cecilnyh@uio.no

Behandlingsansvarlig institusjon

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

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)

Mareile Kaufmann, Mareile.Kaufmann@jus.uio.no, tlf: 22850122

Type prosjekt

Studentprosjekt, masterstudium

Kontaktinformasjon, student

Cecilie Nyhus, Cecilie.Nyhus@student.jus.uio.no, tlf: 95148104

Prosjektperiode

02.01.2020 - 30.11.2020

Status

29.01.2020 - Vurdert

Vurdering (1)

29.01.2020 - 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 29.01.2020 med vedlegg, 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 30.11.2020.

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.

TAUSHETSPLIKT
Informantene i prosjektet har taushetsplikt. Det er viktig at intervjuene gjennomføres slik at det ikke samles inn opplysninger som kan identifisere enkeltpersoner eller avsløre annen taushetsbelagt informasjon.

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.

Lykke til med prosjektet!

Kontaktperson hos NSD: Kajsa Amundsen
Tlf. Personvernтjenester: 55 58 21 17 (tast 1)