Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

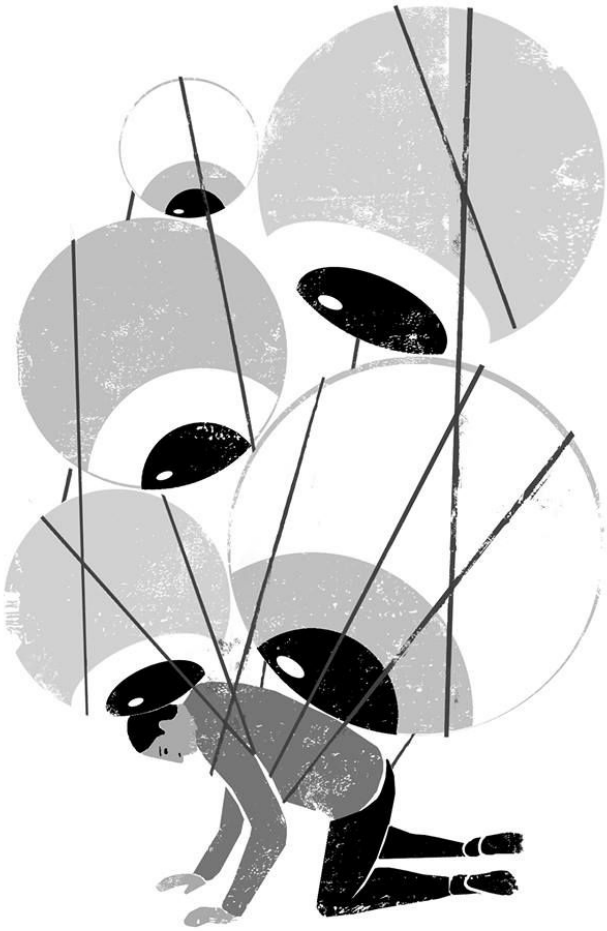
MASTEROPPGAVE

Studieprogram/spesialisering: Master i samfunnssikkerhet	Vårsemesteret, 2021 Åpen
Forfatter: Katharina Hay Risanger	
Fagansvarlig: Claudia Morsut **Veileder:** Claudia Morsut	
Tittel på masteroppgaven: En historisk studie av utviklingen til overvåking og personvern **Engelsk tittel:** A historical study of the evolution of surveillance and privacy	
Studiepoeng: 30	
Emneord: Overvåking, utviklingstrekk, personvern, sikkerhetstiltak, terrorisme, governmentality, risiko, risikobilde, samfunnssikkerhet, statssikkerhet, menneskerettigheter, demokrati	**Sidetall:** 81 + **vedlegg/annet**: 105 Stavanger, 14. juni 2021

Forside for masteroppgaven

Det teknisk-naturvitenskapelige fakultet

En historisk studie av utviklingen til overvåking og personvern



Masteroppgave i samfunnssikkerhet

Universitetet i Stavanger

Juni 2021

Katharina Hay Risanger

Det er et moderne paradoks at vi stadig og med åpne øyne, hamrer løs på grunnmuren, for å sikre huset vi lever i.

- Marie Simonsen, *Dagbladet*

Forsideillustrasjon hentet fra
https://www.nytimes.com/2011/09/13/opinion/protect-our-right-to-anonymity.html?_r=2&hp=

Forord

Denne oppgaven markerer slutten på to fantastiske år som student hos Universitetet i Stavanger. Gjennom masterstudiet i samfunnssikkerhet og kunnskapene jeg har tilegnet meg i denne perioden, har jeg hatt mulighet til å utforske et tema jeg har funnet svært fascinerende over lengre tid. Disse årene har forberedt meg på fremtiden og jeg ser frem til å begi meg ut på neste utfordring!

Jeg vil gjerne takke alle menneskene rundt meg som har bidratt til å forme denne oppgaven. Takk for alle gode innspill og diskusjoner. Bidrag fra dere har gjort denne oppgaven gjennomførbar.

Tusen takk til min veileder, førsteamanuensis Claudia Morsut. Takk for alle innspill og tilbakemeldinger, og for all støtte. Du har pushet en tidvis meget stresset student gjennom krevende perioder. Dette har jeg satt stor pris på.

Jeg vil også rette en stor takk til alle mine venner her i Stavanger som har gjort livet fantastisk de siste årene. Sist, men ikke minst, vil jeg takke min familie. Dere har alltid troen på meg, og dette er jeg uendelig takknemlig for.

Katharina Hay Risanger, 9. juni 2021

Sammendrag

Den teknologiske utviklingen i samfunnet og den verdensomspennende globaliseringen har påvirket de aller fleste samfunnsområder, både på godt og på vondt. I tillegg til å effektivisere og forenkle hverdagen, medfører også utviklingen nye sårbarheter og trusler mot samfunnet. Nye former for terrorisme er en av konsekvensene globalisering og digitalisering har hatt, og for å møte disse truslene er det nødvendig å utvikle nye former for sikkerhetstiltak. Tiltak som dette kan derimot også medføre ulike implikasjoner.

I denne oppgaven undersøkes det hvilke implikasjoner utviklingen av overvåking som sikkerhetstiltak har hatt for personvernet i samfunnet, etter Lund-kommisjonen avdekket grove brudd på det eksisterende lovverket i 1996. Gjennom å studere dokumenter, rapporter og spørreundersøkelser har oppgavens grunnlag blitt formet, og det er disse dokumentene som bidrar til å oppnå målsettingen til oppgaven. Ved å øke forståelsen rundt overvåking som sikkerhetstiltak og implikasjoner dette kan ha for de demokratiske verdiene vi lever etter, vil det bli enklere å håndtere risikoen for mulige konsekvenser.

Politiets sikkerhetstjeneste og Etterretningstjenestens bruk av overvåking har endret seg de siste 25 årene. Funnene fra min undersøkelse blir belyst av to ulike teoretiske perspektiver. Michel Foucault sin teori om governmentality blir diskutert opp i mot myndighetenes styring av befolkningen. Rammeverket rundt governmentality er stort, og dermed har det blitt lagt et fokus på makt og Foucault sin analyse av den panoptiske disiplin, tillit og diskusjonen rundt frihet og sikkerhet. I tillegg bidrar risiko til å se på befolkningens persepsjon og frykt som et bakteppe for innføringen av sikkerhetstiltak, og trefaktormodellen med å belyse hvordan man kan håndtere trusler, verdier og sårbarheter når det kommer til risikoen for terrorangrep.

Funnene viser at det i all hovedsak er større utfordringer når det kommer til personvern i dag enn i 1996. Mye av årsaken til dette er den stadig økende mengden informasjon som eksisterer på nett og trusselaktørers misbruk av denne. I tillegg vil myndighetene gripe inn i et forsøk på å verne samfunnet. Dette gjøres ved blant annet bruk av overvåking via skjulte tvangsmidler, som kan ha implikasjoner for ivaretakelsen av personvern. På en annen side viser også funnene at fraværet av inngrep fra myndighetene kan føre til negative konsekvenser, i form av mistillit, som kan svekke demokratiet. Debatten rundt verdiene frihet

og sikkerhet er dermed veldig relevant for å finne en god balanse mellom styring av risiko og menneskerettigheter. Det som dog er viktig å påpeke er at fokuset på ivaretakelsen av personvernet også har økt i stor grad, og lovverk har de senere årene blitt oppdatert for å imøtekomme samfunnets behov for sikring av slike demokratiske verdier. Ved at det forekommer en åpen dialog mellom befolkningen og myndighetene vil det gjøre det mulig for befolkningen å ha kontroll med myndighetene, ikke motsatt, noe som kan bidra til å forhindre maktmisbruk og andre negative effekter i samfunnet i årene som kommer.

Innholdsfortegnelse

Tabeller:

Figurer:

Kapittel 1. Innledning

I juni 2013 ble to avisartikler publisert, hos henholdsvis The Guardian og Washington Post. Avisartiklene sendte rystelser gjennom store deler av verdens medieoffentlighet. Et par uker tidligere satt en mann på flyet fra USA til Hong Kong. Med seg hadde han en rekke hemmelighetsstemplede dokumenter han hadde fått tilgang til via sin stilling som informasjonsanalytiker hos et privateid amerikansk konsulentfirma. Videre utover i 2013 kom det nye artikler med alvorlige avsløringer på løpende bånd. De hemmelige dokumentene avslørte en omfattende global masseovervåking gjennomført av amerikanske myndigheter. Gjennom hemmelige rettsavgjørelser og overvåkingsprogram hadde myndighetene fått tilgang til telefondata fra millioner av brukere, samt direkte tilgang til serverne i noen av USAs største teknologiselskaper, blant annet Apple, Google og Microsoft. Det ble også avslørt omfattende britisk overvåking av egne borgere, amerikansk overvåking av et stort antall verdensledere og overvåking av organisasjonene EU og FN (Andreassen, 2013).

Ettervirkningene av Snowden-avsløringene har vært enorme og fått verdensomspennende konsekvenser for bruken av overvåking. Flere land har i ettertid gjennomgått sine egne etterretningstjenester og sett på lovverket knyttet til ulike operasjoner. I Norge ble det blant annet gjennomført en granskning i regi av EU om europeisk masseovervåking av europeiske borgere (Eliassen, 2014; Sveinbjørnson, 2013). Utviklingen av overvåking har i stor grad blitt påvirket av den globale digitaliseringen. Vi lever i et samfunn som har hatt en enorm utvikling når det kommer til digitalisering. Digitalisering refererer til en digital transformasjon, der samfunnet beveger seg fra det analoge til det digitale, ved å ta i bruk teknologi til å fornye, forenkle og forbedre (Regjeringen, 2014). Ved å ta i bruk digital teknologi åpner vi samfunnet vårt for et helt nytt domene, nemlig cyberdomenet, som er fundamentalt annerledes enn det analoge samfunnet som var dominerende i så mange år. Ved å omfavne dette domenet åpner vi for utallige muligheter, både når det kommer til forskning, kjøp og salg av tjenester, offentlig administrasjon, kommunikasjon og ellers en simplifisering av hverdagen vår. En slik utvikling vil derimot også medføre sårbarhet knyttet til teknologi og bruk, og hver gang det tas i bruk en ny digital løsning manifesteres tilhørende risiko. Denne risikoen kan innebære alt fra feilsendinger av e-poster som inneholder sensitiv informasjon, omfattende løsepengevirus til alvorlige datainnbrudd og cyberterror som ikke blir avdekket (Aakre, 2020).

Når samfunnet digitaliseres inkluderer det også at større deler av vårt privatliv vil befinne seg i det digitale domenet. Dette medfører en økt sårbarhet for misbruk av personlig informasjon som ikke eksisterte på samme måte tidligere. Avsløringene til Snowden illustrerer hvordan innhenting og deling av informasjon over nett medfører utfordringer som er knyttet til balansen mellom sikkerhet og individets rettigheter (Kveberg & Johnsen, 2013). Tidligere foregikk alt i samfunnet på papir og for at man skulle kunne stjele data var man nødt til å fysisk bryte seg inn. I dag kan hvem som helst tilegne seg kunnskapen som trengs for å bryte seg inn digitalt. Med argumentasjon i dette foreligger det et behov for innføringen av ulike sikkerhetstiltak for å beskytte norske borgere mot ulike former for angrep, der overvåking er et av dem.

I 1994 vedtok Stortinget å nedsette en kommisjon for å granske påstander om ulovlig overvåking av norske borgere, mer spesifikt ulike politiske grupperinger som under den kalde krigen ble ansett som trusler mot rikest sikkerhet, eksempelvis kommunister og sosialister. To år senere ble det, gjennom Lund-rapporten, avdekket at en slik omfattende overvåking hadde funnet sted. Denne overvåkingen ble gjennomført av Politiets overvåkingstjeneste, Forsvarets sikkerhetstjeneste og Forsvarets etterretningstjeneste, samt andre mennesker som hadde vært knyttet til disse tjenestene. Rapporten som ble utgitt i 1996 avdekket en rekke kritikkverdige forhold i tidsrommet 1945 – 1996 rundt de ulike tjenestene, spesielt da det omhandlet Politiets overvåkingstjeneste (Prop. 6. L. (1998-1999)). I lys av den stadige digitale utviklingen og det endrede trusselbildet vil det dermed være interessant å se på hvordan bruken av overvåking har endret seg den siste tiden. Både Lund-rapporten og Snowden-avsløringene er begge viktige bidrag i hvordan overvåking som sikkerhetstiltak har blitt brukt og hvordan personvernets rolle har utviklet seg.

1.1 Problemstilling og forskningsspørsmål

Denne oppgaven vil ha som hensikt å se på utviklingen av overvåking og personvern i Norge etter Lund-rapporten ble publisert i 1996 og frem til 2021. Det vil således være en historisk tilnærming, der dilemmaer rundt overvåking som sikkerhetstiltak og personvern blir presentert, samt utviklingen av landets stats- og samfunnssikkerhet. Problemstillingen for oppgaven lyder dermed som følger:

Hvilke implikasjoner har utviklingen av overvåking som sikkerhetstiltak hatt for personvernet de siste 25 årene?

For å kunne svare på dette spørsmålet har det blitt utviklet tre ulike forskningsspørsmål. For å kunne kartlegge utviklingen av overvåking innenfor de ulike maktinstansene i Norge er det nødvendig å se på både hvordan den teknologiske utviklingen, endringer i risikobildet mot Norge og lovverk har utviklet seg i løpet av denne perioden. Det første forskningsspørsmålet lyder dermed som følger:

Hvordan har overvåking forandret seg de siste 25 årene?

Utviklingen av overvåking har medført at noen skiller blir klarere og andre mindre tydelige. Skillet mellom samfunnssikkerhet og statssikkerhet har i løpet av de siste 25 årene blitt mindre markert enn tidligere, og kan dermed bidra til å gjøre det utfordrende å danne bestemmelser for hva som inngår i overvåkingsarbeidet. Det neste forskningsspørsmålet som blir stilt er dermed:

Hvordan har statssikkerhet og samfunnssikkerhet endret seg i forhold til utviklingen av overvåking?

Det siste forskningsspørsmålet ønsker å belyse siste del av problemstillingen, og tar for seg en nødvendig del av diskusjonen rundt overvåking som sikkerhetstiltak. Personvern blir en viktigere del av samfunnet etter hvert som samfunnet gradvis blir mer digitalisert. Det siste forskningsspørsmålet lyder dermed som følger:

Hva er utfordringer med denne utviklingen i forhold til personvern?

1.2 Avgrensning

I denne oppgaven ønskes det å se på hvordan overvåking som sikkerhetstiltak har utviklet seg siden Lund-rapporten ble publisert i 1996, altså for 25 år siden, og implikasjoner dette har hatt for personvernet. Dette kan inkludere store mengder data, og det har derfor blitt satt en del klare avgrensninger for hva som vil bli inkludert i oppgaven.

Overvåking innebærer mye forskjellig. I denne oppgaven vil det kun bli tatt for seg elektronisk, skjult overvåking. Dette innebærer dermed ikke overvåking gjennom kameraer eller lignende, men overvåking av elektronisk informasjon på nett. Elektronisk, skjult overvåking kan både være generell, nemlig innsamling av metadata, eller individuell, ved at det for eksempel gjennomføres dataavlesning på en spesifikk maskin. Her vil både generell og individuell overvåking bli inkludert i oppgaven.

Ettersom overvåking blir tatt i bruk over mange ulike nivåer, har det blitt tatt et valg om å avgrense til å se på hvordan overvåking som sikkerhetstiltak blir tatt i bruk av maktinstansene i samfunnet vårt, nemlig Politiet og derunder Politiets sikkerhetstjeneste (PST), samt Forsvaret og Etterretningstjenesten. Det vil også forekomme naturlige begrensninger der trussel- og risikovurderinger ikke går tilbake til 1996. Eksempelvis kom den første trusselvurderingen til PST ut i 2004. Avgrensningen er valgt å sette til disse organene, da det er de som er mest relevante for overvåking fra myndighetene mot befolkningen.

Det vil også bli foretatt en avgrensning når det kommer til hva overvåking blir brukt som sikkerhetstiltak for. I oppgaven vil det dermed kun bli sett på hvordan overvåking blir tatt i bruk for å forhindre ulike typer terrorangrep mot Norge. Det er tatt i bruk ulike sikkerhetstiltak for utrolig mange ulike former for kriminalitet, for eksempel menneskehandel, volds- eller seksualforbrytelser, miljø eller økonomisk kriminalitet, hvor terrorisme kun er en av dem. Å omfatte flere former for kriminalitet som blir regulert av overvåking blir å gape over for mye.

1.3 Tidligere forskning

Det har blitt skrevet flere teoretiske bidrag om overvåking, både i Norge og i resten av verden. Feltet som omfatter overvåkingsstudier har vokst i enorm fart siden 90-tallet, noe som har med den teknologiske utviklingen og utviklingen av styringsmekanismer å gjøre, i tillegg til den økende mengden nye tilskudd av teoretiske forklaringer på feltet. Det er funnet flere forskningsbidrag som tar for seg ulike sider av overvåking – mange går langt tilbake til de første diskusjonene som omhandlet overvåkingssamfunnet, men det eksisterer mange nyere bidrag i tillegg. I dette underkapittelet vil det bli lagt frem et utvalg av bøker, forskningsartikler og rapporter fra både norske og internasjonale bidrag på feltet.

Lyon er en forfatter som har bidratt med ulike perspektiver på hvordan overvåking fungerer i et samfunn og hvilke effekter og konsekvenser dette vil kunne føre til. Han har blant annet skrevet «Surveillance after September 11» og «Surveillance after Snowden» som begge tar for seg hvilken effekt de respektive hendelsene hadde på holdningene til overvåking i verden, samt «Surveillance Studies: An Overview» som tar for seg ulike måter overvåking blir konseptualisert på (Lyon, 2003, 2007, 2015), for å nevne noen.

I tillegg har det blitt publisert flere norske bidrag på området. Schartum (2010) har regissert boken «Overvåking i en rettstat» som, med hjelp fra et utvalg av eksperter på området, belyser temaer som personvern, rettssikkerhet og kriminalitetsbekjempelse i forhold til overvåkingen som blir gjennomført i samfunnet. Den tar for seg både PST og Etterretningstjenesten sin virksomhet, samt det relaterte kontrollorganet – EOS-utvalget. Hausken et al. (2014) har skrevet boken «Fra terror til overvåking: Overvåking i Norge, et kritisk prospekt». Også her er det flere viktige bidrag fra mange forskjellige fagområder, som alle tar utgangspunkt i Gjørv-rapporten og terrorangrepene som fant sted 22. juli 2011 (NOU 2012: 14). Her blir ulike spørsmål og dilemmaer diskutert som er av relevans for hvordan overvåking vil fungere som terrorforebyggende tiltak. Engene (2013) og Wessel-Aas (2012) er også to viktige bidragsytere på feltet, der begge serverer gode forskningsartikler som problematiserer utviklingen av overvåking sett opp terrorisme, digitalisering og ulike demokratiske verdier.

Det er flere av de overnevnte bidragene som også inkluderer personvern som et tema, da dette er et meget relevant tema i forhold til overvåking. Andre bidrag er blant annet «Status for ytringsfriheten i Norge» (Staksrud et al., 2014). Dette er en rapport som fremlegger hovedresultatene fra befolkningsundersøkelsen i 2014, samt fire andre spørreundersøkelser som har blitt gjennomført i prosjektet. Et av kapitelene er spesifisert til å handle om overvåking, terror og kontroll, og ser blant annet på både tillit til myndighetene og hvilke rett myndighetene skal ha til å gjennomføre ulik form for overvåking og datainnsamling gjennom blant annet sosiale medier og e-post.

Relevant tidligere forskning inkluderer også flere andre temaer og ulike forskningsbidrag. Boken «Security» til Buzan et al. (1998) tar eksempelvis for seg en utvidet forståelse av sikkerhetsbegrepet, og vil videre være veldig relevant. Olsen et al. (2007) sin artikkel

«Societal safety: Concept, borders and dilemmas» er også meget relevant for mye av forståelsen som ligger til grunn for relevante begreper videre i oppgaven.

I løpet av litteraturgjennomgangen har det blitt funnet utrolig mange interessante bøker, artikler, rapporter og tidligere masteroppgaver. Denne oppgaven vil forsøke å være et bidrag til debatten fra et av de mange relevante fagområdene når det kommer til temaet overvåking og personvern.

1.4 Oppgavens struktur

Kapittel 1 består av en introduksjon til oppgavens tema, problemstilling og medfølgende forskningsspørsmål. I tillegg blir det satt en avgrensning for oppgavens tema, tidligere forskning gjennomført på området og oppgavens struktur.

Kapittel 2 tar for seg konteksten for oppgavens tema, nemlig «Overvåking i Norge». Her blir det først redegjort for utviklingen av digitalisering i Norge, før det deretter kort blir presentert hvordan overvåking i Norge så ut etter 2. verdenskrig og frem til Lund-kommisjonen. Videre presenteres et overblikk over hvordan maktinstansene i Norge er organisert i forhold til overvåking og deres ansvarsområder. Til slutt blir personvern presentert, sammen med relevant lovverk.

I kapittel 3 blir det lagt frem relevant teori, som blir brukt for å diskutere empirien i kapittel 6. Teoriene tatt i bruk er Foucault sitt governmentality-begrep og risiko. Innenfor governmentality blir det fokusert på styring, makt og tillit, samt frihet og sikkerhet. Risiko blir presentert ved trefaktormodellen og risikopersepsjon ved det realistiske og det konstruktivistiske perspektivet. I tillegg blir risiko presentert i forhold til governmentality-begrepet. Til slutt blir det redegjort for noen ulike begreper: stats- og samfunnssikkerhet og terrorisme.

Kapittel 4 er metodekapittelet. Her blir det redegjort for den metodiske tilnærmingen til oppgaven, datainnsamlingen, kvalitetskriterier og metodiske styrker og svakheter.

I kapittel 5 blir empirien fremlagt og presenterer datagrunnlaget som er hentet inn i oppgaven. Kapittelet er strukturert etter forskningsspørsmålene og empirien vil bidra til å svare på oppgavens problemstilling.

Kapittel 6 består av oppgavens analyse og drøfting. I dette kapittelet blir den innsamlede empirien drøftet opp mot det teoretiske rammeverket presentert i kapittel 3.

Til slutt vil det bli presentert en konklusjon av oppgaven i kapittel 7, i tillegg til et kort avsnitt om forslag til videre forskning. Referanseliste og andre vedlegg kommer til slutt.

Kapittel 2. Overvåking i Norge

I dette kapittelet vil det vil det først bli redegjort for digitaliseringen og dens effekt på overvåking gjennom tidene. Deretter blir det presentert hvordan overvåking og trusselbildet så ut før Lund-kommisjonen, nærmere bestemt fra 2. verdenskrig til 1996. Videre blir det presentert en oversikt over de relevante maktinstansene i samfunnet, som vil være de videre subjektene i oppgaven, før begrepet personvern blir presentert i slutten av kapittelet.

2.1 Overvåking og digitalisering

Overvåking kan forstås som mange ulike ting. Begrepet stammer opprinnelig fra det franske ordet «surveiller» som på norsk betyr «å våke over», og refererer til prosesser der noe menneskelig atferd får spesiell oppmerksomhet, som går langt over grensene for uskyldig nysgjerrighet (Lyon, 2007, s. 13). Denne oppmerksomheten vil i slike tilfeller både være av et visst omfang, en viss varighet og bli gjennomført med en viss systematikk. Formålet kan være alt fra å ønske innflytelse, ha kontroll og styring eller generell beskyttelse. Overvåking i Norge har, som de fleste andre tingene i samfunnet, blitt sterkt preget av den stadig økende digitaliseringen. Norge er et av landene som ligger godt over gjennomsnittet i Europa når det kommer til digitale ferdigheter, bruk av digitale tjenester og faktisk bruk av internett. I tillegg har vi en høy tillit til egne myndigheter som er langt over gjennomsnittet sammenlignet med andre (NHO, 2018).

Digitaliseringen kan sies å ha bestått av fem ulike digitaliseringsbølger. Dæhlen (2017) skriver at vi for lengst har beveget oss inn i den femte digitaliseringsbølgen – fra data til innsikt. Nå handler det ikke kun om datainnsamling lengre. Nå ligger derimot det viktigste fokuset på hvordan vi anvender kunnskapen vi har ervervet oss (NHO, 2018). Den første digitaliseringsbølgen omfattet den første bruken av store datamaskiner for å løse ulike samfunnsoppdrag og utfoldet seg mot slutten av 1960-tallet og utover på 1970-tallet. Den andre digitaliseringsbølgen bygger på den første og kjennetegnes av den personlige datamaskinen. Maskinene ble både mindre og rimeligere, og med brukervennlige operativsystemer og funksjonalitet kunne man plassere datamaskinen på skrivepulten og bruke den blant annet i jobbsammenheng. Internett var avgjørende for at brukerne av datamaskinene kunne kommunisere via skjerm og tastatur, og dette var begynnelsen på den tredje digitaliseringsbølgen. Bruken av internett eksploderte tidlig på 1990-tallet, mye på grunn av World Wide Web (WWW). Dette var et redskap som i utgangspunktet ble utviklet

slik at forskere kunne dele data og forskningsresultater, men ble derimot gitt ut gratis til hele verden og er mye av grunnen til hoppet i den digitale utviklingen videre. Den fjerde digitaliseringsbølgen omhandler at alle nå har kraftige datamaskiner så små at de får plass i lommen, nemlig smarttelefoner. Det produseres data i et ekstremt omfang over hele verden, og alt som kan digitaliseres digitaliseres. Dette gir et veldig godt grunnlag for bølgen vi er inne i nå som omhandler at vi evner å utnytte denne ekstreme dataflommen og danne innsikt ut av det. Det utvikles stadig vekk nye måter å ta i bruk data for å oppnå kontroll, nå nye eller allerede eksisterende kunder eller rett og slett ha oversikt over hva som gjøres. Det er derfor også nødvendig at vi evner å håndtere utfordringer knyttet til sikkerhet, ettersom det er viktig at data, spesielt data som inneholder sensitive opplysninger, håndteres på en forsvarlig måte (Dæhlen, 2017).

Overvåking har også endret seg i tritt med den digitale utviklingen. Før ble overvåking brukt via blant annet spaning og telefonavlytting. Ettersom den digitale utviklingen har medført at mer og mer datadeling foregår over nettet vil slike gamle metoder etter hvert anses som utdaterte. Da det har blitt mer utfordrende å eksempelvis overføre penger eller bestille reiser via telefon, vil det bli stadig færre som dermed deler personlig informasjon via slike kanaler. Overvåking ved eksempelvis telefonavlytting vil derfor ikke være like relevant i dag. Overvåking tas i bruk som et sikkerhetstiltak for å kunne avverge ulike angrep mot Norge. Slike angrep kan eksempelvis være statlige terrorangrep mot viktige bygninger, dataangrep på kritisk infrastruktur eller terror utført av enkeltpersoner på åpne plasser. Man kan grovt skille mellom tiltak som har som formål å forebygge, oppdage eller respondere på uønskede hendelser. Overvåking regnes som et overordnet sikkerhetstiltak og har som mål å fange opp kommunikasjonen mellom menneskene som planlegger utførelsen av slike handlinger. Et slikt sikkerhetstiltak omhandler dermed å oppdage og avdekke uønskede hendelser før de forekommer. Det er viktig å være bevisst på hvilken effekt et slik tiltak har og hvordan det tas i bruk, slik at det ikke blir brukt unødvendige ressurser på tiltak som ikke er nødvendig, i tillegg til å se på eventuelle konsekvenser av sikkerhetstiltak og veie det opp mot effekten (Digitaliseringsdirektoratet, 2020).

2.2 Overvåking i Norge

2.2.1 Etter 2. verdenskrig

Overvåking har eksistert i alle år, men måten overvåking har blitt brukt tidligere er i stor grad annerledes enn slik det blir tatt i bruk i dag. I 1996 ble det, som nevnt innledningsvis, avdekket at myndighetene bedrev omfattende masseovervåking av utvalgte grupper i Norge. Det ble nedsatt en kommisjon i 1994 for å granske påstandene om ulovlig overvåking gjennomført av Politiets overvåkingstjeneste (nåværende PST), Forsvarets sikkerhetstjeneste og Forsvarets etterretningstjeneste, i tillegg til mennesker som var knyttet til de ulike tjenestene (Prop. 6. L. (1998-1999)). Rapporten tar for seg årene fra 2. verdenskrigs begynnelse og frem til midten av 90-tallet. I rapporten kommer det frem at de som ble antatt å utgjøre en trussel for landets sikkerhet i stor grad var kommunistene og deres partier, det norske kommunistpartiet og Arbeidernes kommunistparti, samt Sosialistisk Folkeparti. I tillegg blir det også utredet for en ny trussel fra høyreekstreme grupper. Funnene i rapporten baserer seg i hovedsak på bruk av ulovlige virkemidler i PST, og innebærer både det daværende mangelfulle regelverket, rom- og telefonavlytting og medfølgende kontroll. Telefonavlytting hadde ikke hjemmel i lov før 1960, men ble brukt for å overvåke kommunister allerede i 1950-årene. Omfanget økte også vesentlig etter 1957 da overvåkingspolitiet fikk båndopptakere. Kontrollutvalget for telefonavlyttingen ble også kraftig kritisert.

2.2.2 Organisering av overvåkings- og kontrollorganer i Norge

PST er et særorgan innen politietaten og direkte underlagt Justis- og beredskapsdepartementet. De følger politiloven (1995) og PST-instruksen (Instruks for Politiets sikkerhetstjeneste, 2005), og ansvarsområdet deres omhandler i all hovedsak å forebygge og motvirke straffbare handlinger og annen virksomhet som kan medføre fare for rikets sikkerhet i vid forstand. Det som skiller PSTs virksomhet fra resten av Politiet er tjenestens forebyggende arbeid mot både enkeltpersoner eller miljøer som *ikke* er mistenkt for konkrete straffbare forhold, jfr. PST-instruksen § 13, annet ledd. Etterretningstjenesten er på en annen side underlagt Forsvaret og er Norges militære utenlandsetterretningstjeneste. De støtter blant annet norske myndigheter med informasjon og vurderinger og utenriks-, sikkerhets- og forsvarspolitiske forhold. Tjenesten er underlagt etterretningstjenesteloven (2020).

Etter Lund-kommisjonen ble offentlighetens søkelys rettet mot PST og det forelå et sterkt ønske om sterkere politisk kontroll og styring av tjenesten og etterlevelse av gjeldende regler. EOS-utvalget er et eksempel på en kontrollmekanisme som blir tatt i bruk når det kommer til kontroll av bruk av ulike tvangsmidler hos blant annet Politiet og påtalemyndighetene. EOS-utvalget handler om å kontrollere etterretnings-, overvåkings- og sikkerhetstjenester som styres av offentlige myndigheter. De er uavhengig av Stortinget og målet deres er å ivareta nasjonale sikkerhetsinteresser, som enkeltpersoners rettssikkerhet og personvern. Utvalget sin oppgave er å klarlegge om og forbygge at rettigheter krenkes, samt følge med på om tjenestene kun tar i bruk midler som er nødvendige etter forholdene og at menneskerettighetene opprettholdes (EOS-utvalget, u.å.). Når det kommer til PST kontrollerer utvalget særlig innhenting og behandling av personopplysninger, forbyggende og avsluttede etterforskningssaker, bruken av tvangsmidler og hvordan informasjon blir delt med andre aktører og samarbeidspartnere, både innad i Norge og i utlandet. Hos Etterretningstjenesten er det en hovedoppgave å påse at forbudet mot overvåking eller andre fordekte metoder for innhenting av informasjon om norske borgere overholdes (EOS-utvalget, u.å.) For EOS-utvalget er særlig Menneskerettighetskonvensjonen, art. 8 relevant, om retten til privatliv og personvern, som blir videre utdypet i kapittel 2.3.

2.3 Personvern

Personvern vil videre i oppgaven bli forstått som retten til privatliv, samt retten til å bestemme over egne personopplysninger. Som enkeltmenneske skal man ha rett på en privat sfære, hvor en kan handle fritt uten verken tvang eller innblanding fra staten eller andre mennesker. Å opprettholde et godt personvern omhandler ikke kun den enkeltes privatliv, men er også nødvendig både for å opprettholde et sterkt demokrati og at man skal ha innflytelse på bruk og spredning av egne personopplysninger (Datatilsynet, 2019a). Hvert enkelt menneske skal altså ha rett og reell mulighet til å både ha kunnskap om og rådighet over bruken av egne personvernopplysninger (NOU 2015: 13, s. 27). Personopplysninger innebærer mye forskjellig og kan både skrives på papir, lagres elektronisk, overføres via post eller elektroniske media eller formidles muntlig (Datatilsynet, 2018).

Ivaretakelse av personvernet er forankret i Menneskerettighetskonvensjonen (EMK). EMK ble vedtatt i 1950 for å beskytte menneskerettighetene og de grunnleggende friheter, og i 1999 ble den gjort til norsk lov ved å inkorporere den i Menneskerettsloven. EMK art. 8 (1) leser:

«Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse» (Menneskerettsloven, 1999). I 2014 ble det også vedtatt å ta denne bestemmelsen inn i Grunnloven § 102: «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integritet» (Grunnloven, 1814). Retten til privatliv etter Grunnloven § 102 er dermed ikke absolutt, og det har i Rt. 2014 (avsnitt 28) blitt presentert tre vilkår som må være til stedet for å gjøre inngrep i Grunnloven § 102. Det må være lovhjemlet, inngrepet må ivareta et legitimt formål eller være saklig begrunnet og det må være forholdsmessig, altså at inngrepet ikke må gå mer utover hensynet til privatlivet enn nødvendig (Prop. 131. L. (2018-2019)).

I Norge er den mest relevante loven for personvern loven om behandling av personopplysninger. Personopplysningsloven (2018) omhandler hvordan innsamling og bruk av personopplysninger skal gjennomføres, og består både av nasjonale regler og EUs personvernsforordning (GDPR). GDPR er regler som gjelder alle EU og EØS-land når det kommer til personvern, og forordningen går foran norsk lov om det oppstår konflikt. Det er også flere tilfeller der personopplysningsloven ikke gjelder, der et av tilfellene er når myndighetene jobber for å forebygge, etterforske eller straffeforfølge straffbare forhold (Datatilsynet, 2019b).

2.3.1 Konfidensialitet, integritet, tilgjengelighet og robusthet

Direktoratet for IKT og fellestjenester i høyere utdanning og forskning har utgitt en veileder som blant annet forklarer hvilke krav GDPR stiller til informasjonssikkerheten ved behandling av personopplysninger (UNIT, 2020). Informasjonssikkerhet brukes for å forklare evnen til å forebygge, avdekke og håndtere hendelser og risiko som kan føre til brudd på personopplysningenes *konfidensialitet, integritet* og *tilgjengelighet.* I GDPR er en fjerde sikkerhetsegenskap også nevnt, nemlig *robusthet*. De fire overnevnte egenskapene skal bidra til en effektiv ivaretakelse av personvernprinsippene og de ansvarlige som håndterer dataen har nå en plikt om å følge dette. Dataen det er snakk om vil anses som verdier. Konfidensialitet er beskyttelse mot uvedkommendes tilgang til å observere en verdi. Spionasje kan være et eksempel på brudd på sikkerhetsmålet konfidensialitet. Integritet er beskyttelse mot uønsket endring av en verdi. Dataormen Stuxnet er et godt eksempel på brudd på integritet som sikkerhetsmål. Stuxnet var svært avansert og endret parameterne til dataprogrammene til et iransk anlegg for å anrike uran, noe som forårsaket store fysiske

ødeleggelser. Tilgjengelighet er beskyttelse mot uønsket tap, reduksjon eller stans av en verdi. Eksempler på brudd på sikkerhetsmålet tilgjengelighet kan blant annet være løsepengevirus som krypterer alle filene på laptopen eller problemer med innlogging i nettbanken (Bergsjø et al., 2020). Den siste, robusthet, omhandler at systemene som behandler verdiene er motstandsdyktige og evner å raskt gjenopprette normaltilstand ved uønskede hendelser. På grunn av den teknologiske utviklingen utvikler det seg også stadig nye sikkerhetstrusler som tar i bruk nye verktøy og metoder. Det vil si at de som er ansvarlige for å håndtere dataen også er nødt til å ta hensyn til dette og oppdatere systemene etter behov. Dette stiller GDPR krav til (Datatilsynet, 2018).

Kapittel 3. Teori

Dette kapittelet tar for seg den teoretiske tilnærmingen som blir tatt i bruk for å videre belyse oppgavens empiri. Først blir det teoretiske rammeverket presentert. Det begynner med en introduksjon til begrepet *governmentality* fra filosofen Michel Foucault, som vil bli brukt som et analytisk rammeverk videre i oppgaven. Begrepet governmentality har ofte blitt oversatt til norsk ved bruk av begreper som styringsmentalitet eller regjering. I denne oppgaven vil derimot det engelske begrepet governmentality bli tatt i bruk videre, da ordene som fremkommer i den norske oversettelsen kan ha flere betydninger. Foucault rakk å gjøre seg innledende tanker om begrepet governmentality før sin død i 1984. Andre forskere har videre gjort seg opp egne tanker om governmentalitybegrepet, der flere fungerer godt til å belyse hvordan digitaliseringen og trusler har påvirket overvåking, og medfølgende personvern. Mye av fokuset ligger på Dean (2010) sin tolkning av begrepet, samt kjernebegreper som makt, tillit, frihet og sikkerhet som alle vil være nødvendig for forståelsen av konseptet. Videre blir det redegjort for *risiko* som konsept. Her blir det redegjort for hva begrepet innebærer, en distinksjonen mellom et realistisk og et konstruktivistisk syn på risiko, i tillegg til hvilken rolle risiko har innenfor governmentality. Kapittelet avsluttes med en forklaring på den tradisjonelle forskjellen mellom stats- og samfunnssikkerhet, i tillegg til en forklaring av begrepet terrorisme.

3.1 Governmentality

Begrepet governmentality ble først presentert av Michel Foucault gjennom foredragene *Sikkerhet, territorium, befolkning* i 1977 og 1978 (Foucault, 2007). Foredragene tok for seg hvordan politisk makt i samfunnet kunne bli forstått og hvilke teknikker og prosedyrer som eksisterte for styring av mennesker i praksis. Det var tydelig at begrepet governmentality i seg selv var nytt på tiden da foredragene ble holdt. Begrepet ble ikke lagt frem på en systematisk måte, men ble heller formet gjennom foredragene. Det som ble lagt frem var derimot et sett med veldig generelle definisjoner på hva governmentality er, men ingen nøyaktig forståelse av begrepet. Joseph (2009) argumenterer dermed for hvordan governmentality må sees på som en del av et analysefelt der det krysses med andre konsepter og ideer. Siden Foucault sin tid har nemlig begrepet blitt brukt for å analysere flere ulike temaer i diverse kontekster, som blant annet helse, kriminalitet og økonomi (Miller & Rose, 1986; O'Malley, 1992; Power, 1997).

Dean (2010) bruker beskrivelsen 'conduct of conduct' når han snakker om governmentality, noe som kan oversettes til styring av styringen. Uttrykket spiller på flere ulike betydninger av begrepet styring. Styring kan på en side sees på som en samlebetegnelse for den praksisen og de prosedyrer og teknikker som har som formål å forme, lede og påvirke menneskets atferd, slik at de selv oppfatter at de oppnår egne mål (Dean, 2010). På en annen side er ikke styring kun forbeholdt staten. Governmentality omfatter både hvordan styring av subjekter forekommer, men også styring av en selv. Når alle betydningene av forklaringen 'conduct of conduct' samles, tegnes det et bilde av styring som:

> Government is any more or less calculated and rational activity, undertaken by a multiplicity of authorities and agencies, employing a variety of techniques and forms of knowledge, that seeks to shape conduct by working through the desires, aspirations, interests and beliefs of various actors, for definite but shifting ends and with a diverse set of relatively unpredictable consequences, effects and outcomes. (Dean, 2010, s. 18).

For Foucault (2007) er dermed befolkningen det virkelige objektet for governmentality, enten om det gjelder styring av eget selv, som for eksempel å følge en diett fordi man har diabetes, eller for eksempel myndighetenes implementering av tiltak for å sikre befolkningen mot angrep utenfra. Governmentality vil dermed være åpent for hvem som besitter styringsmyndigheten, men de som blir styrt vil alltid være befolkningen.

Begrepet blir i stor grad diskutert i konteksten av liberale demokratier, slik som det norske. Fra et liberalt perspektiv regnes governmentality som både teknikk og rasjonale til myndighetene. Foucault utdyper dermed betydningen av ordet governmentality som «fremveksten av en ny form for tenkning og utøvelse av makt i visse samfunn» (Dean, 2010, s. 28). Begrepet vokste frem i Vest-Europa i den tidlige moderne tid, da teknikkene og kunnskapen dannet gjennom humaniora og samfunnsvitenskapene ble integrert i styringskunsten[1]. Foucault utdypet tre aspekter ved governmentality. For det første var befolkningen som nevnt objektet for governmentality, samtidig som politisk økonomi stadig ble en viktigere del av samfunnet. Styringen skulle være en styring for alle, både for

[1] Styringskunst eller «art of government» referer til styring som en aktivitet som innebærer håndverk, fantasi, tilpasning, bruk av både taus og praktisk kunnskap, intuisjon osv. Dean, M. (2010). *Governmentality. Power and rule in modern society* (2. ed.). Sage Publications.

enkeltmenneskene og for befolkningen som en gruppe. Dette innebar altså helse, velferd, velstand og lykke for befolkningen. For å oppnå dette var det derfor en nødvendighet å styre gjennom et bestemt register – økonomien. For det andre måtte det fremkomme en relasjon mellom styring og andre former for makt, spesielt suverenitet og disiplin. Suveren makt innebærer konstitusjoner, lover og parlamenter, og er utøvelse av autoritet over subjekter i en befolkning innenfor et bestemt territorium. Disiplinær makt har derimot en mangfoldig opprinnelse innen blant annet klostre, militæret og utdanningsinstitusjoner, og regnes som regulering og kontroll over antall mennesker innenfor det territoriet, som for eksempel oversikt og regulering over skolegang, militær trening eller organisering av arbeid. Selv om styringsmyndigheten innen governmentality beholder og benytter seg av flere av de samme teknikkene og rasjonale som i disiplinær makt og suverenitet, så viker de på samme tid vekk fra dem og søker å omskrive dem. Her ønskes det heller en forvaltning av egenskapene til befolkningen, være seg hvor mange som bor i territoriet, døds- og fødselsrate, antall gifte, ugifte eller skilte, hvordan folk bruker tiden sin, hvor mye kriminalitet det er, samt mange andre ting. Dette kan være nødvendig av økonomiske grunner, og gjennomføres gjennom overvåking og kontroll av befolkningens egenskaper (Grimen, 2010). På denne måten regnes objektet for governmentality som en befolkning, som individer og som ressurser som kan fostres, brukes og optimaliseres. Det tredje aspektet Foucault nevner ved governmentality er at myndighetene gradvis har bygget opp noe Foucault kalte *apparatuses of security.* Inkludert i disse apparatene for sikkerhet var blant annet hærer, politistyrker, etterretningstjenester, diplomatkorps og spioner. I tillegg inkluderte Foucault alle praksiser og institusjoner som måtte til for å sikre en optimal funksjon av de økonomiske, vitale og sosiale prosessene som eksisterer innenfor en befolkning, som blant annet helse-, velferd- og utdanningssystemer. Et slikt apparat vil på denne måten legge til rette for, samt forme, befolkningen i den retningen styringsmyndighetene ønsker (Dean, 2010).

Styringsteorien til Foucault går dermed kort ut på at staten gradvis har blitt mer styringsdyktige, der ulike institusjoner, praksiser og instanser har utviklet apparater for kontroll av hendelser, som eksempelvis fødsel, død, helsetilstand og byutvikling. Det blir på et vis etablert en styringskultur, som mer eller mindre manipulativt påvirker befolkningen til å velge atferd de tror de velger selv. Styringsmyndighetene etablerer ulike måter å tenke på og slik blir subjektene påvirket til å opptre forholdsvis disiplinært. Dette gjelder handlinger som å gå på skole, spise sunt, gå til legen og lignende. De styrte handlingene blir på denne måten

ansett som egeninteresse hos subjektene i befolkningen. Governmentality kan dermed regnes som en form for ledelse, det målet er å styre menneskets selvstyring av sin egen atferd.

3.1.1 Makt

Foucault sin måte å beskrive makt på bryter i stor grad med andre, mer tradisjonelle maktteorier. Fokuset til Foucault var at makt er overalt og at det eksisterer i alle relasjoner. Han skrev: «Power is not something that is acquired, seized or shared, something one holds on to or allows to slip away» (Foucault, 1981, i Grimen, 2010, s. 107). Han mente heller at makt var relasjonelt – at det blir tydelig når det utøves. På grunn av dette relasjonelle aspektet mente ikke Foucault at makt var assosiert med en bestemt institusjon, men heller med ulike praksiser, teknikker og prosedyrer. Makt forekommer på alle nivåer og på tvers av mange dimensjoner. Det er vanskelig å omfatte alt som Foucaults tolkning av makt innebar, men hans tolkning bidro til å utvide området for maktanalyser. Han satte fokus på moderne maktteknologier som er tett knyttet opp til styringen av staten og som trenger inn i alle sider av menneskets liv (Grimen, 2010).

Foucault hadde spesielt to fremstillinger av makt som er spesielt relevante for moderne styringsformer. Den første omhandler hvordan det eksisterer en indre sammenheng mellom kunnskap og makt, noe som kommer tydeligst frem i boken hans *Overvåking og straff* fra 1975. Her gjennomfører han en analyse av Jeremy Benthams modell for det perfekte fengsel, *panoptikon*. Fengselet var utformet slik at vokterne til en hver tid kunne se fangene, men fangene kunne verken se hverandre eller vokterne. På denne måten visste de at de kunne bli overvåket, men de visste ikke når. Vokterne kunne også overvåke hverandre. Foucault omtalte en slik panoptisk disiplin som mønsteret bak en ny form for maktmekanisme, som gradvis formet det nye overvåkingssamfunnet. Det spredte seg til blant annet militæret, fengsler, fabrikker, sykehus, og ligger nå nedfelt i moderne samfunn sine institusjoner og arkitektur. Panoptikon ble tilrettelagt slik at det skulle være mulig å samle inn kunnskap om fangene, noe som er helt essensielt for slik maktutøvelse. Det foreligger dermed en tett relasjon mellom makt og kunnskap, der det ikke forekommer en motsetning mellom de (Nortvedt & Grimen, 2004).

Det andre punktet omhandler hvordan makt ikke kun setter grenser for hva som kan gjøres, men hvordan den også kan være produktiv. Makt kan forme menneskets sinn, samtidig som

en bestemt innretning på sinnet kan være en forutsetning for at den samme maktutøvelsen skal være effektiv. Et eksempel på dette kan være hvordan mange former for medisinsk behandling innebærer at pasientene er nødt til å være disiplinerte til å handle på ulike måter for at behandlingen skal fungere, som for eksempel selvbehandlingsregimet nødvendig for god diabetesbehandling. Diabetikere kan i dag styre behandlingen sin i stor grad selv, ved bruk av ny teknologi som insulinpenner og -pumper, samt instrumenter for å måle blodsukkeret. Helsevesenet tar derimot prøver med jevne mellomrom for å kontrollere langtidsblodsukkeret, som viser om de har vært flinke de siste månedene. Det å følge en slik behandling krever dermed et bestemt type sinn som klarer å gjennomføre et slikt regime, både med selvbehandling og gjennom helsevesenet, diabetesorganisasjoner og alt opplysningsmateriale. Diabetikere trenes på denne måten opp, de drilles, til å bli disiplinerte og «gode pasienter» (Grimen, 2010). Grimen (2010) skriver at årsaken til at diabetes er valgt som eksempel, er fordi det beskriver et godt eksempel på moderne maktteknologi. I den moderne styringskunsten er det i tillegg viktig å opprettholde en god helsetilstand hos befolkningen. En av måtene å holde helsetilstanden under kontroll er ved å styre subjektene sin atferd gjennom å disiplinere de i å styre seg selv: pusse tennene morgen og kveld, bruke prevensjonsmidler, ta medisinene etter legens dosering, holde det rent i huset osv. Moderne styringskunst utnytter dermed det Foucault kaller for den produktive makten, ved å forme sinn og atferdsmønstre hos befolkningen.

3.1.2 Tillit

Tillit er et konsept som har blitt diskutert i stor grad opp gjennom tidene. Hovedårsaken til dette er at tillit er grunnsteinen til ethvert velfungerende demokrati. Det forutsettes at det i et demokrati forekommer en viss grad av tillit mellom innbyggerne, mellom innbyggerne og myndighetene, mellom myndighetsorganer, mellom arbeidsgiver og ansatt osv. Det er rett og slett en forutsetning for at de demokratiske prosessene skal kunne forekomme, i tillegg til økonomisk vekst, velferd og stabilitet i et samfunn. Når stadig mer av den nasjonale veksten er knyttet til digitalisering vil også tillit på dette området bli viktigere (Bergsjø et al., 2020). Nortvedt and Grimen (2004) trekker frem særlig tre viktige trekk med tillit. Tillit vil for det første gjøre giveren av tillit sårbar for tillitsmottakerens mulige inkompetanse og onde vilje, da man ikke kan være sikker på om mottakeren vil handle som man forventer. For det andre blir verden mindre kompleks om man stoler på noen. Tillit reduserer altså kompleksitet. Det tredje trekket de nevner er at tillit ikke er noe som kan påtvinges noen og at det ikke kan

kjøpes. Om det kan kjøpes er det god grunn til å mistro det man har kjøpt (Nortvedt & Grimen, 2004)

Foucault (2007) la vekt på at høy konformitet hos befolkningen tilsier at tilliten fra befolkningen til myndighetene er høy. Flere ulike rapporter og undersøkelser viser til at Norge ligger høyt på verdenstoppen når det kommer til tillit til både myndighetene, lokaldemokrati og politiet. I rapporten *Samfunnsspeilet* kommer det frem at norske borgere generelt har høyt tillit til de ulike politiske institusjonene i samfunnet sammenlignet med resten av Europa. På tillitstoppen i Norge ligger tilliten til politiet og deretter rettsvesenet. Stortinget ligger på en tredjeplass. Tilliten til de politiske partiene og politikerne er klart lavere enn de øvrige, men sammenlignet med Europa er nordmenns tillit på disse punktene høyest i Europa (Kleven, 2016). I rapporten *Politisk tillit, lokaldemokrati og legitimitet* kommer det frem at av utvalget som var med i undersøkelsen sier 24% at de er fornøyd og 62% at de er ganske fornøyd med måten demokratiet virker på i Norge (Haugsgjerd & Segaard, 2020).

Foucault var veldig interessert i fenomenet tillit. Han opplevde at det liberale samfunnet tidvis fremstod som hyklersk, i form av at tillit i institusjoner og arkitektur er bygget på systematisk overvåking, kontroll av og mistillit til befolkningen. Eksamener, billettkontroller, jevnlige valg, passkontroll, kredittvurdering og habilitetsregler er et utvalg av eksempler på institusjonalisert mistillit i samfunnet. Luhmann (1999, i Nortvedt og Grimen, 2004) påpeker derimot at tillit og mistillit begge kan vokse samtidig, og at tillit i et samfunn også kan være avhengig av en slik institusjonalisert mistillit.

3.1.3 Styring, frihet og sikkerhet

Frihet er en verdi som blir høyt verdsatt av de aller fleste mennesker og liberale demokratiske samfunn er stolte av hvor mye individuell frihet som vektlegges. Det eksisterer derimot en pågående debatt rundt hvorvidt individenes frihet skal innskrenkes når det kommer til sikkerhet i samfunnet, da det argumenteres for at de to verdiene i seg selv ikke kan utfoldes fullt ut samtidig.

De tre mest kjente formene for frihet er negativ, refleksiv og sosial frihet. Negativ frihet, også omtalt som juridisk frihet, er rett og slett fraværet av begrensninger eller ytre påvirkning når det kommer til et individs atferd. At befolkningen har individuelle rettigheter gjør det mulig

for dem å ta egne valg om hvordan de skal leve deres liv uten å måtte rettferdiggjøre dette for noen andre – så lenge de følger loven og respekterer andre individers rettigheter. Refleksiv frihet handler på den andre siden ikke om ytre påvirkning, men heller om hvordan ens atferd og handlinger stemmer overens med ens moralske selvfølelse. Refleksiv frihet kan også omtales som fornuft. Sosial frihet innebærer at individer oppnår frihet når de blir godt integrert i et samfunn. Denne formen for frihet inkluderer dermed en gjensidig avhengighet mellom individet og diverse institusjoner i samfunnet og er derfor omdiskutert (Honneth, 2015). Foucault er også skeptisk til denne formen for frihet, da han mener at integrering medfører en slags paternalistisk normalisering, som igjen vil føre til konformitet.

I et samfunn vil det alltid forekomme ulike sikkerhetstrusler, enten det er svak infrastruktur, terror eller dataangrep. Myndighetene vil dermed innføre diverse sikkerhetstiltak for å beskytte samfunnet og befolkningen som blir utsatt for disse truslene. Slike tiltak vil på en side begrense den individuelle friheten til subjektene i et samfunn. I moderne, liberale samfunn eksisterer det mange pålagte begrensninger i den individuelle, negative friheten, eksempelvis trafikkregler, sikkerhet på arbeidsplassen eller forbud mot røyking på visse offentlige plasser. Slike begrensninger blir ofte innført grunnet at myndighetene ønsker å redusere risiko og dermed beskytte befolkningen (Engen et al., 2016). Fra et annet perspektiv kan derimot sikkerhet sees på som bidragsyter til vår frihet. Ved at hvert enkelt menneske i et samfunn gir fra seg litt av sin individuelle frihet til fordel for beskyttelse, oppnår menneskene frihet fra kaos, og på denne måten kan sikkerhet betraktes som en form for frihet. Dilemmaet som foreligger blir da hvor mye sikkerhet som skal etableres, samtidig som friheten til befolkningen opprettholdes. Så lenge ikke sikkerhetstiltakenes medfølgende konsekvenser rammer oss direkte blir slike tiltak lett akseptert i samfunnet, spesielt når det kommer til hendelser som eksempelvis terrorisme. Ettersom det for befolkningen ikke vil være noe sjanse for å forutse terrorisme er dette heller ikke en risiko man som enkeltmenneske kan kontrollere. På denne måten blir det lettere å godta tiltak myndighetene ønsker å innføre for å forhindre at det skjer. Lar man dette utfolde seg fritt kan dette gi en god grobunn for en kontrollkultur som vil gi overvåking i samfunnet en større gjennomføringskraft (Engen et al., 2016).

Foucault har dannet seg egne tanker om hva frihet innebærer. Definisjonen av governmentality som ‘conduct of conduct’ innebærer en antagelse om at den som styres er en aktør, og dermed besitter en grunnleggende frihet. Denne formen for frihet innebærer at de er

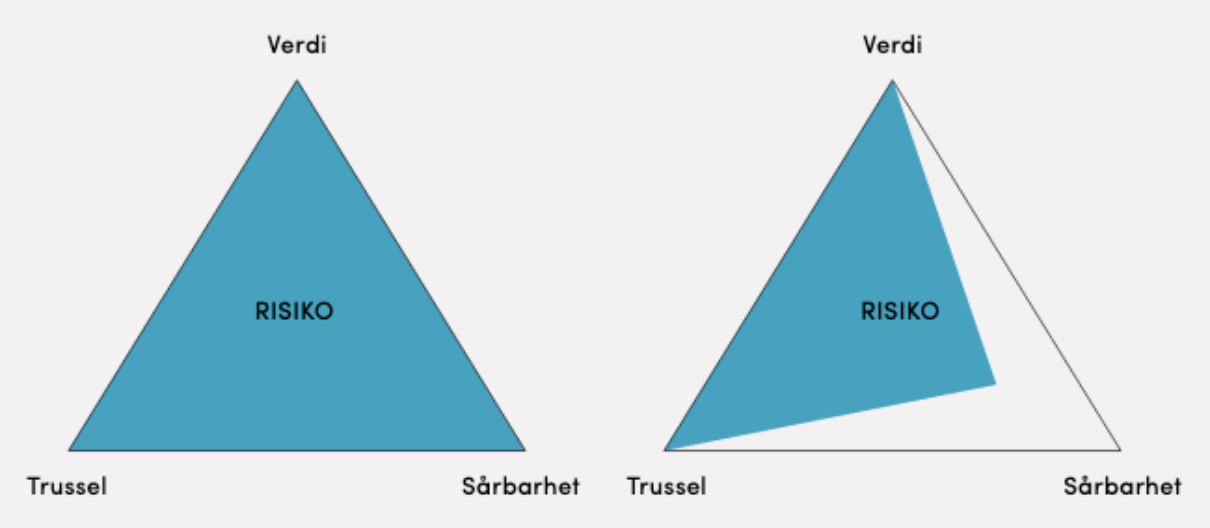
fri til å tenke og handle på ulike måter, selv på måter som styringsmyndighetene ikke nødvendigvis forventer (Dean, 2010). Liberalisme som en form for regjeringsregime ønsker å konstruere en verden som består av selvstyrte individer eller «frie subjekter», men Dean (2010) påpeker derimot at dette kun tydeliggjør ambivalensen i liberalismen når det kommer til det selvstyrte individet. Et subjekt sin frihet er en betingelse for underkastelse. Utøvelse av autoritet forutsetter at det eksisterer et fritt subjekt, med behov, ønsker, rettigheter, interesser og valg. Men, subjektets underkastelse er også en betingelse for frihet: «In order to act freely, the subject must first be shaped, guided and molded into one capable of responsibly exercising that freedom through systems of domination» (Dean, 2010, s. 193). Det Dean (2010) mener med dette er at de liberale styreformene vil arbeide for å styre og organisere forholdene som er nødvendig for at mennesket kan være 'fritt'. Det liberalistiske fokuset på det frie individet er dermed en hjørnestein i forståelsen av governmentality.

3.2 Risiko

Risiko er noe som forekommer rundt oss til en hver tid. Helt generelt kan det forstås som en usikkerhet om hva som blir konsekvensene eller utfallene av en gitt aktivitet (Aven et al., 2004). Dette innebærer altså at hendelser som har konsekvenser for noe som er av verdi for oss mennesker kan inntreffe (Aven, 2019). Individer, organisasjoner og samfunn vil alltid stå overfor et stort antall valgmuligheter som kan ha utallige utfall, og er derfor alltid nødt til å handle med en viss risiko involvert.

3.2.1 Trefaktormodellen

Norsk Standard 5830:2012 definerer risiko som et «uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen» (Standard Norge, 2012). Dette beskrives ofte som trefaktormodellen og kan dermed forstås som en kombinasjon av verdier vi ønsker å verne, trusler som kan ramme disse verdiene og sårbarheten verdiene har i forhold til de aktuelle truslene. Her nevnes ikke sannsynlighet direkte, men er implisitt med i trusselvurderingen. Årsaken til at sannsynlighet for forekomst av hendelsen er utelatt er at det er en fare for at hendelser med lav sannsynlighet og stor konsekvens, som terrorangrep, får for lav skåre i en risikomatrise og dermed blir nedprioritert når det kommer til fordeling av beredskapsressurser.



Figur 1. Trefaktormodellen (NSM, 2015, s. 10).

Formålet med forebyggende sikkerhet er å verne om samfunnets verdier. En verdi kan defineres som «en ressurs som hvis den blir utsatt for en uønsket påvirkning vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen» (NOU 2016: 19, s. 44; Standard Norge, 2012). Norge har flere verdier som ondsinnede aktører kan ønske å skade. Dette kan være både verdier av materiell og ikke materiell art, eksempelvis informasjon og sensitiv data, opprettholdelsen av kritisk infrastruktur eller menneskeliv. Disse verdiene ønsker vi å verne fra ulike trusler. En trussel kan defineres som «en mulig uønsket handling som kan gi en negativ konsekvens for en entitets sikkerhet» (NOU 2016: 19, s. 49; Standard Norge, 2012). Trusler kan sees på som en negativ endring i en eller flere av sikkerhetsmålene konfidensialitet, integritet og tilgjengelighet, og kan for eksempel være terror, spionasje, sabotasje, cyberangrep eller annen kriminalitet. Ulike aktører vil ha ulik kapasitet og intensjon, og dette tas det en vurdering av når man gjennomfører en trusselvurdering. I informasjonssamfunnet vi lever i kan trusler og trusselaktører utvikle seg raskt. Dette vil diskuteres videre i kapittel 5.1.1 og 5.1.2 Sårbarhet kan defineres som «manglende evne til å motstå en uønsket hendelse eller å opprette ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning» (Standard Norge, 2012). Det omhandler altså hvor mye av en tilsiktet, uønsket handling en trusselaktør kan utføre uten å bli stanset. Her kommer det an på hvilke tiltak som er iverksatt for å forhindre handlingene eller hvilke tiltak som kan iverksettes for å forminske skadene et angrep kan føre til (Busmundrud et al., 2015). En trusselaktør vil kunne utnytte slike sårbarheter, enten om de er menneskelige, teknologiske eller organisatoriske. Sårbarhetsbildet i samfunnet blir stadig mer komplekst, mye grunnet at befolkningen i økende grad blir avhengig av et større utvalg digitale tjenester (NSM, 2020).

Mengden verdier blir dermed større, og således fører det til økt sårbarhet om det skulle forekomme svikt i en av disse tjenestene (NOU 2016: 19, s. 66). Økt digitalisering medfører på denne måten en økt risiko, både for samfunnet, virksomheter og individet, da mer og mer av samfunnets verdier befinner seg i det digitale rom (NSM, 2020).

3.2.2 Realisme og konstruktivisme

"Nothing is a risk in itself; there is no risk in reality. But on the other hand, anything can be a risk; it all depends on how one analyses the danger, considers the event" (Dean, 2010, s. 206).

For å forstå risiko er det nødvendig å diskutere hvorvidt risiko oppfattes som sosialt eller kulturelt konstruert, eller om risiko er noe som til enhver tid eksisterer. Det skilles gjerne mellom et realistisk og et konstruktivistisk syn på risiko. Mens det realistiske perspektivet går ut på at risiko eksisterer uavhengig av mennesket, baserer det konstruktivistiske perspektivet seg på at risiko er en sosial konstruksjon som dermed vil avhenge av oppfatningen til mennesket som blir utsatt for risikoen. Realister ser dermed på risiko som en objektiv trussel eller fare som eksisterer, mens risikoen innenfor sterk konstruktivisme skapes av de preferanser og forventninger som finnes innenfor en kultur eller sosiale konvensjoner (Douglas & Wildavsky, 1982). Forholdet mellom realisme og konstruktivisme kan sees på som en skala som består av glidende overganger fra «sterk realisme» til «sterk konstruktivisme». Douglas og Wildavsky med sin kulturelle teori om risiko, Luhmann sin teori om sen-modernitetens selvmotsigelse og Foucault og governmentality er noen eksempler på forskere som stort sett har jobbet innenfor en retning med et sterkt konstruktivistisk syn på risiko (Engen et al., 2016).

I denne oppgaven vil det i stor grad lagt vekt på et konstruktivistisk perspektiv på risiko. Risikoen for terrorangrep i et liberalt demokrati som Norge er både reell og er en trussel som er nødt til å håndteres. Hvordan dette håndteres og hvilke effekter dette har er dermed nødt til å bli underlagt fokus. Risikopersepsjonen til samfunnet vil være formet av kulturen de er en del av og de medfølgende sosiale konvensjonene. Menneskets persepsjon blir påvirket av det som skjer rundt en. Dette kan medføre et urealistisk syn på den faktiske risikoen, men kan likevel påvirke politikere sine beslutninger rundt risiko og medfølgende sikkerhet. Denne formen for risiko reflekterer hva mennesker observerer i virkeligheten og hva de erfarer, altså konstrueres individers risikopersepsjon gjennom sosiale interaksjoner og inntrykk (Clarke & Short, 1993).

3.2.3 Governmentality og risiko

Det sosialkonstruktivistiske perspektivet på risiko fremmet av Foucault har generert betydelige krusninger i kriminalitetsstudier. Selv om risiko ikke var i hjertet av teorien til Foucault, har teorien hans om governmentality de siste tiårene blitt utvidet til å imøtekomme måtene risikoen blir tenkt på og mobilisert i liberale samfunn. Governmentality som både et sett med organiserte praksiser og som et veiledende rasjonale har vært en grunnleggende del av politisk makt siden 1700-tallet. Risiko ble sett på, i et foucauldiansk perspektiv, som en ny form for styring, som ikke tok i bruk tvang for å kontrollere befolkningen, men heller styring gjennom statistiske fordelinger. Ved utviklingen av statistikk ble kategorier som «befolkning» og «økonomi» dannet, og det var ikke lengre nødvendig med den individuelle dominansen som tidligere utgjorde disiplin (Mythen & Walklate, 2006). Kunnskap om befolkningen gjorde på denne måten regulering av atferd mulig. Risikobasert styring kan anses å være mindre dominerende enn styring gjennom suverenitet eller disiplin. Et eksempel er utviklingen av fartsovertredelser. Kun i ekstreme tilfeller vil sjåføren bli straffet med fengsel – de aller fleste får bøter i stedet. Sjåførene kan på denne måten fortsette å bryte reglene, men boten setter en pris på slik aktivitet. Ettersom målet er å minimere risikoen for skade og død vil ikke denne atferden bli tolerert for alltid, og vil dermed bli straffet på en annen måte, ved for eksempel tap av førerkortet sitt (O'Malley, 2016). Gjennom implementering av disiplinære praksiser, som eksempelvis fartsbøter, helseforsikringer, straffeutmåling eller overvåking fra myndighetene, gir risiko en måte å organisere tid og rom på, for å kunne styre fremtiden (Mythen & Walklate, 2006). Governmentality-grenen har dermed undersøkt hvordan det liberale demokratiet har beveget seg fra en kollektiv til en mer individualistisk risiko, der hver enkelt borger får større ansvar for sitt eget liv.

3.3 Begrepsavklaring

3.3.1 Samfunnssikkerhet og statssikkerhet

Sikkerhet kan på engelsk ha to ulike betydninger; *safety* eller *security*. På norsk eksisterer det kun ett begrep som omfatter de to ulike forståelsene av sikkerhet. I denne oppgaven vil begrepet sikkerhet innebære tilsiktede, ondsinnede handlinger, som eksempelvis terrorisme.

Begrepet sikkerhet innebærer mye forskjellig. I Norge kan begrepet deles inn i fire ulike typer: samfunnssikkerhet, statssikkerhet, menneskelig sikkerhet og økonomisk trygghet. Figur

2 viser til de ulike nivåene av sikkerhet vi har i Norge. I denne oppgaven er begrepene samfunnssikkerhet og statssikkerhet relevant.

Figur 2. Nivåer av sikkerhet (NSM, 2015, s. 9).

Statssikkerhet innebærer tradisjonelt sett ivaretakelse av suverenitet, territoriell integritet og politisk handlefrihet, og aktørene som jobber med dette er hovedsakelig innenfor forsvaret til en stat. Ting som kan utfordre statssikkerhet er blant annet væpnet angrep, politisk og militært press mot politiske myndigheter og alvorlige anslag mot norske interesser fra statlige eller ikke-statlige aktører. Når slike trusler forekommer kan bruk av militære og andre ressurser legitimeres (NOU 2016: 19). Samfunnssikkerhet handler på en annen side mer om trygghetsfølelsen til befolkningen, ivaretagelse av deres liv og helse, sikring av sentrale samfunnsinstitusjoner og viktig infrastruktur (Kveberg & Johnsen, 2013). Samfunnssikkerhet kan dermed defineres som:

> vern av samfunnet mot hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være et utsalg av tekniske eller menneskelige feil eller av bevisste handlinger. (NOU 2016: 19, s. 29).

Tradisjonelt sett regnes ikke statssikkerhetsbegrepet som en del av samfunnssikkerheten. Begrepene har derimot sklidd mer over i hverandre de siste tiårene og det foreligger stadig flere gråsoner og sammenfallende interesser mellom samfunnssikkerhet og statssikkerhet. På

bakgrunn av den økende digitaliseringen i samfunnet øker også de tverrsektorielle avhengighetene og blir mer komplekse, noe som påvirker sårbarheten i samfunnet. Dette medfører et mer sammensatt risiko- og trusselbilde enn tidligere (Størdal, 2016).

3.3.2 Terrorisme

Terrorisme kan beskrives som noe som er sosial konstruert. Begrepet er i endring hele tiden, og tiltakene som innføres i samfunnet er preget av hvordan begrepet forstås (NOU 2017: 9). Straffeloven § 131 definerer terror som

> en handling som begås med hensikt å a) alvorlig forstyrre en funksjon av grunnleggende betydning i samfunnet, b) skape alvorlig frykt i en befolkning, eller c) urettmessig tvinge offentlige myndigheter eller en mellomstatlig organisasjon til å gjøre, tåle eller unnlate noe av vesentlig betydning for landet eller organisasjonen, eller for et annet land eller en mellomstatlig organisasjon. (DSB, 2019, s. 175).

Terrorisme har vært et fenomen i lang tid, og har gjennom tidene blitt brukt med forskjellig formål. Fra myndigheter har terrorisme blitt brukt for å presse befolkningen til underkastelse, mens fra ikke-statlige aktører har heller formålet vært å påvirke myndigheter eller ramme et helt maktapparat. Terrorhandlinger har dermed også en politisk dimensjon. Ikke-statlige aktører forholder seg ikke til konvensjoner på samme måte som stater, og retter seg dermed i stor grad mot «myke mål» som ikke er omkranset av høy sikkerhet, som for eksempel sivilbefolkningen (NOU 2016: 19). For at voldsbruken skal få ønsket effekt fra en terrorist sitt ståsted er også dekning gjennom mediene viktig, noe både TV-mediet, internett og sosiale medier har bidratt til (DSB, 2019). Det har også vokst frem en ny form for terrorisme i senere tid, nemlig det man kaller digital sabotasje eller cyberterrorisme. Cyberterrorisme er et forholdsvis nytt begrep og det foreligger fremdeles stor uenighet rundt hva begrepet skal innebære og om cyberterror faktisk er en trussel. Flotz (2004) gjengir en definisjon av cyberterrorisme som innebærer trusselaktørenes intensjon, formål og objekter som blir brukt i angrepet:

> Cyberterrorisme kan sees på som konvergensen mellom terrorisme og cyberspace. Dette innebærer ulovlige angrep og trusler om angrep mot datamaskiner, nettverk og informasjonen som er lagret der, når angrepene blir gjennomført for å skremme eller

> tvinge en regjering eller befolkningen til fremme politiske og sosiale mål. (Flotz, 2004, s. 154, egen oversettelse).

Begrepet har blitt diskutert siden slutten av 1990-tallet etter USA hadde blitt utsatt for en rekke terrorangrep, og det er gjennomført mange studier for å finne ut hva cyberterrorisme innebærer. Et av de største studiene som er gjennomført rundt cyberterrorisme til dags dato ble gjennomført i 1999 for US Defense Intelligence Agency. Her ble cyberterrorisme definert som: «Ulovlig ødeleggelse eller forstyrrelse av digital eiendom, gjennomført for å skremme eller tvinge regjeringer eller samfunn i jakten på politiske, religiøse eller ideologiske mål». (Soesanto, 2020, s. 2). Det er dermed flere definisjoner på begrepet cyberterrorisme, og fra et rent strategisk perspektiv kan cyberterror forklares som et domene (cyber) og en motivasjon (terrorisme). Begrepet er ikke alltid klart da verken domenet eller motivasjonen ikke nødvendigvis blir kjent ved første øyekast. Gode eksempler er hvordan Russland to ganger har slått ut det ukrainske strømnettet ved hjelp av digitale våpen, hvordan USA både har funnet kinesisk og russisk skadevare i sine strømnett (Friis & Hansen, 2020) eller Stuxnet – den avanserte dataormen som angrep iranske atomanlegg på en så intrikat måte at det tok flere måneder før et angrep i det hele tatt ble mistenkt. Ormen har blitt kalt for et militært cyber-supervåpen (Hamnes, 2010). Slike cyberangrep mot blant annet kritisk infrastruktur eller andre industrielle systemer starter med et innbrudd som gjør det mulig for en trusselaktør å få fotfeste i nettverket, før de deretter kan gjøre mer skade. Hendelser som dette vil være vanskelig å vite at er knyttet til et cyberangrep før det blir gjennomført en etterforskning. Om det så blir klart gjennom en etterforskning at det er et cyberangrep vil det muligens ta dager, uker eller måneder, om noensinne, før det blir klart at det er terror som har skjedd (ISE Bloggers, 2017).

3.4 Oppsummering av teori

I dette kapittelet har det blitt redegjort for det teoretiske fundamentet i oppgaven. Begge teoriene, governmentality og risiko, vil bli brukt gjennomgående i drøftingskapittelet for å besvare problemstilling og tilhørende forskningsspørsmål. Da begrepene i stor grad beveger seg over i hverandre vil de også bli tatt i bruk på denne måten, da de på hver sin måte belyser flere av de samme funnene i oppgaven. Selv om risiko aldri var hovedfokuset i Foucault sin teori, er det fremdeles svært relevant da governmentality i stor grad baserer seg på risikobasert styring, og det er den eksisterende risikoen i et samfunn som til slutt vil forme

befolkningen. Stats- og samfunnssikkerhet har gjennom årene også blitt formet av risikoen og den sikkerhetspolitiske situasjonen i samfunnet, noe som dermed også vil påvirke styringen. Dette blir forelagt et videre fokus i kapittel 5.2. Begrepene beskrevet i kapittel 3.3 vil bli brukt gjennomgående i både empiri- og drøftingskapittelet.

Kapittel 4. Metode

Denne oppgaven har til hensikt å undersøke hvordan overvåking som sikkerhetstiltak har utviklet seg de siste 25 årene og hvilke implikasjoner dette har for personvernet til individene i samfunnet. I denne delen av oppgaven er hensikten å legge frem det metodiske opplegget for oppgaven, og her vil det redegjøres for fremgangsmåten, hvilke valg som har blitt tatt, samt hvilke steg som har blitt tatt for å belyse problemstillingen. Problemstillingen «Hvilke implikasjoner har utviklingen av overvåking som sikkerhetstiltak hatt for personvernet de siste 25 årene?» legger føringer for hvilken metode som er hensiktsmessig å bruke. Det vil dermed bli brukt en kvalitativ forskningsmetode. Med grunnlag i at studien er en historisk tilnærming vil datainnsamlingen skje ved bruk av dokumentanalyse. Det vil først bli redegjort for denne metoden, deretter datainnsamlingen og videre legges fokuset på dataanalysen og forskningens kvalitetskriterier og begrensninger.

4.1 Metodisk tilnærming

4.1.1 Kvalitativ metode

Det finnes flere ulike forskningsmetoder. Innen samfunnsvitenskapelig metode jobber man med hvordan man skal gå frem for å finne informasjon om den sosiale virkeligheten, hvordan denne informasjonen skal analyseres og relasjoner og koblinger mellom fenomenene som oppdages. Det dreier seg dermed om å samle inn, analysere og tolke dataen. Innenfor samfunnsvitenskapene finnes det to ulike tilnærminger til hvordan dette gjennomføres, nemlig kvalitativ metode og kvantitativ metode. I denne oppgaven fokuseres det på å skape en dybdeforståelse av hvordan overvåking og personvern har utviklet seg de siste 25 årene, og det blir dermed tatt i bruk kvalitativ metode. Kvalitativ metode er en hensiktsmessig metode å velge om man skal undersøke fenomener som vi ønsker å forstå på et dypere nivå, eller at det er lite utforsket fra tidligere av (Johannesen et al., 2016). Kvalitativ metode innebærer både innsamling og generering av data. I denne oppgaven vil det kun bli tatt i bruk datainnsamling, altså dokumentanalyse. Når dokumentanalyse blir tatt i bruk i en kvalitativ setting er målet å identifisere fenomener og forbindelser blant disse (Blaikie & Priest, 2019). Dette vil utdypes videre i kapittel 4.2.1.

4.1.2 Forskningsdesign

Helt fra begynnelsen var ønsket for oppgaven å ha en fleksibel og åpen forskningsstrategi. På denne måten låses ikke den første ideen, og designet kan være eksplorativt i mye større grad. I

begynnelsen av prosessen ble det tatt utgangspunkt i ulike teoretiske bidrag som skulle bidra til å forme analysen av den innsamlede dataen. Underveis i prosessen til dataanalysen har det stadig dukket opp nye temaer, og på denne måten har nye teoretiske perspektiver blitt relevante. Dette tilsier at oppgaven ligger på et punkt mellom induktiv og deduktiv forskningsdesign, noe som Thagaard (2018) kaller for en abduktiv tilnærming. Induksjon innebærer at man jobber fra data mot teori, mens deduksjon går andre vei hvor man sjekker fra det mer teoretiske til det mer empiriske (Tjora, 2017). Et abduktivt forskningsdesign innebærer at dataen som samles inn både blir tolket i lys av allerede eksisterende teori, i tillegg til at dette også danner utgangspunktet for nye teoretiske perspektiv. Ønsket for oppgaven var som sagt å ha en åpen forskningsstrategi, og jeg ønsket dermed ikke å låse mitt metodiske utgangspunkt til verken ren induksjon eller ren deduksjon. Slik sammenfaller denne fremstillingen av et abduktivt forskningsdesign med tilnærmingen som har blitt tatt i bruk i løpet av forskningsprosessen.

4.1.3 Forskningsstrategi

Forskningsstrategi går ut på hvilke prosedyrer og teknikker som er tatt i bruk for å svare på oppgavens problemstilling og medfølgende forskningsspørsmål i løpet av forskningsprosessen. Prosessen består av ulike trinn som videre vil bli presentert i tabell 1. Her blir det gått gjennom hva som har blitt gjort i løpet av de ulike månedene masteren ble skrevet, og viser oversikten over hvilke steg som har blitt gjennomført for å svare på problemstillingen: «Hvilke implikasjoner har utviklingen av overvåking som sikkerhetstiltak hatt for personvernet de siste 25 årene?». Dette kan gi et inntrykk av hvor omfattende prosessen har vært, i tillegg til hvorfor og hvordan endringer har blitt gjennomført underveis. Det har altså ikke vært en lineær prosess for å nå oppgavens mål.

Når	**Hva ble gjennomført?**	**Hensikt**
Januar	Det ble utviklet en idé om problemstilling som omhandlet hvordan personvern ble ivaretatt i forhold til den nye etterretningstjenesteloven som ble vedtatt i 2020.	Ønsket var å komme i gang tidlig med prosessen i begynnelsen av januar, da det av erfaring kan det oppstå diverse problemer med utformingen av en idé.

Februar	I begynnelsen av måneden forstod jeg og veileder at det ble for vanskelig å løse den originale ideen til oppgaven, pga. at loven er under behandling fremdeles. Dermed ble det formet en ny problemstilling med medfølgende forskningsspørsmål i begynnelsen av måneden. Da begynte arbeidet med å utforme innledning og kontekst til oppgaven, og det ble besluttet at dokumentanalyse ville være den mest hensiktsmessige formen for datainnsamling i forhold til problemstillingen. Det ble også gjennomført litteratursøk. Arbeidet med teorikapittelet ble påbegynt i slutten av måneden.	Det ble utformet en ny problemstilling med hensikt om at det var nødvendig å finne noe som var gjennomførbart. Etter problemstilling og forskningsspørsmål ble dannet begynte jeg på innledning og kontekst for å utforme ideen videre. Ved å gjennomføre litteratursøk fikk jeg en god forståelse for hvilken litteratur som eksisterte fra før og hvordan jeg kunne ta denne i bruk videre i oppgaven, i tillegg til å øke min kompetanse og forståelse for temaet.
Mars	Etter veiledning ble det bestemt at teorikapittelet skulle skrives om og at det skulle fokuseres på governmentality som hovedteori. Teorikapittelet ble på nytt revidert og endret, samtidig som arbeidet med metodekapittelet ble startet. Det ble løpende samlet inn empiri gjennom måneden ved siden av arbeid med teorikapittel og metodekapittel.	Hensikten var å ferdigstille så mye som mulig for å kunne komme i gang med empiri og drøfting. Ved å få ferdigstilt teorikapittelet ble datainnsamlingen enklere å gjennomføre, ettersom det var mulig å snevre inn hvilken informasjon som ville bli nødvendig for å drøfte forskningsspørsmålene.
April	Teori- og metodekapittel ble ferdigstilt. Arbeidet med empiri- og drøftingskapittel fortsatte, og det ble tatt et valg om at funnene fra empiri og drøfting skulle presenteres i samme kapittel.	Ved å fortsette datainnsamlingen og begynne drøftingsprosessen samtidig ble det utformet nye ideer til hvordan analysen kunne se ut kontinuerlig.

Mai	Empiri og drøfting ble jobbet med simultant. Underveis i prosessen ble jeg innforstått med at resultatene ville ta seg bedre ut fordelt over to kapitler, og omskrivingsprosessen av kapitlene begynte. Det separate empirikapittelet ble ferdigstilt i løpet av måneden og arbeidet fortsatte videre med drøftingskapittelet.	Ønsket var å presentere resultatene på best mulig måte. Ved å strukturere empiri- og drøftingskapitlene på denne måten ble resultatene mer oversiktlige.
Juni	Drøftingskapittelet ble ferdigstilt i begynnelsen av måneden. I tillegg ble korrektur av oppgaven gjennomført, teksten ble moderert og irrelevante avsnitt ble fjernet slik at alt hang sammen.	Hensikten var å forsikre meg om at det forelå en rød tråd gjennom oppgaven og at uklarheter ble fjernet, før oppgaven ble ansett som ferdig skrevet.

Tabell 1. Månedlig fremdrift i forskningsprosessen.

4.1.4. Ontologi og epistemologi

Ontologi og epistemologi kan være begreper som ofte blir tatt for gitt når det kommer til samfunnsvitenskapelig forskning. Det eksisterer derimot veldig forskjellige oppfatninger av hva som er grunnleggende trekk ved den sosiale virkeligheten og begrepene bør dermed synliggjøres og settes fokus på. Ontologi refererer til den virkelighetsoppfatningen man har og beskrives som «læren om det som eksisterer». Epistemologi omhandler derimot hvordan man anskaffer seg kunnskap om denne verdenen. Det dreier seg om hva vi egentlig kan vite om virkeligheten og hvordan vi kan gå inn for å få kunnskap om samfunn og mennesker, noe som er veldig relevant for forskning. Ettersom mennesket og samfunn har ulike ontologier, vil det dermed også eksistere uenighet om hvordan man skal samle inn kunnskap om verden og om det i det hele tatt er mulig å danne seg en objektiv virkelighetsforståelse (Johannesen et al., 2016).

Ettersom den metodiske tilnærmingen i oppgaven er kvalitativ og dokumentanalyse er metoden for datainnsamling, vil måten dokumentene blir bearbeidet på være påvirket av min egen forståelse av hvordan verden ser ut. Implisitt i min tilnærming til forskningstemaet ligger derfor mitt ontologiske og epistemologiske perspektiv. Hvordan man tolker empiri kan i stor grad være påvirket av antakelser man besitter, og dermed vil det være viktig å begrunne konklusjonene man trekker. Analysen vil på denne måten i stor grad være preget av min egen virkelighetsoppfatning, i tillegg til metoden som har blitt anvendt for å samle inn datamaterialet. Dette gjelder også forfatterne av dokumentene tatt i bruk i dokumentanalysen, og det vil dermed være spesielt nødvendig å være kildekritisk til empirien som blir tatt i bruk i studien.

4.2 Datainnsamling

4.2.1 Dokumentanalyse

Johannesen et al. (2016, s. 99) definerer en dokumentanalyse som: «en type kvalitativ innholdsanalyse der forskeren samler inn data som analyseres for å få frem viktige sammenhenger og relevant informasjon om det eller de forholdene i samfunnet vi ønsker å studere». Slike dokumenter gir informasjon om en situasjon i fortiden, et saksforhold som er nedfelt i dokumenter fra et spesifikt tidspunkt og gjerne på et spesifikt sted. Slike dokumenter sier noe om forfatterne og deres virkelighetsforståelse, da de presenterer meninger og faktabeskrivelser som forfatterne ønsker å gjengi. Dokumentene som tas i bruk er dermed sekundærkilder, altså kilder som ikke er generert av forskeren selv og som ble skrevet for å brukes til et annet formål (Johannesen et al., 2016). En slik form for analyse tar gjerne utgangspunkt i at vi lever i en kultur som i stor grad baserer seg på skrevet materiale og andre former for dokumenter, og dokumenter vil på dette viset fungere som en organisasjons kollektive minne. Det vil dermed være fare for at en analyse som ikke inneholder dokumenter fra de relevante institusjonene vil fremstå som mangelfull (Syvertsen, 1998).

Dokumentanalyse er en hovedmetode for datainnsamling innen historieforskning, humaniora og samfunnsvitenskapen. Dokumenter er en bestemt type tekster, men innen dokumentanalysen regnes alt fra offentlige dokumenter som stortingsmeldinger og årsrapporter til nyheter, dagbøker, fotografier og brev som dokumenter (Johannesen et al., 2016). Audiovisuelle medier kan også være aktuelt som datamateriale i en dokumentanalyse, men vil ikke bli tatt i bruk i denne oppgaven. Det finnes flere ulike måter å kategorisere

dokumenter på. Noen former for distinksjoner kan være skrevne vs. audiovisuelle dokumenter, offentlige tilgjengelige dokumenter vs. hemmelige dokumenter, institusjonelle vs. private dokumenter, samtidige vs. retrospektive dokumenter osv. I denne studien vil det kun bli tatt i bruk skrevne, offentlige tilgjengelige, institusjonelle og samtidige dokumenter som analysemateriale (Syvertsen, 1998). De relevante dokumentene vil videre kun bli henvist til som *offentlige dokumenter*. Med offentlige dokumenter menes derfor ikke kun dokumenter som det offentlige (regjeringen og Stortinget) produserer. Samtidige dokumenter innebærer informasjon som beskriver situasjonen slik den fremstod da dokumentet ble publisert, og er dermed ikke samtidige i den forstand at de ble produsert nylig.

Å bruke offentlige dokumenter som sitt viktige kildemateriale har flere fordeler. Ofte er offentlige dokumenter den eneste kilden til innsikt om mange saksforhold, det er en god måte å verifisere informasjon som er samlet inn under andre forhold, de er lett tilgjengelige og krever ikke noe spesielt utstyr og det er mye materiale å ta av. Det er i tillegg en fordel at offentlige dokumenter med hovedsak er produsert kontinuerlig, og er dermed forholdsvis like fra utgave til utgave. Dette gjør de godt egnet til å dokumentene en utvikling over tid (Syvertsen, 1998). I tillegg egner en slik metode seg godt når det er vanskelig å samle inn primærdata direkte fra kildene (Grønmo, 2016). Da denne oppgaven er en historisk tilnærming til overvåking og personvern ville det vært problematisk å kun samle inn primærdata fra ulike kilder. Kildene ville da ha vært nødt til å huske ulikhetene og utviklingen fra år til år, noe som ville vært utfordrende for enhver. Ved å ta i bruk offentlige dokumenter i form av offentlige utredninger, stortingsmeldinger, trusselvurderinger og lignende, opprettes det en direkte kobling til årstallet rapporten ble publisert.

4.2.2 Utvalg

Når en studie som dette skal gjennomføres er det mulig at det gjøres på et rent teoretisk grunnlag. Det er allikevel nødvendig, som med alle andre former for data, å være kildekritisk. Syvertsen (1998) skriver at det første steget man er nødt til å gjennomføre er å anslå dokumentets autentisitet. Når det kommer til offentlige dokumenter, slik som datautvalget for denne analysen er, er dette sjeldent et problem. Det er allikevel flere spørsmål forskeren kan stille for å sjekke autentisiteten til dokumentene som er valgt ut:

Hva er dokumentets hensikt? Hvorfor er det utgitt? Hva vil avsender oppnå?

Hvem har vært ansvarlig for å innhente informasjon? Kommer informasjonen fra partsrepresentanter eller mer uavhengige kilder?
Hva slags informasjon er samlet inn? Hva var mandatet, hvordan ble nøkkelbegrepene definert osv. Hva slags informasjon falt utenfor mandatet?
Når ble informasjon samlet inn? Er dataene fortsatt gyldige eller har de primært historisk interesse?
Hvordan ble opplysningene samlet inn? Metode? Reliabilitet? Validitet?
I hvor stor grad stemmer opplysningene fra denne kilden med opplysninger fra andre kilder?

Tabell 2. Sjekkliste med spørsmål (Syvertsen, 1998, s. 10).

En av grunnene til at flere av disse stadiene er viktig å gjennomgå er reliabiliteten til opplysningene i dokumentene. Offentlige dokumenter inneholder mye fakta, blant annet statistikk og annet tallmateriale, og feilsitering eller regnefeil kan forekomme. Når det skal gjennomføres en dokumentanalyse er det dermed nødvendig at man ser kritisk på fakta. Skal statistikk gjengis er det nødvendig å vurdere beregningsgrunnlaget til de som har produsert det. Dette gjelder også for datamateriale i tekstform. I dokumentanalyse er dermed kritisk vurdering, samt sammenkobling fra flere kilder en forutsetning. Sammenkobling fra flere kilder omhandler at det er nødvendig å la ulike kilder supplere og utfordre hverandre. Målet er dermed ikke å finne én god kilde og utnytte den for alt det er verdt. Ofte vil ulike institusjoner, organisasjoner og enkeltpersoner ta i bruk dokumenter for å fremstille seg selv i best mulig lys. Offentlige dokumenter vil dermed ikke nødvendigvis alltid presentere et nøyaktig bilde av hvordan en organisasjon fungerer eller i hvilken grad den oppfyller sine målsettinger. Dokumenter, som alle andre datainnsamlinger, presenterer dermed én versjon av virkeligheten (Syvertsen, 1998).

De intenderte mottakerne eller målgruppen til dokumentene er også nødvendig å vurdere når det skal gjennomføres en dokumentanalyse, ettersom det vil virke styrende for et dokument sin utforming. Eksempelvis vil en nyhetsmelding på radioen rette seg til allmennheten og dermed ha en form som er beregnet på et stort publikum. Trusselvurderinger derimot vil for eksempel i stor grad være rettet mot myndighetene og menneskene med beslutningsmyndighet som tar avgjørelser som påvirker institusjonene ansvarlig. Alle som

skriver dokumenter er på den andre siden klar over at mennesker utenfor målgruppen også vil lese dokumentet og dermed tilrettelegge slik at andre, være seg forskere, frivillige organisasjoner eller lignende vil få et godt inntrykk av organisasjonen.

I denne studien utgjør dokumentene hele det empiriske materialet, og det er dermed nødvendig at det har vært en systematisk innsamling av dokumenter. Problemstillingen knytter seg til en utvikling som har foregått de siste 25 årene, og det sier seg dermed selv at det ikke er representativt å ta i bruk én trusselvurdering for å vurdere hvordan trusselbildet i Norge har utviklet seg. Derfor har et representativt utvalg av alle tilgjengelige dokumenter blitt inkludert i punktene der utviklingen står i fokus. En av utfordringene som oppstår med dette er at det blir store mengder datamateriale. Dette kan løses ved enten å forkorte tidsperioden som skal analyseres eller så kan problemstillingen avgrenses. Avgrensningen for hvilken empiri som er relevant er redegjort for i kapittel 1.2.

4.2.3 Dokumenter

I denne studien har det blitt gjennomført en omfattende datainnsamling og dokumentstudien er bygget opp av totalt 59 ulike dokumenter. En rekke ulike dokumenter har blitt brukt der nasjonale trusselvurderinger, offentlige utredninger, spørreundersøkelser og proposisjoner utgjør hovedvekten. I tillegg har også medieartikler, Stortingsmeldinger og andre former for rapporter blitt inkludert. Av dokumentene tatt i bruk er 18 trussel- og risikovurderinger, 10 offentlige utredninger, 7 proposisjoner, 7 spørreundersøkelser, 7 andre former for rapporter og 10 andre former for dokumenter. Dokumentene tatt i bruk er listet opp i vedlegg 1.

Det er mange ulike måter å tolke og analysere kvalitative data på (Johannesen et al., 2016). I begynnelsen av datainnsamlingen ble det besluttet at dataprogram, som eksempelvis NVivo, ikke skulle tas i bruk til bearbeidingen av data. På bakgrunn av at det tidlig ble besluttet at forskningsspørsmålene kunne tas i bruk som overordnede kategorier i både empiri- og drøftingskapittelet, ble det ikke ansett som nødvendig. Det ble dermed viktig å finne en annen måte å redusere informasjonsmengden på – et rammeverk for å kunne formidle innholdet på en forståelig måte. Første steg ble dermed å organisere data etter tema. Da empiri- og drøftingsdelen allerede var delt opp etter forskningsspørsmålene ble det lettere å systematisere datamaterialet. Videre ble datamaterialet som var plassert under hvert forskningsspørsmål kategorisk inndelt. Det vil si at det ble laget kategorier over ulike temaer som gikk inn under de ulike forskningsspørsmålene. På denne måten ble mengden informasjon redusert i stor

grad. Koding ble tatt i bruk som en ekstra reduksjonsteknikk, i tillegg til at det ble brukt til å identifisere mønstre i datamaterialet (Johannesen et al., 2016). Når det tas i bruk koding vil det være viktig å være bevisst på forskerens ontologi. Denne kan medføre at retningen til analysen blir påvirket og medføre at analyseprosessen ikke blir fullstendig objektiv.

4.3 Kvalitetskriterier

For å vurdere kvaliteten på forskningen brukes det ofte tre ulike kvalitetskriterier; reliabilitet, validitet og overførbarhet (Johannesen et al., 2016).

4.3.1 Reliabilitet

Reliabilitet handler kort fortalt om hvorvidt forskningen er troverdig og til å stole på (Jacobsen, 2015). Målet er å produsere et konsistent resultat, basert på hvilken forskningsmetode som blir tatt i bruk (Blaikie & Priest, 2019). Fullstendig nøytralitet vil være umulig å oppnå innen den kvalitative metoden, da metoden er avhengig av tolkning og analysering fra forskeren. Det vil derfor være viktig å være bevisst på egen erfaringsbakgrunn, da ingen andre har den samme. Forskerens erfaringsbakgrunn kan sees på som støy, men er også en helt nødvendig ressurs når det kommer til å forklare hvordan det kan påvirke analysen av dataen og diskusjonen av resultatene. I stedet for å problematisere det må det redegjøres for hva som er datagenerering og hva som er forskerens egne analyser (Tjora, 2017). I denne studien er temaet som undersøkes overvåking fra myndighetene, hvordan dette har endret seg og personvernets rolle. Temaet er valgt ut på bakgrunn av forskerens egne interesser, og vil dermed påvirke reliabiliteten til studien. Ved å redegjøre for eget forhold til temaet overvåking, samt interessen for personvern, og ved å ta det i betraktning i løpet av forskningsprosessen, vil det kunne minimere mulige effekter det vil ha på forskningen.

4.3.2 Validitet

En studies validitet handler om at problemstillingen og det påfølgende datamaterialet besvarer det det søker å besvare (Tjora, 2017). Dette er sentralt når det kommer til all forskning. En av ulempene når det kommer til å ta i bruk en abduktiv forskningsstrategi er at det ikke eksisterer faste kriterier for å måle validiteten til konklusjonen en kommer frem til (Danemark et al., 1997). For å styrke validiteten til et forskningsprosjekt må det tydeliggjøres hvordan forskningen skal gjennomføres, basert på spørsmålene vi stiller og hvordan disse formes med

utgangspunkt i temaene som ønskes utforsket. I løpet av forskningsprosessen har problemstillingen og forskningsspørsmålene måtte blitt endret flere ganger. Det er ikke uvanlig i forskningsprosjekter at dette må justeres underveis og gjerne i møte med feltet man studerer. Når dokumentanalysen ble gjennomført har det dukket opp nye temaer og sårbarheter som forsker ikke har vært klar over. Dette har ført til at forskningsspørsmål og analyse har hatt behov for å bli moderert gjennomgående i løpet av prosessen.

For å øke validiteten har det også bli tatt i bruk tidligere forskning og faglitteratur fra samme felt, som vil støtte opp under funnene fra datainnsamlingen. Dette bidrar med å skape et solid fundament og støtter i tillegg opp under de empiriske funnene i studien. En utfordring som har dukket opp underveis er at alle dokumentene som er tatt i bruk er offentlige, tilgjengelige dokumenter. Innenfor overvåking er det mye hemmelighold og hemmelighetsstemplede dokumenter. En av årsakene til dette er at offentlig tilgang til disse kan øke sårbarheten for angrep mot Norge. Det dette betyr er at det er tilbakeholdt store mengder med informasjon i de offentlige dokumentene, og vil i sin tur påvirke validiteten til studien.

4.3.3 Overførbarhet

Overførbarhet kan også omtales som «ekstern validitet» og omhandler studiens relevans utover de enheter som faktisk er undersøkt (Tjora, 2017). Dette er et mål innenfor det meste av samfunnsforskningen, men det forekommer uenighet blant forskere om hvordan dette best mulig skal gjennomføres. Overførbarhet vil i denne situasjonen innebære overføring av kunnskap heller enn generalisering, noe som omhandler hvorvidt det lykkes å etablere beskrivelser, begreper, fortolkninger og forklaringer som er nyttige for andre områder enn kun det som studeres (Johannesen et al., 2016). Prosjekter som kun ønsker å løse eller belyse et spesifikt problem, som casestudier, ser ofte bort fra overførbarhet. Om ønsket derimot er å utvikle innsikt som går ut over ett spesifikt case vil det være et mål (Tjora, 2017), noe som gjelder den aktuelle studien. Studien har store avgrensninger og også begrensninger, som vil påvirke i hvilken grad god overførbarhet er mulig å oppnå. Det er både slik at det kun blir tatt i bruk offentlige dokumenter, i tillegg til at det ikke er mulig å bruke all offentlig informasjon som eksisterer rundt temaet. Mye informasjon er også taushetsbelagt og gjør dermed at store deler av informasjonsgrunnlaget ikke er mulig å inkludere i oppgaven. Utviklingen av risikobildet i Norge og sammenhengen med relevant lovverk eller endringen av ansvarsområdene til maktinstansene i samfunnet er derimot eksempler på temaer som kan tas

i bruk på andre fagfelt enn kun det som forskes på i denne oppgaven, og målet vil dermed være å oppnå en høy grad av overførbarhet innenfor disse temaene.

4.4 Metodiske styrker og svakheter

Først og fremst ville det kunne styrket noen sider av metoden å inkludere intervjuer som en del av datagenereringen. Ved at jeg som forsker kun har tatt i bruk dokumentanalyse, kan det raskt føre forskningsprosessen i en bestemt retning, bevisst eller ubevisst. Ved å danne kategorier fra dokumentanalysen, forme intervjuguide ut fra dette og deretter ta i bruk intervjuer som en andre datainnsamlingsmetode, ville min entydige tolkning som forsker blitt nøytralisert ved bruk av intervjuer. Ettersom studien vil se på utviklingen til overvåking som sikkerhetstiltak og personvern de siste 25 årene, mener jeg allikevel at intervjuer ikke ville styrket empirien betraktelig. Da jeg har vært bevisst på min egen erfaringsbakgrunn gjennom hele prosessen, vil det minimere sjansen for at den former retningen til studien i betydelig grad. Bruk av intervjuer har dermed blitt ansett som unødvendig for å svare på forskningsspørsmålene. Å ta i bruk intervjuer i tillegg til dokumentanalysen kunne også muligens ha overskygget funnene fra dokumentene. Utvalget av representanter ville trolig vært forholdsvis lite, og deres personlige meninger ville dermed kunne tatt større plass enn det som er ideelt i et forskningsprosjekt med historisk tilnærming.

I dokumentanalysen har det blitt inkludert både offentlige, tilgjengelig dokumenter, men også ulike medieartikler. Det har vært nødvendig for meg som forsker å være bevisst på hvordan forfatterne og journalistene har vinklet innholdet i sine dokumenter, da det ofte kan ligge et politisk motiv i grunn for utformingen. Offentlige dokumenter er i stor grad ofte utformet av myndighetene selv, og kan dermed være påvirket av i hvilket lys de ønsker å bli sett i av befolkningen. Mediehus er også ofte formet av et politisk perspektiv, som i stor grad kan påvirke hvordan artiklene er utformet.

I tillegg kunne bruk av mixed methods, nemlig en kombinasjon av kvalitativ og kvantitativ metode, vært en mulig måte å løse prosjektet på. Bruk av spørreundersøkelser kunne eksempelvis ha gitt en mye bredere innsikt i hvordan befolkningen opplever fenomener, men ville dermed gitt et annet svar enn det problemstillingen spør om. Dette ville derimot vært en spennende tilnærming til videre forskning. Samtidig har det blitt tatt i bruk større spørreundersøkelser som datamateriale (se vedlegg 1), men en kvantifisering av resultater fra

disse ville også falt utenfor problemstillingen og ville dermed trolig ikke styrket empirien i særlig stor grad.

At datamaterialet ble inndelt etter forskningsspørsmålene tilsier at kategoriene allerede er forhåndsdefinerte, noe som kan medføre utfordringer når det skal gjennomføres en åpen datainnsamling. For å løse denne utfordringen har det derimot blitt dannet kategorier under forskningsspørsmålene underveis i analysen, samtidig som det har blitt endret på gjeldene kategorier om det viser seg at dette genererer bedre materiale.

Kapittel 5. Empiri

I dette kapittelet vil oppgavens empiri presenteres, gjennom datamaterialet fra dokumentanalysen. Kapittelet er inndelt etter forskningsspørsmålene og utgjør dermed strukturen for diskusjonen. Datamaterialet som blir presentert er basert på 59 dokumenter, som presentert i vedlegg 1. Dette skal bidra til å svare på problemstillingen som lyder som følger:

Hvilke implikasjoner har utviklingen av overvåking som sikkerhetstiltak hatt for personvernet de siste 25 årene?

5.1 Hvordan har overvåking forandret seg de siste 25 årene?

5.1.1 Det nasjonale risikobilde

For å få et overblikk over hvordan overvåking som sikkerhetstiltak har forandret seg vil det være nødvendig å legge frem hvordan det nasjonale risikobilde i Norge har utformet seg i tiden etter 1996. Ulike utredninger viser at det har vært en generell nedgang i kriminalitetsnivået i Norge siden midten av 90-tallet, på lik linje med kriminalitet i resten av den vestlige verden (Meld.St. 29 (2019-2020); NOU 2017: 9). Tradisjonelt sett har Norge vært et land med en relativt lav grad av politisk motivert vold og terrorangrep, men med samfunnets stadig større avhengighet til teknologi øker også den medfølgende sårbarheten.

Det var for alvor i 2001 at terrorisme ble satt på verdenskartet etter historiens mest omfattende terrorangrep ble utført mot de to tårnene i World Trade Center 11. september. Nasjonal sikkerhetsmyndighet (NSM) trakk i risikovurderingen for 2003 frem terrortrusselen mot Norge og norske interesser som lav, men at den fremstod som mer aktuell mot vår nasjonale sikkerhet enn tidligere (NSM, 2003). Det siste året har det blitt skildret i både PST sin trusselvurdering og NSM sin risikovurdering at trusselen anses som høy, og at det regnes som en mulighet at det vil bli gjennomført terrorangrep på norsk jord i løpet av året (NSM, 2021; PST, 2021). Alene gir dette et overordnet inntrykk om at det nasjonale risikobilde har utviklet seg i stor grad de siste 20 årene. I 2003 vurderte NSM at terrorangrep i all hovedsak ble gjennomført ved bruk av tradisjonelle virkemidler, som eksempelvis bruk av sprengstoff (NSM, 2003). Denne metoden ble også regnet som den dominerende angrepsmetoden i risikovurderingen fra 2005 (NSM, 2005). Utover 2000-tallet var det derimot terrorrelatert

støttevirksomhet som blant annet finansiering, og mennesker som utgjorde ordensproblemer, som fremstod som mest relevant i forhold til den norske terrortrusselen (PST, 2010).

Terrorangrepene som tok sted i Madrid 2004 og London 2005 styrket oppfatningen om at risikoen for terrorangrep i vestlige land i Europa var større enn tidligere antatt. I NSMs risikovurdering fra 2005 legges det vekt på at det tidligere var territoriell integritet som har vært beskyttelsesverdig for Norge, men at det, grunnet en utvikling i trusselbildet, ikke lengre var dette som ble regnet som hovedmålet for terroranslag (NSM, 2005). Norges sikkerhetsinteresser ble derfor vurdert til å omfatte kritisk infrastruktur, innenfor blant annet vitale samfunnsfunksjoner som energi- og matforsyning, samferdsel, telekommunikasjon, helseberedskap, samt bank- og pengevesen (NSM, 2005).

I 2010 vurderte NSM at både verdiene vi ønsker å beskytte, truslene mot disse verdiene og sårbarhetene knyttet til dette er i kraftig økning. I tillegg ble det vurdert at tiltakene for reduksjon av disse sårbarhetene ikke utvikles i samme takt som truslene (NSM, 2010). Dette ble terrorangrepet 22. juli 2011 et tydelig eksempel på. Terroranslaget medførte derimot ingen økning i trusselnivået fra nasjonale ekstreme miljøer i Norge de neste årene (PST, 2012). Risikoen for terrorangrep ble allikevel oppjustert i 2014, og har i de senere år blitt vurdert som stadig økende, noe som primært skyldes internasjonal terrorisme. Skandinavia har over lengre tid vært utpekt som et mål for terror for ulike ekstreme islamistgrupper. Årsaker til dette kan eksempelvis være hendelser som republiseringen av Muhammed-karikaturene, den norske håndteringen av mulla Krekar, Norges militære nærvær i Afghanistan og bombingen i Libya (NOU 2012: 14). I hovedsak er terrorangrepene som har forekommet i Norge derimot utført av mennesker med en høyreekstrem ideologi, og de siste 10 årene har trusselen for angrep fra høyreekstreme blitt oppskalert (NOU 2012: 14). PST kalkulerte at det i 2020 var like stor sannsynlighet for at det ble utført terrorangrep fra høyreekstremister som fra ekstreme islamistgrupper (PST, 2020). I 2021 ble derimot trusselnivået for angrep fra ekstreme islamistgrupper oppjustert igjen etter flere angrep lengre sør i Europa (PST, 2021). Relevante trusselaktører vil utdypes i større grad i 5.1.2.

Teknologiens utvikling

Digitaliseringen har påvirket det nasjonale risikobildet i Norge i stor grad. Den globale teknologiutviklingen, samt den omfattende bruken av internett, er både et gode, samtidig som det fører med seg alvorlige og grenseoverskridende utfordringer. Utviklingen har bidratt til

både effektivisering og nyskapning i samfunnet, men medfører også gjensidige avhengigheter på tvers av land og sektorer. Angrep i det digitale domenet kan dermed ha omfattende konsekvenser, noe som igjen medfører et mer uforutsigbart risikobilde (NOU 2016: 19).

Den kritiske infrastrukturen i Norge blir stadig mer digital og blir ifølge Etterretningstjenesten utsatt for angrep av ulike aktører daglig (Etterretningstjenesten, 2015). Realisering av den digitale terrortrusselen er allikevel foreløpig begrenset, noe som hovedsakelig bunner i at trusselaktørene ikke besitter kunnskapen nødvendig for å gjennomføre 'vellykkede' terrorangrep i cyberdomenet enda (NOU 2015: 13). Truslene i det digitale rom handler i stor grad om informasjon, enten det er å stjele, endre eller plante informasjon, eller forhindre overføring av informasjon mellom to parter. Dette kan ramme for eksempel informasjonssystemer som inneholder sensitive opplysninger, kontrollsystemer for krisehåndtering og beredskap eller styrings- og kontrollsystemer for andre samfunnsviktige funksjoner og finansielle systemer (NOU 2016: 19). Norges kritiske infrastruktur er området som antas å ville bli mer utsatt i en eventuell global maktkamp, og med den nåværende utviklingen er det ikke fjernt å anta at det er her en fremtidig politisk konflikt vil utarte seg (Friis & Hansen, 2020). Tidligere forsvarsminister og nåværende utenriksminister Ine Eriksen Søreide uttalte i 2013:

> Cyberterrorisme er en av mange grunner til å sikre samfunnskritiske systemer. Vi må bygge opp sikkerheten i våre systemer for å kunne møte slike trusler, selv om FFI mener det i dag er liten sannsynlighet for cyberterrorisme og selvstendige cyberkrigshandlinger mot kritiske samfunnsfunksjoner. Vi må sikre oss mot trusler i hele aktørspennet fra trivielle inntrengingsforsøk til statsdrevet spionasje og cyberterrorisme. (Mathisen, 2013, avsn. 14).

Internett har også i stor grad blitt brukt til rekruttering og radikalisering av terrorister. I PST sin trusselvurdering fra 2009 blir internett pekt ut som et viktig propagandaverktøy i radikaliserings- og rekrutteringssammenheng for norske islamister (PST, 2009), og i 2017 ble radikalisering blant asylsøkere og migranter oppnevnt som en av de største utfordringene (PST, 2017). I årene etter dette og frem til i dag fremstår det ut fra trusselvurderingene at radikalisering av ekstreme islamister gjennom internett minker, men at det hos høyreekstreme grupper derimot har fått et økt fokus (PST, 2019).

Risikopersepsjon

Risikopersepsjon er måten mennesker oppfatter risikoen som eksisterer rundt oss til enhver tid. Befolkningsundersøkelsen er en undersøkelse som omfatter spørsmål om den norske befolkning sin risikopersepsjon og inntrykket befolkningen har av hvor god beredskapen i Norge er. I befolkningsundersøkelsen fra 2016 er det størst grad av bekymring for at det blir gjennomført terrorangrep og cyberangrep mot styringssystemer de neste fem årene. 35% av deltagerne oppgir at de er svært bekymret for å bli rammet av terrorangrep de kommende fem årene, og 30% oppgir samme bekymring for at det skal gjennomføres et cyberangrep mot norske styringssystemer. 15% oppgir en sterk bekymring for at det skal forekomme et langvarig strømbrudd på over 24 timer (Epinion, 2016). Ved å foreta en sammenligning på bakgrunn av hva befolkningen svarte i Befolkningsundersøkelsen fra 2013, ser man at punktet med størst økning omhandler hvor stor sannsynlighet det vil være for at det blir gjennomført et terrorangrep på norsk jord. Resultatene fra Befolkningsundersøkelsen 2016 kan antas å ha en sammenheng med terrorangrepene i Frankrike årene i forkant, blant annet attentatet mot Charlie Hebdo og en økende frykt knyttet til dette (Epinion, 2016). Befolkningsundersøkelsen fra 2020 viser allikevel at bekymringen for terrorangrep er lik som i 2016 og ligger forholdsvis stabilt på 30%. I forhold til undersøkelsen i 2016 viser derimot undersøkelsen fra 2020 at bekymringen for at det skal bli gjennomført cyberangrep mot norske styringssystemer en økning på 9 prosentpoeng, og ligger dermed på 39% (Ipsos, 2020).

5.1.2 Trusselaktører

Fra PST sine egne trusselvurderinger er det tydelig at det har forekommet en forandring i hvilke aktører som har utgjort en terrortrussel mot Norge siden 1996. I Lund-rapporten var det i all hovedsak kommunister og sosialister som ble ansett som den største trusselen mot nasjonal sikkerhet. I dag har derimot trusselen fra ekstremister både med islamistisk og høyreekstremistisk ideologi økt i stor grad, og sammen med den økende trusselen fra statlig etterretning og ikke-statlige terrorgrupper anses disse grupperingene som de største trusselaktørene for Norges sikkerhet. Hvem som anses som trusselen i samfunnet vil ha mye å si for hvordan sikkerhetstiltak blir innført.

PST trakk, som nevnt, frem i trusselvurderingen sin for 2004 at terrortrusselen mot norske interesser generelt ble ansett som lav. Den globale jihadismen som hadde fått fokus etter 11.

september 2001 var det som kunne oppfattes som en trussel mot norske interesser. Det ble ansett som mulig at islamske ekstremister fremdeles kunne ha både intensjon og kapasitet til å gjennomføre terroraksjoner mot vestlige land, spesielt i Europa. Disse landene ville, samtidig som å fremstå som attraktive mål, i tillegg kunne bli brukt som oppholdssted for støttegrupper (PST, 2004). Støttevirksomhet kan inkludere både identitetsforfalskning og terrorfinansiering, og fremstod som hovedtrusselen for Norge frem til tidlig på 2010-tallet. Her begynte bildet av den økende radikaliseringen og rekrutteringen å dannes, noe som medførte usikkerhet og dermed utgjorde en større trussel. I tillegg til radikalisering og rekruttering medførte den økende bruken av internett at det ble ytret flere ekstreme meninger på nett, noe som også kunne føre til en enklere radikalisering av enkeltmennesker og sympatisører (PST, 2008). I 2016 ble det anslått at det var en mulighet for at terrorangrep ville bli gjennomført på norsk jord av ekstreme islamister. På dette tidspunktet var flyktningkrisen på sitt verste i Europa, og påvirket trusselbildet i stor grad. Frem til 2019 anså PST ekstreme islamister som aktørene som utgjorde den primære terrortrusselen og det ble ansett som mulig at det kunne bli gjennomført et terrorangrep mot Norge (PST, 2019). I trusselvurderingen for 2020 ble det konkludert med at terrortrusselen fremdeles ble ansett som høy, men at antall terrorangrep hadde gått dramatisk ned de siste 3 årene. I 2021 ble trusselen igjen skjerpet etter flere angrep i andre vestlige land i Europa. Det oppstod en økt spenning mellom ytringsfrihet og krenkelser av islam, og det ble derfor tillagt ekstra fokus på ekstreme islamister da trusselnivået for 2021 ble vurdert (PST, 2020, 2021).

I tillegg til ekstrem islamisme har det blitt satt fokus på høyreekstremister, venstreradikale personer og autonome grupper. Disse formene for politisk ekstremisme har gått gjennom en stor utvikling siden slutten av 90-tallet. I trusselvurderingen fra 2004 skrev PST at høyreekstreme grupper ble ansett som en trussel, med bakgrunn i at disse gruppene ofte hadde fellestrekk i at deres ideologi var antistatlige, rasistiske og antisemittiske. Dette gjaldt i all hovedsak voldelige aksjoner og demonstrasjoner, og en terrortrussel utført av det høyreekstremistiske miljøet ble på dette tidspunktet ansett som lav (PST, 2004). Venstreradikale grupper ble også inkludert i det nasjonale trusselbildet, men utgjorde i all hovedsak et ordensproblem knyttet til voldelige demonstrasjoner da det kom til dyrevern eller i konfrontasjon med de høyreekstreme miljøene. Utover 2000-tallet utgjorde ingen av de overnevnte gruppene en reell trussel mot nasjonale interesser, utenom at gruppene kunne skape frykt og utrygghet gjennom voldsepisoder (PST, 2007, 2008, 2009, 2010). I årene etter 22. juli 2011 økte sympatien for fremmedfiendtlig retorikk og det ble etablert flere

antiislamske aktører, som baserte seg kun på skepsis mot religion (PST, 2012). Fra midten av 2010-tallet og frem til i dag har trusselen fra de høyreekstreme miljøene vært i vekst, men omhandler i stor grad enkeltpersoner (PST, 2013, 2014, 2015). Det anses fremdeles som lite sannsynlig at høyreekstreme personer vil gjennomføre terrorangrep, og sannsynligheten for angrep fra ytre venstre regnes som svært usannsynlig. Det fokuseres derimot på radikalisering i de høyreekstreme miljøene. Flere islamfiendtlige grupper har fått økt tilstedeværelse i de høyreekstreme gruppene og fremstår som en særlig utfordring (PST, 2019).

Det digitale domenet er en arena der spesielt stormaktene aktivt kan forfølge sine målsettinger, og utenlandsk etterretningsaktivitet har i over 10 år blitt ansett som en betydelig trussel mot norske interesser. PST har også inkludert vurderinger av etterretningsvirksomhet i sine trusselvurderinger, og i 2009 ble utenlandsk statlig etterretningsaktivitet ansett som den største trusselen mot Norge (PST, 2009). Etterretning er målrettet innhenting og bearbeiding av informasjon for å gi et forbedret beslutningsgrunnlag for politiske og militære beslutningstakere. Med den hensikt å fremme egne interesser driver stater etterretningsaktivitet mot hverandre, ofte på bekostning av andres interesser. Årsakene til at Norge blir ansett som et mål for utenlandsk etterretning er blant annet fordi landet er medlem av NATO. I tillegg besittes det store energiressurser, avansert teknologi og store mengder olje- og gassressurser i nordområdene (PST, 2010). Frem til 2009 ble det i hovedsak vektlagt tradisjonelle etterretningsmetoder i trusselvurderingene, som innebar bruk av åpne kilder og personlige kontakter (PST, 2019). Fra 2009 og utover får internett en større rolle for de statlige aktørene som driver etterretning. Spionasje, tjenestenektangrep (DDoS) og informasjonsoperasjoner ble vurdert med et stadig høyere trusselpotensial, ettersom det kunne påføre Norge betydelig økonomisk og politisk skade. Skadepotensialet ved tap av sensitiv informasjon kan være stort (PST, 2009). Fra begynnelsen av 2010-tallet og utover anses utenlandsk etterretning å ha et stabilt høyt trusselnivå. Fra 2014 ble trusselen vurdert som trolig økende og den har fortsatt å øke i nivå frem til i 2021 (PST, 2014, 2021). Russland og Kina blir vurdert som de aktørene som vil ha størst skadepotensial for norske interesser i 2021, både i form av informasjonsinnhenting og påvirkning av beslutninger.

Både statlige aktører som driver etterretning og spionasje eller ikke-statlige terrororganisasjoner og andre ekstremister kan ta i bruk ulike metoder for å gjennomføre terrorangrep mot landet (Etterretningstjenesten, 2015). Cyberterrorister tilhører ideologisk motiverte grupper som bruker IKT for å ramme ulike samfunnsfunksjoner eller grupper med

vold eller trusler om vold (NOU 2015: 13). På lik linje med annen terrorisme gjennomføres terror i det digitale domenet ved å utnytte samfunnets sårbarhet for å spre vold, skape frykt, fremme politiske synspunkter eller påvirke atferd (Etterretningstjenesten, 2015).

USA har lengde vært en pioner når det kommer til digitale trender. I 2020 gikk de ut med en advarsel til den russiske presidenten hvor de uttalte hvordan de selv vil ta i bruk nye cyberverktøy mer offensivt og møte motstanderen i deres egne nettverk. Dette ble i all hovedsak kun regnet som en trussel, men ble også delvis gjort for å være klar til å gjennomføre cyberangrep om det plutselig skulle bryte ut en konflikt mellom Washington og Moskva (Sanger & Perlroth, 2019). Grunnet at ulike angripere er nødt til å bevege seg via en rekke servere i ulike land, vil Norge bli berørt og dermed bli en del av en fremtidig internasjonal og digital maktkamp. Dette øker omfanget av internasjonale trusselaktører i stor grad (Friis & Hansen, 2020).

5.1.3 Forslag til lovverk

Norges hemmelige tjenester argumenterer for at det trengs et oppdatert lovverk rundt overvåking. Dette begrunnes i både det nasjonale risikobildet og den stadige utviklingen av trusselaktører som kan ramme Norge. I tillegg til å fange opp relevante trusselaktører innad i Norge, påpekes det at Norge risikerer å bli et sort hull om vi ikke får et oppdatert lovverk som omfatter at den norske Etterretningstjenesten får verktøy for å fange opp utenlandske digitale trusselaktører, sett i sammenheng med den teknologiske utviklingen og det sikkerhetspolitiske landskapet (Friis & Hansen, 2020). Utenriksminister Ine Eriksen Søreide uttalte i 2013 at det er nødvendig med sikkerhetstiltak for terror, både fysisk og i det digitale domenet, samt for etterretning, og at begge deler inngår som en del av det forebyggende sikkerhetsarbeidet i Norge: «Dette omfatter et stort knippe med tiltak innen fysisk sikring, personellsikring og rene informasjonssikkerhetsmessige tiltak» (Mathisen, 2013). Tidligere statssekretær Hans J. Røsjorde uttalte videre: «En terroraksjon i cyberdomenet er et alternativ som ikke skal undervurderes. Det er viktig at vi dimensjonerer dette slik at man svarer på det trusselbildet som beskrives» (Mathisen, 2013).

Samfunnet forventer i større og større grad at trusler og terrorplanlegging skal fanges opp før et eventuelt angrep blir gjennomført. Som vist har det nasjonale risikobildet endret seg i stor grad de siste 25 årene, og for å forsøke å tilpasse seg dette har det i løpet av årene blitt presentert ulike lovforslag, som vil bli presentert nedenfor. Lovforslagene som blir presentert

er forslaget om innføringen av Datalagringsdirektivet (DLD), innføringen av preaktiv strafferett og forslag til ny etterretningstjenestelov (også kalt Det digitale grenseforsvaret (DGF)). I tillegg blir Politiets fullmakt til bruk av skjulte tvangsmidler, da spesielt metoden dataavlesning, diskutert i kapittel 5.3.2. Forslagene har blitt foreslått og/eller vedtatt i en prosess der målet er å avverge terrorangrep før de blir gjennomført.

Etter terroranslagene som ble utført i USA i 2001, i Madrid i 2004 og i London 2005, ble EUs direktiv 2006/24/EF vedtatt i 2006. Dette påla tele- og internettilbydere å lagre data som omfatter hvor, hvordan og med hvem du kommuniserte med på telefon, mobil og e-post, også kjent som metadata. Formålet var å sikre tilgang til denne dataen i forbindelse med etterforskning, avsløring og rettsforfølgelse av alvorlig kriminalitet, og særlig organisert kriminalitet og terrorisme (Graver & Hardborg, 2015). Spesielt en hendelse tok stor plass i diskusjonen rundt hvorvidt et slikt direktiv var nødvendig, nemlig terrorangrepet 22. juli 2011. Angrepet 22. juli 2011 har ført til mye debatt om hvorvidt Norge har hatt behov for endringer i lovverk vedrørende terrorangrep (NOU 2012: 14). Direktivet skapte derimot også stor debatt rundt hvorvidt personvernet ble opprettholdt på en god nok måte. I 2011 ble det allikevel vedtatt endring i ekom- og straffeprosessloven, noe som også medførte implementering av DLD i norsk rett (Sæbø & Gisle, 2019). DLD skulle i utgangspunktet trådt i kraft i 2012, men ble utsatt flere ganger. I april 2014 ble det derimot konkludert med at DLD var i strid med EMK art. 8. Kort fortalt vil det si at direktivet ble ansett som mer inngripende i retten til privatliv og personvern enn det som ble ansett som nødvendig for kriminalitetsbekjempelse. Dermed stanset regjeringen det videre arbeidet med direktivet (Graver & Hardborg, 2015).

Etter 22. juli 2011 ble det stadig fremmet forslag om nye strafferettslige bestemmelser for å ramme terrorisme. Ettersom PST er aktøren med hovedansvar for å avverge dette fikk de ulike fullmakter til å overvåke personer de mistenkte at utgjorde en trussel mot landet (NOU 2012: 14). Offentligheten la press på at de ønsket at PST skulle følge med på politiske og ideologiske yttergrupper, selv når disse ikke utøvde voldelige handlinger, og dermed la PST frem flere forslag som de mente ville bidra til å ramme terrorangrep mot Norge. Flere av disse har blitt omtalt som problematiske, da de blant annet omhandler omfattende datainnsamling og kriminalisering av diverse vage handlinger.

En av endringene som ble gjennomført, som fremstår som en tydelig kursendring i forhold til norsk rettstradisjon, er innføringen av preaktiv strafferett (Justis- og beredskapsdepartementet, 2012). Preaktiv strafferett innebærer at man ikke lengre må ha gjennomført en handling før straff kan gis, og en slik utvikling utfordrer tradisjonelle prinsipper for kriminalisering og straff i Norge (NOU 2020: 4). Ifølge lovverket vil det dermed være mulig å straffe før handlingen faktisk blir utført. Forslagene til PST gikk ut på å endre den daværende lovgivningen, slik at det ikke var nødvendig å inngå et terrorforbund for at en handling skulle regnes som terrorisme (Prop. 66 L. (2019-2020)). Straffeterskelen ble dermed senket. Ved å tette hull i den eksisterende lovgivningen mente PST at strafferammen også ville omfatte enkeltmannsterrorisme eller soloterrorisme. Det ble dermed innført et forbud mot planlegging av terrorhandlinger, som blant annet inkluderte forbud mot å motta trening til nytte for terror, samt tilstedeværelse på et sted hvor det bedrives terrortrening. Det ble også utformet forbud mot besittelse av både gjenstander og informasjon som kan være relevant med tanke på fremtidige terrorhandlinger, samt kriminalisering av medlemskap i terrororganisasjoner (Justis- og beredskapsdepartementet, 2012).

I 2016 ble det igjen lagt frem et nytt forslag rundt tilrettelagt datainnsamling, denne gang i sammenheng med den nye etterretningstjenesteloven. Den forrige etterretningstjenesteloven trådde i kraft i 1998. Det har foreligget mye kritikk om hvorvidt denne loven har vært åpen om hvordan Etterretningstjenesten har operert siden loven ble vedtatt, og det har dermed eksistert et behov for et nytt, oppdatert lovverk. I tillegg til en mer åpen beskrivelse av gjeldende regelverk og praksis for Etterretningstjenesten, har den nye loven også en sikker rettslig forankring. En av de mest omdiskuterte endringene omhandlet den tilrettelagte datainnsamlingen av grenseoverskridende elektronisk kommunikasjon, som innebar at Etterretningstjenesten ville fått lagret all metadata som krysset de norske landegrensene (Regjeringen, 2020). Metadataen skulle bli samlet inn via land- eller sjøbaserte fiberoptiske kabler, og skulle være relevant for utenlandsetterretningen. Lysne-II-utvalget anbefalte i sin rapport at Etterretningstjenesten fikk adgang til masselagringen av informasjonen som krysset landegrensene og at de kunne gjennomføre søk i denne datatrafikken (Lysne II-utvalget, 2016). Etter en lang prosess gikk forslaget om et nytt digitalt grenseforsvar gjennom og 11. juni 2020 ble loven vedtatt på Stortinget. I oktober samme år ble derimot kapittel 7 og 8 i den nye loven derimot avslått, da disse kapitlene omhandler tilrettelagt innhenting av informasjon og bryter både med Grunnloven § 102, EMK art. 8 og EU-retten når det omhandler om person- og kommunikasjonsvern (Skjevestad, 2020).

5.1.4 Oppsummering

Empirien som har blitt presentert i kapittel 5.1 demonstrerer at risikobildet i Norge har endret seg betydelig siden 1996. Norges verdier, trusler og sårbarheter har alle økt i stor grad de siste 25 årene, i tillegg til hvem som er de relevante trusselaktørene. Både trusselen fra høyreekstreme grupper og utenlandsk statlig etterretning har økt i stor grad. Trusselen fra ekstreme islamistiske miljøer har også økt, men var mer tilstedeværende i årene etter 11. september 2001 enn de ovenstående. Dette er faktorer som har bidratt til at risikobildet Norge står overfor er veldig annerledes i dag enn det var for 25 år siden. Terrortrusselen er betydelig mer aktuell for Norge i dag enn den var på begynnelsen av 2000-tallet, men det er ikke kun en høyere terrortrussel som er aktuelt for Norge. Også måten terrorangrepene er utformet på har forandret seg. Gjennom den teknologiske utviklingen har både målet ved å gjennomføre angrep, og metoden bak utformet seg på nye måter. Tidligere var målet for terrorisme i stor grad å skape frykt ved å tilføre skade mot en stat eller et samfunn ved bruk av tradisjonelle virkemidler, som eksempelvis sprengstoff. Nå omhandler terrorisme også å tilegne seg informasjon som kan brukes mot den aktuelle staten. Å tilegne seg, forandre og plassere informasjon, eller å forhindre informasjonsoverføring mellom to parter kan ha store konsekvenser om det rammer eksempelvis informasjons- eller kontrollsystemer for krisehåndtering eller samfunnsviktige funksjoner.

Overvåking som sikkerhetstiltak har blitt forsøkt formet mye frem og tilbake siden 1996, ettersom risikobildet har utviklet seg. I 1996 ble kravene til PST og Etterretningstjenesten skjerpet inn etter Lund-kommisjonens rapport, men det har stadig blitt presentert nye forslag til fullmakter for maktinstansene. Mange av forslagene er lagt frem etter press fra offentligheten, og særlig etter terroranslag har blitt gjennomført i Norge og andre europeiske land. Innføringen av preaktiv strafferett og forslagene om Datalagringsdirektivet og Det digitale grenseforsvaret har skapt mye debatt rundt hvor grensen burde gå for overvåking gjennom en slik form for datainnsamling, satt opp mot ulike demokratiske prinsipper. Da stadig mer informasjon flyttes over til det digitale domenet er det lite som tilsier at utformingen av nye regler og forslag til lovverk vil avta. Det er også tydelig at det foreligger en større bekymring hos befolkningen for at det skal gjennomføres et terrorangrep i dag enn det gjorde for 25 år siden. Dette kan påvirke presset Politiet og Forsvaret opplever, og hvilke tiltak befolkningen godtar at myndighetene innfører.

5.2. Hvordan har statssikkerhet og samfunnssikkerhet endret seg i forhold til utviklingen av overvåking?

5.2.1 Sikkerhetspolitisk utvikling

Den sikkerhetspolitiske situasjonen til Norge endret seg i stor grad ved oppløsningen av Sovjetunionen på begynnelsen av 90-tallet, og trusselen om invasjon og konflikter i nærområdet var betydelig redusert i denne perioden (NOU 2000: 24). I 2004 ble det beskrevet hvordan tiden var preget av økende globalisering, noe som ble ansett som overveiende positivt. Globalisering bidro til nye muligheter, både innenfor teknologi, økonomi, politikk og kultur, samt at det internasjonale samarbeidet ble oppfattet som styrket. Globalisering ble derimot ikke kun oppfattet som et fremskritt. For noen stater eller grupper ble globalisering derimot oppfattet som noe truende mot egen kultur, egenart og autonomi, og kunne dermed føre til ulike typer mottiltak mot de aktører som i sterkest grad ble oppfattet å stå bak globaliseringen. Terrorisme er et av eksemplene på slike mottiltak (St.prp. nr. 42 (2003-2004)). Risikobildet i Norge preger dermed også den sikkerhetspolitiske utviklingen.

Tidlig på 2000-tallet var truslene mer diffuse enn tidligere og ble kjennetegnet av glidende overganger mellom fred, krise, væpnet konflikt og krig. Ettersom det ble vanligere med trusler som i hovedsak var knyttet til faktorer utenfor Norges nærområdet ble truslene også oppfattet som langt mer uoversiktlige (St.prp. nr. 42 (2003-2004)). Utover 2000-tallet økte globaliseringen, noe som for Norge utgjorde den største trusselen mot samfunnssikkerheten (St.prp. nr. 48 (2007-2008)). Samfunnet ble mer og mer sårbart på grunn av dette, i tillegg til den økte sentraliseringen, spesialiseringen og teknologiavhengigheten. Etter 22. juli 2011 ble det lagt et ekstra fokus på at Forsvaret også var blitt mer avhengig av det sivile samfunn når det kom til teknologi og leveranse av varer og tjenester. Dermed ble også et sivil-militært samarbeid mer og mer sentralt, både i kriser og normalsituasjoner (Prop. 73 S. (2011-2012)). Dette utdypes videre i kapittel 5.2.3. I 2016 ble det anslått at Norge ville gå gjennom en negativ sikkerhetspolitisk utvikling de kommende årene, noe som frem til i dag har vært en realitet. Det blir tatt høyde for en ytterligere negativ utvikling av sikkerhetssituasjonen i våre nærområder, samtidig som det påpekes at Norge er bedre rustet for å ivareta egne sikkerhetsinteresser enn i 2016 (Prop. 1 S (2020-2021)).

5.2.2 Utvikling av sikkerhetsbegrepene

De siste 25 årene har innholdet i betydningen til begrepene *samfunnssikkerhet* og *statssikkerhet* gjennomgått en viss endring. Fra den kalde krigen og frem til slutten av 90-tallet var det den tradisjonelle statssikkerheten som ble vektlagt når det kom til den nasjonale sikkerheten mot terrorangrep. Terroranslaget mot USA 11. september 2001 regnes som en avslutning på overgangsperioden etter den kalde krigen, og bidro til en utvidelse av forståelsen av sikkerhet til å omfatte en samfunnssikkerhet og menneskelig sikkerhet i tillegg (Forsvarsdepartementet og Justis- og beredskapsdepartementet, 2018).

Sikkerhetsbegrepet har i all hovedsak blitt knyttet til sikkerhetsbehovet til statens eksistens og integritet, nemlig statssikkerhet (St.prp. nr. 48 (2007-2008)). Å ivareta statssikkerheten er det sentrale formålet til sikkerhetspolitikken. Statssikkerhetsbegrepet har blitt brukt i sammenheng med det militære og har omhandlet beskyttelsen av Norges suverenitet og territorium. Frem til slutten av 90-tallet var det dette sikkerhetsbegrepet i all hovedsak handlet om. Tradisjonelt har statssikkerhet vært Forsvarets ansvarsområde, men en endring i det nasjonale risikobilde medfører også en endring av Forsvarets tradisjonelle arbeidsoppgaver, som utdypes nærmere i kapittel 5.2.3. Endringer i det sikkerhetspolitiske landskapet kan skje raskt, og det kan være vanskelig å vite hva intensjonen bak nye former for angrep mot staten er. Ved at nye former for terrorisme dannes vil dermed også trusselen mot statssikkerheten opptre i nye former, som ikke nødvendigvis kan stoppes i det fysiske domenet (DSB, 2019). En konsekvens av dette er at samfunnsstrukturen blir utsatt for nye trusler og farer, mange av de knyttet til økt avhengighet og sårbarhet i kritisk infrastruktur og lignende. En følge av dette har vært et økt fokus på samfunnssikkerhet.

Begrepet samfunnssikkerhet ble for første gang i Norge presentert i Sårbarhetsutvalget, ledet av Kåre Willoch (NOU 2000: 24). Et år senere ble rapporten *Samfunnssikkerhet - veien til et mindre sårbart samfunn* publisert (Meld.St. 17 (2001-2002)). Samfunnssikkerhet blir i denne rapporten definert som: «Den evne samfunnet som sådan har til å opprettholde viktige samfunnsfunksjoner og ivareta borgernes liv, helse og grunnleggende behov under ulike former for påkjenninger» (Meld.St. 17 (2001-2002), s. 4). Her blir det vektlagt at ansvaret for samfunnssikkerheten ligger på både nasjonalt, regionalt og lokalt nivå. Alle sektorer ble pålagt ansvar, så vel som den enkelte borger (Meld.St. 17 (2001-2002)). Samfunnssikkerheten ble dermed gitt en mer fremtredende rolle i den nasjonale sikkerhetspolitikken.

Fokus har i stor grad ligget på samfunnssikkerhetsbegrepet de siste 10 årene. Ettersom samfunnssikkerhet dreier seg om å ivareta sivilbefolkningens trygghet og sikre sentrale samfunnsfunksjoner og viktig infrastruktur mot angrep, innebærer dette også situasjoner som ut fra trusselbildet må defineres som en statssikkerhetssituasjon (Forsvarsdepartementet og Justis- og beredskapsdepartementet, 2018). Begrepet er ikke entydig, og vil derfor bli påvirket ettersom kriser inntreffer og påvirker samfunnet. Globalisering var en viktig årsak til at begrepet ble etablert av myndighetene og hendelser av global karakter har vært viktig for utviklingen av innholdet i begrepet, som terroranslaget 11. september 2001 (NOU 2006: 6). Trusselen mot terrorisme i Norge blir også fremhevet av globaliseringen, da det blir lettere å ta seg over landegrenser, teknologien utvikler seg og nye former for terrorisme dannes. Terrorangrepet 22. juli 2011 medførte store endringer innen både beredskap og krisehåndtering, noe som videre førte til en ny formulering av samfunnssikkerhetsbegrepet:

> Samfunnssikkerhet handler om samfunnets evne til å verne seg mot hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være et utslag av tekniske eller menneskelige feil eller bevisste handlinger. (NOU 2016: 19, s. 29).

Forebyggende sikkerhet settes dermed mer i fokus, og uønskede, tilsiktede handlinger blir fremhevet som hendelser som kan påvirke samfunnssikkerheten. En slik fokusendring i begrepsutformingen påvirker dermed også maktinstansene til å endre ansvarsområdene sine, slik at deres arbeidsoppgaver fortsatt favner over innholdet til begrepene slik de er utformet i dag.

5.2.3 Ansvarsområder i utvikling

Når sikkerhetsbegrepene forandrer seg vil dette også påvirke ansvarsområdet til Politiet og Forsvaret. Med tanke på digitalisering og globalisering vil dette si at ansvarsområdene til maktinstansene vil omfatte mer, ettersom risikobildet stadig er i utvikling og truslene mot landet endrer seg i høyt hastighet. Empirien i kapittel 5.1 viser hvordan risikobildet i stor grad har endret seg i tritt med den teknologiske utviklingen. I 2000 tydeliggjorde Sårbarhetsutvalget at det sikkerhetspolitiske landskapet var preget av en forskyvning fra det manuelle mot det elektroniske. Det forelå en stor forandring i bruk av IKT, som bidro til en endret betydning av landegrensene i sikkerhets- og beredskapssammenheng (NOU 2000: 24). Det digitale domenet er globalt og gjør det mulig for «hvem som helst» å angripe elektroniske

mål «hvor som helst» i verden (Meld.St. 10 (2016-2017)). Geografisk avstand får dermed stadig mindre betydning (Ekspertgruppen for Forsvaret av Norge, 2015). En endret sikkerhetspolitisk utvikling, kombinert med hybride trusler, aktualiserer et samarbeid mellom det militære og det sivile i det digitale rom (Forsvarsdepartementet og Justis- og beredskapsdepartementet, 2018).

Av hendelser som har påvirket ansvarsområdene til det norske politiet troner 22. juli 2011 høyt på toppen. Politiets rolle innenfor samfunnssikkerhet har fått stadig større oppmerksomhet i ettertid av hendelsene (Meld.St. 29 (2019-2020)). Aktørene relevante for overvåking i samfunnet er som tidligere presentert PST, underlagt politietaten og den sivile sektoren, og Etterretningstjenesten, underlagt Forsvaret og den militære sektoren. Utviklingen viser at både ansvarsområdene og hva begrepene stats- og samfunnssikkerhet innebærer har forandret seg siden slutten av 90-tallet. Tradisjonelt har det vært en skarpt skille mellom ansvarsområdene til Forsvaret og Politiet, statens maktinstitusjoner, der Forsvaret har hatt ansvar for statssikkerheten og Politiet har jobbet innenfor samfunnssikkerhetsområdet. I 2015 ble det derimot gjort tilpasninger til det nasjonale trusselbildet via endringer i Politiloven § 27a, som tilrettela for at Forsvaret kan bistå Politiet, der Politiets egne ressurser antas å ikke være tilstrekkelige eller tilgjengelige, som for eksempel ved et terrorangrep (Forsvarsdepartementet og Justis- og beredskapsdepartementet, 2018). På denne måten blir også Forsvaret inkorporert i samfunnssikkerhetsarbeidet. Samfunnssikkerhet har dermed gått bort ifra å kun ansvarliggjøre sektorer og enkelte borgere, til å hovedsakelig bli et myndighetsansvar. I en sikkerhetspolitisk krise eller væpnet konflikt er derimot også Forsvaret avhengig av at samfunnet fungerer på en mest mulig normal måte. Dermed er også god samfunnssikkerhet viktig for Forsvarets evne til å ivareta statssikkerheten. På lik linje som det militære vil bistå det sivile med de kapasitetene som er tilgjengelig i en krisesituasjon, vil også det sivile søke å støtte opp under det militære, i form av blant annet tjenester, varer, personell og tilgang til infrastruktur, når dette anses som nødvendig (Meld.St. 10 (2016-2017)). Myndighetene vil dermed sitte på en viss kontroll og styring av sikkerheten til både private og samfunnskritiske virksomheter, da bortfall kan få store konsekvenser utover disse og prege samfunnet i stor grad (NOU 2018: 14).

I overgangen til det digitale domenet kan endringer forekomme svært raskt og trusler mot stats- og samfunnssikkerheten vil forekomme i stadig nye former. Det digitale domenet fører dermed med seg en rekke utfordringer. Skillene mellom stats- og samfunnssikkerhet blir i

utgangspunktet enda vanskeligere å gjenkjenne, da domenet er flytende og grenseoverskridende, og det vil på mange måter bli vanskelig å skille mellom om en trusselsituasjon er av sivil eller militær karakter (Meld.St. 10 (2016-2017)). PST og Etterretningstjenesten har et utstrakt kontraterrorsamarbeid gjennom Felles kontraterrorsenter som ble etablert i 2014, spesielt når det kommer til trusselbildet og trusselaktørene som kan ramme Norge (Meld.St. 10 (2016-2017)). Det er derimot fremdeles utfordringer som er knyttet til roller og ansvar i en trusselsituasjon, noe som spesielt gjelder når et angrep gjennomføres i det digitale domenet. Det er ofte i startsfasen at det blir utfordrende å vite hvem som er ansvarlig for angrepet og hva formålet er, for eksempel om det er et cyberangrep for økonomisk vinning eller et terrorangrep som gjennomføres mot den norske stat. Dette utfordrer arbeidsfordelingen mellom de ulike myndighetsorganene, slik at det ikke er tydelig hvem som har beslutningsmyndighet til å iverksette tiltak dersom det oppstår interessekonflikter mellom aktuelle aktører i håndteringen av hendelser (NOU 2015: 13). Ved at den militære og den sivile sektoren i økende grad benytter seg av felles IKT-infrastruktur tydeliggjør utfordringene ytterligere. Når digitale sårbarheter blir felles er dermed et godt samarbeid mellom sivile og militære myndigheter avgjørende (Forsvarsdepartementet og Justis- og beredskapsdepartementet, 2018).

Både stats- og samfunnssikkerheten innebærer forebyggende sikkerhet (NOU 2015: 13). Dette innebærer blant annet innføringen av tiltak for å identifisere, vurdere og håndtere risiko, men det finnes grenser for hvor langt arbeidet bør strekkes. Selv ved innføringen av ulike tiltak for å sikre samfunnet mot risiko mot terrorangrep vil en restrisiko alltid eksistere. Ulemper ved tiltak kan være at kostnadene overstiger nytten vi anslår at tiltaket gir oss. I tillegg kan tiltak komme i konflikt med grunnleggende verdier, som selvbestemmelse, personlig frihet, rettssikkerhet og personvern (Meld.St. 10 (2016-2017)). Dette er Snowden sin avdekking av NSAs omfattende informasjonsinnhenting et godt eksempel på, og viser nødvendigheten av å ha en god balanse mellom innføring av tiltak og forebygging av slike mulige virkninger (NOU 2015: 13).

Utviklingen av ansvarsområder som beskrevet ovenfor vil kunne medføre ulike konsekvenser. Ansvarsområdene har tidligere hatt klare territorielle begrensninger, men desto mer ansvarsområdene til PST og Etterretningstjenesten sklir over i hverandre, jo mer uklare blir de. Etter forslaget om endring av etterretningstjenesteloven, ble det skapt stor tvil rundt hvorvidt Etterretningstjenesten kan operere på norsk jord og bruke metoder som berører

personer eller virksomheten innenfor norsk jurisdiksjon. Her ble det blant annet foreslått at overvåking av norske personer ble tillatt, så fremt innhentingen av informasjon var rettet mot etterretningsmål i utlandet. Oppgaver som dette var i hovedsak utenfor deres ansvarsområder og ved at det forekommer tvil om slike arbeidsområder kan det i verste fall føre til overlapping med PSTs mandat eller etterretningssvikt (Prop. 80 L. (2019-2020)). Ved overlapp av ansvarsområder og rapportering kan tjenestene operere mot samme miljø uten å være kjent med det, rapportere inn samme informasjon som ulik informasjon, og kan ha store konsekvenser for norske beslutningstakere og internasjonalt samarbeid, om tjenestene hver for seg deler lik informasjon med andre samarbeidende tjenester.

5.2.4 Oppsummering

Siden tusenårsskiftet har den sikkerhetspolitiske situasjonen i Norge endret seg i stor grad, og både stats- og samfunnssikkerhet har gjennomgått betydelige rolleskifter. Globalisering har bidratt til nye muligheter innen teknologi, økonomi, politikk, kultur og internasjonalt samarbeid, men dette medfører også sårbarheter. Gjennom utvikling av teknologi blir trusler langt mer komplekse og uoversiktlige. Dermed blir det plutselig mer aktuelt med et sivil-militært samarbeid, ettersom truslene i det digitale domenet ikke holder seg til enkelte territorielle grenser. Dette har ført til endring av begrepene statssikkerhet og samfunnssikkerhet. Etter 22. juli 2011 vinkles samfunnssikkerhetsbegrepet mot en mer forebyggende sikkerhet og kaster lys på at Norges beredskap må styrkes, noe som også påvirker maktinstansene sine ansvarsområder. Myndighetene får mer ansvar, og vil i større grad styre sikkerheten til både private og offentlige samfunnskritiske aktører og virksomheter. Det utformer seg derimot store utfordringer knyttet til ansvarsområdene til PST og Etterretningstjenesten, både når det kommer til beredskap og krisehåndtering. Innen krisehåndtering er beslutningsmyndigheten en utfordring. Når et angrep blir utført i det digitale domenet er det utfordrende å vite hva som er formålet bak angrepet, og det vil være en stor utfordring for tjenestene å vite hvem som har beslutningsmyndighet i ulike situasjoner. Med beredskap og forebyggende sikkerhet kan det ha store implikasjoner rundt hvorvidt hvilke sikkerhetstiltak som gjelder for de ulike instansene. Overlapp av overvåking av samme miljøer og innsamling av informasjon kan blant annet føre til etterretningssvikt, ha store konsekvenser for norske beslutningstakere og problematisere internasjonalt samarbeid ved overlappende deling av informasjon.

5.3. Hva er utfordringer med denne utviklingen i forhold til personvern?

5.3.1 Personvern som ideal for et demokratisk samfunn

Alle mennesker har behov for sin egen private sfære, der man slipper å forholde seg til innblanding fra myndighetene eller andre enkeltmennesker (NOU 2009: 15). Retten til privatliv som ideal er en menneskerettighet etter EMK art. 8. Ettersom konvensjonen er inkorporert i norsk rett vil den gå foran norsk lovgivning dersom det møtes på motstrid. Personvern omhandler ikke kun retten til å være i fred, men innebærer også en rett til å ha kontroll over opplysninger om en selv, spesielt personlige. Ytringsfrihetskommisjonen gir uttrykk for følgende om forholdet mellom den private sfære og inngrep utenfra:

> Den private sfære, eller intimsfæren, er sfæren der man omgås med dem man kjenner som personer. Den er, og bør være, en frihetssfære i den forstand at den i omfattende grad er beskyttet mot reguleringer og inngrep fra det offentlige. (NOU 1999: 27, s. 28).

Det argumenteres videre for at den private sfæren skal være beskyttet for innsyn fra det offentlige, så vel som fra offentligheten. Denne sfæren regnes som en viktig del av grunnlaget for et reelt demokrati, og er helt nødvendig for at individer kan bearbeide og utvikle tanker og oppfatninger, for videre å kunne bidra i demokratiske prosesser (NOU 2009: 15). Demokratiet og samfunnet vårt bygger på verdier og prinsipper som skal være førende for fremtidens samfunn, og innebærer ulike rettsstatsprinsipper og menneskerettigheter, blant annet personvern og ytringsfrihet.

Det motsatte av et samfunn der individer sin private sfære er tatt vare på er et samfunn der myndighetene besitter kunnskap om enkeltindividenes privatliv. Dersom myndighetenes innsyn i den private sfære øker ved at myndighetenes mulighet til å overvåke befolkningens privatliv utvides, vil mulighetene for maktmisbruk også øke (NOU 2009: 15). I en rettsstat skal det være tydelige regler for myndighetenes besittelse av makt og adgangen myndighetene har til å bruke denne makten (NOU 2015: 13). Uten dette vil både tillit og maktbalansen mellom myndighetene og befolkningen kunne bli forstyrret. Konsekvensene av dette kan være ødeleggende for demokratiet. Den private sfære og personvern er dermed en forutsetning for demokratiet og maktbalansen i samfunnet. Dette tilsier at denne sfæren i utgangspunktet burde være fri for både regulering og innsyn fra den offentlige (NOU 2009: 15).

Dermed oppstår det ofte et dilemma mellom myndighetene og befolkningen når det kommer til å ivareta Norges stats- og samfunnssikkerhet. Opprettholdelsen av grunnleggende verdier som statens selvstendighet, suverenitet og handlefrihet er noe av det mest grunnleggende for et demokratisk samfunn. Ved at myndighetene innfører sikkerhetstiltak for å forhindre at trusler mot staten manifesteres, vil dette igjen påvirke de grunnleggende samfunnsverdiene. Derfor er det nødvendig at dette begrunnes som legitimt og forholdsmessig for å beskytte andre grunnleggende rettigheter, som personvern (NOU 2016: 19).

5.3.2 Skjulte tvangsmidler

Personvern er derimot ikke absolutt og alvorlig kriminalitet veier tyngre, jfr. EMK art. 8 (2), som lyder:

> Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter. (Menneskerettsloven, 1999).

Hensynet til statssikkerhet, offentlig trygghet og bekjempelse av alvorlig kriminalitet tilsier at det kan gjøres inngrep i den enkeltes rett til personvern (NOU 2015: 13). Som empirien i 5.2.1 viser står Norge ovenfor en økende negativ sikkerhetspolitisk situasjon, og det argumenteres for at det, på bakgrunn av dette, foreligger et behov for overvåkingstjenester som har egne fullmakter når det kommer til bruk av ulike tvangsmidler. Inngrep i personvernet skjer både ved all behandling av personopplysninger, og ved innhenting av opplysninger ved bruk av skjulte tvangsmidler (NOU 2009: 15). I 2016 la Justis- og beredskapsdepartementet frem et forslag om lovendringer som ville utvide Politiets adgang til å ta i bruk skjulte tvangsmidler ved etterforskning, avverging og forebygging av alvorlige lovbrudd, som senere samme år trådte i kraft. Departementet skriver at det reiser særlige personvernmessige spørsmål å tillate bruk av tvangsmidler i forebyggende øyemed, men at ved å veie alvorlig kriminalitetsbekjempelse på den ene siden og personvernhensyn på den andre bør skjulte tvangsmidler kunne brukes for å forbygge de mest alvorlige straffbare handlingene (Prop. 68 L. (2015-2016)). Et av tvangsmidlene som ble innført i kampen mot

alvorlig kriminalitet og som har reist flere personvernmessige spørsmål er metoden rundt dataavlesning. Dataavlesning innebærer diverse utstyrs- og kunnskapsbaserte metoder for å skaffe tilgang til opplysninger i et datasystem som ikke er offentlig tilgjengelig. Blant annet kan ulik programvare, som trojanere, plasseres i mistenktes datasystem, slik at Politiet blant annet kan få tilgang på mistenktes kommunikasjon gjennom key-logging[2], lagret informasjon og andre opplysninger rundt datasystemet (Prop. 68 L. (2015-2016), s. 261-266). Anders Anundsen, tidligere justis- og beredskapsminister, uttalte i sammenheng med ikrafttredelsen av det nye lovverket:

> Dataavlesing, for eksempel ved å logge tastetrykk, er integritetskrenkende. Men samfunnet må ha et effektivt politi som kan bekjempe alvorlig kriminalitet. Det er vanskelig å tenke seg noe mer integritetskrenkende enn terror […]. Vi må ha metoder for å etterforske, avverge og forebygge slik kriminalitet. (Regjeringen, 2016).

Det argumenteres for i proposisjonen at endringene er nødvendige for å møte dagens trusselbilde og at det sikres tilstrekkelige virkemidler for å forebygge alvorlig kriminalitet. Det foreligger en økende bevissthet og kunnskap rundt viktigheten om egen informasjonsbeskyttelse i samfunnet, blant annet ved kryptering av informasjon eller annen type informasjonsbeskyttelse. Dette regnes som noe positivt, så lenge beskyttelsen er ment å verne lovlig aktivitet, men kan på en annen side brukes med kriminelle formål. Utredningen og høringen til lovforslaget viser at de eksisterende skjulte tvangsmidlene har mistet mye av sin effekt i lys av den teknologiske utviklingen, og det argumenteres derfor for at det er nødvendig med nye måter for Politiet å tilegne seg nødvendig informasjon på (Prop. 68 L. (2015-2016)).

Det er derimot uenigheter i hvor balansegangen mellom behov for og bruken av tvangsmidler går. Det er utledet ulike prinsipper som skal bidra til å sette denne grensen, kalt de europeiske personvernprinsippene. Prinsippene ligger til grunn for blant annet personopplysningsloven. Mange av disse prinsippene har stor overføringsverdi til de regler som bør ligge til grunn for Politiets bruk av skjulte tvangsmidler og behandling av informasjon i straffesaker. Noen av de relevante prinsippene er lovreguleringsprinsippet, formålsbestemthetsprinsippet, nødvendighetsprinsippet og sensitivitetsprinsippet (NOU 2009: 15). Lovreguleringsprinsippet

[2] Key-logging innebærer at tastetrykkene på et tastatur registreres.

går ut på at all behandling av personopplysninger må ha hjemmel i lov. Kravet om formålsbestemthet går ut på at informasjonsinnhenting kun kan foregå med bestemte forhold. På bakgrunn av dette kan ikke informasjon som er hentet inn som et ledd i etterforskning og forebygging av straffbare handlinger brukes til noe annet formål, uten at det blir gitt samtykke av personen det gjelder. Nødvendighetsprinsippet handler om at det kun skal tas i bruk skjulte tvangsmidler i etterforskning der det er nødvendig, og skal kun omfatte informasjon som er relevant for etterforskningen. Det siste prinsippet, sensitivitetsprinsippet, innebærer at spesifikke typer informasjon anses som særlig personlige, og at innsamling av dette bør underkastes strengere regulering enn informasjon som ikke er like sensitiv. I hvor stor grad personopplysninger er sensitive er derimot ingen fast størrelse, men påvirkes av mange faktorer. Her kan for eksempel myndighetene og befolkning ha ulik oppfatning, og dette kan også forandres over tid (NOU 2009: 15).

5.3.3 Befolkningens holdninger til personvern

Basert på personvernundersøkelsene gjennomført i Norge siden slutten av 90-tallet har samfunnets holdninger til personvern på flere områder holdt seg relativt stabile, mens de på andre områder har utviklet seg. Det er mange faktorer som har bidratt til denne utviklingen. Det er publisert flere personvernundersøkelser i tidsspennet mellom 1996 og 2021. De fem største ble gjennomført i henholdsvis 1997, 2005, 2008, 2014 og 2020.

I undersøkelsen fra 1997 blir det trukket frem at rundt halvparten av utvalget er interessert i personvern. De fleste respondentene sier seg derimot enige i at personvern som verdi ikke overgår oppklaring av kriminelle handlinger, og mener dette er viktigere enn hensynet til personvern (Gulløy, 1997). 2005-undersøkelsen viser at befolkningen har stor tillit til hvordan ulike offentlige organer og private virksomheter behandler personopplysninger, hvor Politiet blir plassert i en særstilling (Ravlum, 2005). Dette er det samme som ble oppgitt i undersøkelsen fra 1997. Det legges frem at befolkningen ikke er bekymret for at sensitive personopplysninger vil bli misbrukt av myndighetene (Ravlum, 2005).

Tillit er et viktig aspekt når det kommer til ivaretakelse av personvernet. Personvernsundersøkelsen fra 2014 viser at det fremdeles er en gjennomgående høy tillit i samfunnet til hvordan ulike private og offentlige virksomheter behandler deres personopplysninger. Både Politiet og helsevesenet skiller seg ut som instansene med høyest tillit i befolkningen, der 85% har stor eller noe tillit til hvordan de behandler

personopplysninger (Datatilsynet, 2014). Tallene i personvernundersøkelsen fra 2014 kan antas å være preget av Snowden-saken og avsløringene av amerikanske etterretningsmyndigheters fullmakter til datainnsamling av vanlige mennesker. Den norske Etterretningstjenesten har et høyt antall mennesker som har svart *vet ikke*, men 68% svarer at de fremdeles besitter stor tillit til hvordan Etterretningstjenesten behandler personopplysninger. Dette tyder på at Snowden-saken ikke har bidratt til å ødelegge tilliten til den norske Etterretningstjenesten. Undersøkelsen viser også at det befolkningen frykter minst ved å miste kontroll over egne personopplysninger er Politi- og etterretningsovervåking. Å oppleve identitetstyveri eller hacking av mobil eller datamaskin slik at noen får tilgang til det som er lagret der fremstår som den største frykten (Datatilsynet, 2014).

Personvernundersøkelsen fra 2014 tar også opp forholdet mellom kriminalitetsbekjempelse og personvern. Det foreligger et overordnet inntrykk at mange mener både Politi- og sikkerhetsmyndigheter bør kunne ta i bruk inngripende midler for å bekjempe kriminalitet, også når det går utover den enkeltes personvern. 43% er enig eller delvis enig, mens 31% er uenig eller delvis uenig (Datatilsynet, 2014). På spørsmål om Politiet og andre sikkerhetsmyndigheter burde kunne overvåke ved bruk av åpen informasjon fra sosiale medier og andre internettjenester har svarene endret seg i stor grad fra 2005. I 2005 svarte 56% seg helt enig, og 24% seg delvis enig om at Politiet og sikkerhetsmyndigheter burde kunne bruke slike virkemidler for å avdekke planlegging av kriminelle handlinger (Ravlum, 2005). I 2014 har derimot utsagnet fått svakere støtte. Begge undersøkelsene viser at en klar majoritet er enig i utsagnet, men resultatene fra 2014 viser at kun 27% sier seg helt enig, og 36% sier seg delvis enig. Faktorer som kan ha betydning for slike holdningsendringer kan blant annet være den store økningen i bruk av internett, med bakgrunn i at overvåking gjennom åpne kilder plutselig kan omfatte en selv (Datatilsynet, 2014).

I 2018 trådte GDPR i kraft i Norge, som har bidratt til å styrke personvernet for befolkningen i EU og EØS-land (Datatilsynet, 2020). Dette vil også være med å påvirke svarene befolkningen har gitt på personvernundersøkelsen i 2020. I 2020 har befolkningen i Norge fremdeles en gjennomgående høy tillit til hvordan offentlige virksomheter behandler personopplysninger. Av virksomhetene som har størst tillit fra befolkningen er fremdeles Politiet og helsevesenet på toppen, sammen med Skatteetaten og bankene. Siden 2014 har derimot Etterretningstjenesten sin tillit falt med 8 prosentpoeng, noe som kan antas å være et resultat av forslaget om DGF.

Selv om tilliten i samfunnet generelt blir ansett som høy til offentlige virksomheter når det kommer til lagring og bruk av personlig data, fremkommer det allikevel svært høye tall på individer som har avstått fra å bruke en tjeneste på grunn av manglende tillit. Halvparten sier at de har avstått bruk av tjenester grunnet at de er usikre på hvordan personopplysningene deres blir lagret og brukt, og 16% har unnlatt å gjøre noe på nettet i frykt om at noen skal følge med på dem (Datatilsynet, 2020). Dette er en stor andel i et liberalt sosialdemokrati, slik som Norge. Flere uttrykker også at de føler seg maktesløse når det kommer til å ha kontroll over egne personopplysninger på nett (Datatilsynet, 2020).

I dokumentene kommer det tydelig frem at det er flere faktorer som har hatt stor betydning for hvordan fokuset på personvern har endret seg fra slutten av 90-tallet og frem til i dag. I 1997 ble det påpekt at kun halvparten av respondentene hadde tilgang til internett, og det som fremkom som den største bekymringen var datidens utstrakte bruk av personnummer (Gulløy, 1997). Daglige brukere av internett og e-post ble omtalt som «storforbrukere» og viser at flere av problemstillingene knyttet til personvern i stor grad var annerledes enn de er i dag. Sammenlignet med 1997 brukte en gjennomsnittsnordmann i 2018 nær tre timer på internett hver dag (Datatilsynet, 2020). Utover 2000-tallet ble det en mer ustrakt bruk av internett, og problemstillingene har endret seg i takt med digitaliseringen og det faktum at det foreligger mye mer informasjon på nettet enn før.

5.3.4 Nedkjølingseffekt

Når det forekommer en usikkerhet rundt hvordan personopplysninger om oss blir tatt i bruk kan dette føre til en endring i atferdsmønster. Ved at det dannes en frykt for overvåking vil dette kunne føre til en selvregulering som kalles *nedkjølingseffekten.* En slik overvåkingsfrykt kan blant annet føre til at mennesker lar vær å søke om hjelp for tabubelagte forhold i frykt for at informasjonen ikke forblir konfidensiell (Datatilsynet, 2020).

> En utilbørlig innblanding i den enkeltes personvern kan både direkte og indirekte begrense den frie utvikling og utveksling av ideer. En krenkelse av den ene rettigheten kan både være årsak og konsekvens av en krenkelse av den andre. (Datatilsynet og teknologirådet, 2014, s. 26).

Nedkjølingseffekten er vanskelig å forske på da det er vanskelig å kvantifisere fravær av en handling, som nedkjølingseffekten ofte manifesteres som. Dette kan også forekomme uten at individet er klar over det selv, og gradvis kan våre ubevisste vaner omgjøres som et resultat av en usikkerhet om hva som lagres om oss og hvordan det brukes (Datatilsynet og teknologirådet, 2014).

Som tidligere empiri har vist er det en betydelig andel av den norske befolkningen som utøver selvsensur som følge av usikkerhet knyttet til myndighetsovervåking (Datatilsynet, 2020). Som følge av usikkerheten for overvåking på internett har halvparten fra personvernundersøkelsen 2020 sagt at de avstår fra å delta i fri meningsutveksling på nett. Én av tre har også svart at de unnlater å søke på ulike informasjon på internett og én av to unnlater å kjøpe ting på nett. Et liberalt, demokratisk samfunn som Norge er tuftet på diverse demokratiske verdier, og en konsekvens av en slik nedkjølingseffekt er en svekkelse av ytrings- og informasjonsfriheten. Digitalisering påvirker også denne effekten i stor grad, ettersom internett samler inn en omfattende mengde informasjon, som samlet kan føre til en svært nærgående kartlegging av enkeltindividers liv. I personvernundersøkelsen fra 2020 blir den nye internettøkonomien også kalt for en «overvåkingsøkonomi» (Datatilsynet, 2020).

5.3.5 Oppsummering

Det er flere utfordringer med samfunnets utvikling i forhold til ivaretakelsen av personvern. Ettersom det eksisterer store mengder informasjon på internett er kravet om ivaretakelse av personopplysninger enda viktigere. Den private sfæren er en menneskerettighet og er en viktig del av grunnlaget for et velfungerende demokrati. Om myndighetenes innsyn i den private sfære øker kan både tillit og maktforhold mellom myndighetene og befolkningen ta skade, og igjen være ødeleggende for demokratiet. Da det også er viktig å ivareta stats- og samfunnssikkerheten i landet er det helt avgjørende å finne en god balansegang. Innføringen av ulike tvangsmidler i forebyggende øyemed reiser mange personvernmessige spørsmål, her eksemplifisert ved innføringen av det skjulte tvangsmiddelet dataavlesning. Det kan antas at det alltid vil forekomme uenigheter i debatten rundt hvilke behov samfunnet har i forhold til personvernet rolle.

Befolkningens holdninger til personvern har på noen områder holdt seg stabile, mens det på andre områder har forekommet store endringer. Den teknologiske utviklingen har ført til at nye problemstillinger har dukket opp som ikke fantes før og kan antas å være årsaken til flere

av utviklingstrendene man ser. Tillit til myndighetene har i stor grad holdt seg på et høyt nivå, med noen variasjoner hos spesielt Etterretningstjenesten, spesielt i etterkant av forslagene om DLD og DGF. Selv om tilliten generelt blir ansett som høy over tid er det markante resultater som tyder på en nedkjølingseffekt i samfunnet. Halvparten av respondentene i 2020 uttalte at de hadde avstått fra bruk av tjenester grunnet usikkerhet rundt hvorvidt personopplysningene deres ble misbrukt. 16% hadde i tillegg unnlatt å gjøre noe på nettet i frykt om at de ble overvåket. Det er tydelig at det eksisterer ulike utfordringer i forhold til personvern og utviklingen samfunnet har gått gjennom de siste 25 årene. Så lenge det fremdeles er usikkerhet rundt tiltak og hvordan angrep i det digitale domenet skal håndteres og hvem som har beslutningsmyndighet, vil personvernet være i en usikker posisjon.

Kapittel 6. Drøfting

I dette kapittelet vil empirien presentert i kapittel 5 drøftes opp mot oppgavens teoretiske grunnlag, presentert i kapittel 3. På lik linje som empirikapittelet er drøftingen delt inn etter forskningsspørsmålene og utgjør dermed strukturen for diskusjonen. Drøftingen vil lede opp til problemstillingen for oppgaven, nemlig hvilke implikasjoner utviklingen av overvåking som sikkerhetstiltak har hatt for personvernet de siste 25 årene. Svaret på problemstillingen vil bli presentert i konklusjonen i kapittel 7.

6.1 Hvordan har overvåking forandret seg de siste 25 årene?

Empirien viser at det har forekommet store endringer i hvordan overvåking har forandret seg de siste 25 årene. Funnene skisserer et stadig mer komplekst risikobilde i Norge, som særlig kommer frem i lys av nye former for trusler og trusselaktører. Utviklingen av ny angrepsmetodikk og skiftet over til det digitale domenet er de største truslene, og utviklingen må sees i lys av hvem som er trusselaktøren, deres intensjon og kapabilitet, og hvordan lovverket rundt overvåking er utformet og utviklet. Empirien retter dermed lyset mot hovedsakelig to utviklingstrekk: 1) et risikobilde preget av teknologisk utvikling og nye trusselaktører, og 2) økt fokus på informasjonsinnsamling fra myndighetene.

6.1.1 Risikobildet i samfunnet

Risikobildet i Norge de siste 25 årene har vært preget av digitalisering og teknologisk utvikling. Med ny teknologi utformes også nye trusselaktører og angrepsmetoder som gjør at myndighetene søker å forme og tilpasse seg situasjonen. Risiko er noe som eksisterer rundt oss til enhver tid, og dreier seg om en usikkerhet rundt hva som vil bli utfallet av en fremtidig hendelse (Aven et al., 2004). I kapittel 3.2.1 ble risiko definert som: «et uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen» (Standard Norge, 2012). Risiko knyttet til tilsiktede, uønskede handlinger kan i stor grad endre seg fra år til år, avhengig av hvordan risikobildet i samfunnet ser ut. I vurderingen av en trussel er det aktørens intensjon og kapasitet som blir vektlagt. En aktørs mulighet til gjennomførelse er også relevant. PST og Etterretningstjenestens arbeidsform er tradisjonelt å avdekke personer eller grupper sin intensjon om å utføre terrorangrep, før de eventuelt går videre og undersøker om vedkommende i tillegg hadde kapasitet og mulighet til å iverksette sine planer (NOU 2012: 14).

Trefaktormodellen, presentert i figur 1, viser hvordan risiko kan bli vurdert basert på forholdet mellom verdi, trussel og sårbarhet (NSM, 2015). På bakgrunn av risikobildet og relevante trusselaktører diskutert i kapittel 5.1.1 og 5.1.2 kan det skisseres ulike scenarier som kan plasseres i trefaktormodellen. Scenariene vil være tenkte situasjonsbeskrivelser der en relevant trusselaktør vil gjennomføre et terrorangrep. Det eksisterer en rekke ulike trusler mot Norge som kommer fra forskjellige trusselaktører med forskjellig intensjon og kapabilitet. Trusselaktørene kan grovt deles inn i to aktører: de tradisjonelle trusselaktørene og de digitale trusselaktørene. De tradisjonelle aktørene bruker fysiske terrorangrep mot en befolkning, mens de digitale trusselaktørene vil gjennomføre angrep i det digitale domenet. Slike angrep kan bli gjennomført med intensjon om å slå ut eksempelvis kritisk infrastruktur i landet, som eksempelvis strømnettet, eller tilegne seg sensitiv informasjon som senere kan misbrukes. Aktørene har forskjellig intensjon og har ulike verdier i hva de ønsker å oppnå. Sårbarhetene kan knyttes opp mot blant annet dårlig beredskap, sorte hull i lovverk, sårbarheter i teknologi og manglende sikkerhetstiltak.

Scenario 1 blir som følger: En ung mann stiger ut av et tog på Oslo Sentralbanestasjon, midt i Oslo sentrum. Han setter fra seg en koffert og beveger seg raskt vekk fra området. Mannen har nylig blitt rekruttert av en profilert terrorgruppe (trusselaktør) og via radikalisering over nett (sårbarhet) skal mannen ha blitt overbevist til å gjennomføre en terroraksjon som vil skape frykt i samfunnet (verdi), da samfunnets verdier strider i mot hans egne. Det er tidlig en fredag ettermiddag, og perrongen er full av personer som er på vei hjem fra jobb. Noen minutter senere detoneres eksplosivene som er plassert i kofferten.

Scenario 2 er inspirert av IT-angrepet som både Stortinget og flere virksomheter ble rammet av i mars 2021. En statlig terrorgruppe (trusselaktør) har beveget seg over til det digitale domenet og planlegger å gjennomføre et cyberterrorangrep mot den norske regjeringen. Ved å benytte seg av et sikkerhetshull i Microsoft sitt program Exchange (sårbarhet), bryter trusselaktørene seg inn og henter ut sensitiv informasjon (verdi) som bryter med sikkerhetsmålene konfidensialitet, integritet og tilgjengelighet for informasjonen. Stortinget utgjør både et sterkt symbolmål og er i tillegg en av de viktigste bærebjelkene for integriteten til norsk suverenitet og til de demokratiske prosessene mellom norske folkevalgte. I tillegg sitter Stortinget på svært sensitiv informasjon som kan være kritisk for Norge og av stor interesse for fremmede staters etterretningstjenester. Ved å se på trusselaktøren sin intensjon

og kapasitet, samt ved bruk av en sårbarhetsanalyse av Exchange, vil det være mulig å kvantifisere risikoen.

Begge scenarioene viser hvilken nytte trefaktormodellen kan ha i å fremlegge risiko for ulike typer terrorangrep. Ved hjelp av kvalitative vurderinger kan det legges vekt på trusler, verdier og sårbarheter når det kommer til risikoen for terrorangrep. Empirien viser hvordan formålet med terrorangrep kan anses for å ha endret seg fra å hovedsakelig ta i bruk tradisjonelle virkemidler, til å i dag i økende grad omhandle tilegnelsen av informasjon og misbruk av denne. Dette er knyttet opp til teknologiutviklingen og de nye verdiene og sårbarhetene i samfunnet. Trusselaktørers evne til å gjennomføre et angrep avhenger i stor grad av deres intensjon og kapabilitet, som med teknologiutviklingen utvikler seg i høy fart. Dette illustreres gjennom myndighetenes stadig nye forslag til nye lover og vedtak. Ved at vi lever i et liberalt demokrati kan trusselaktører dra fordel av hensynet som tas til de demokratiske prinsippene vi lever etter.

Risikopersepsjon

Empirien viser at frykten for terrorangrep og cyberangrep mot styringssystemer har økt i stor grad bare de siste 8 årene, og risikopersepsjonen til befolkningen har dermed endret seg. Trusselen for terrorangrep mot samfunnet har økt, men ved at informasjon blir mer tilgjengelig kan dette også danne et inntrykk av en større trussel enn det som faktisk er tilfellet. Det konstruktivistiske perspektivet på risiko innebærer en menneskelig forståelse og omhandler dermed at risikoforståelsen skapes innenfor ulike kulturer og sosiale konvensjoner (Douglas & Wildavsky, 1982). Mennesker vil altså bli påvirket av det som skjer rundt en, noe som i verste fall kan medføre et urealistisk syn på risiko. Med all tilgang på informasjon fra sosiale medier, nyheter og andre typer medier, vil befolkningens risikopersepsjon i stor grad være bestemmende for hva som godtas gjennomført av myndighetene. Hvorvidt befolkningen ønsker at maktinstansene skal få ta i bruk inngripende verktøy som overvåking for å forhindre terrorisme, vil dermed være avhengig av hvor stor risiko man tror man er utsatt for. Det blir gjennomført et stort antall unntak når det kommer innføring av sikkerhetstiltak for å avverge terrorisme, på bakgrunn av at det oppfattes som en stor risiko, og innebærer alvorlige konsekvenser dersom det skulle forekomme. Oppfattes risikoen som vedvarende i et samfunn kan unntaket bli normen, og det kan stilles spørsmål om terrortrusselen gir en evig unntakstilstand. Barrieren er stor for å fjerne allerede eksisterende lover, noe som dermed vil kunne føre til en holdningsendring i samfunnet.

Foucault sin styringsteori omhandler den praksisen og de prosedyrer og teknikker som har som formål å forme, lede og påvirke menneskets atferd (Dean, 2010). Utviklingen av samfunnets risikobilde og befolkningens risikopersepsjon vitner om at myndighetene har styringsmyndighet overfor befolkningen. Ved utvikling av lovforslag og stadige debatter rundt hvorvidt lovverket må oppdateres for samfunnets beskyttelse mot terrortrusler, i tillegg til påvirkning fra ulike informasjonskilder i samfunnet, følger den generelle risikopersepsjonen til befolkningen i stor grad det nasjonale risikobilde. Hvorvidt dette samsvarer med den faktiske risikoen for terrorangrep i samfunnet er vanskelig å si sikkert. Dean (2010) beskrev governmentality som «fremveksten av en ny form for tenkning og utøvelse av makt i visse samfunn». Denne nye formen for tenkning og maktutøvelse baserer seg på en kombinasjon av styring av økonomi og statistikk i relasjon til lovverk og regulering av befolkningen. For å kunne forme et samfunn preget av velferd, blir det, fra et foucauldiansk perspektiv, tatt i bruk risiko som den nye formen for styring (Mythen & Walklate, 2006).

6.1.2 Informasjonsinnsamling fra myndighetene

Empirien presenterer ulike lovforslag som har blitt lagt frem etter Lund-kommisjonen, som Datalagringsdirektivet, det digitale grenseforsvaret og preaktiv strafferett. De er alle drevet frem av den internasjonale terrortrusselen og kan anses som eksempler på overvåking i nyere tid. Forslagene viser hvordan myndighetene er interessert i innsamling av informasjon om befolkningen, og kan sees i lys av Foucault sine tre aspekter ved governmentality, i tillegg til Foucault sin analyse av panoptisk disiplin.

Det første aspektet ved governmentality er at styringsobjektet alltid vil være befolkningen (Dean, 2010). Her kan DLD og DGF oppfattes som særlig relevant, grunnet at det ved innføring av slike lovverk direkte ville påvirket den norske befolkningen gjennom omfattende datainnsamling enten hos tele- og internettoperatører eller via fiberoptiske kabler. Lover, konstitusjoner og parlamenter inngår i det Foucault beskrev som suveren makt, og innebærer en autoritet over individene innenfor et visst territorium. Disiplinær makt er på en annen side reguleringen av individene innenfor dette territoriet og dette foregår som nevnt, ifølge Foucault, gjennom en risikobasert styringsprosess. Å gjennomføre en slik datainnsamling på bakgrunn av et økonomisk og statistisk aspekt vil kunne bidra til en befolkning med individer som kan optimaliseres i henhold til myndighetenes ønsker. Styringen ville dermed favne om

samfunnet som helhet og enkeltindividene, både ved bruk av suveren og disiplinær makt, men også for å skape helse, velferd og lykke hos befolkningen. Det siste aspektet til Foucault er også relevant i forhold til demokratiske styringsregimer. Foucault mener at for å sikre et optimalt samfunn er det nødvendig med ulike sikkerhetsapparater, noe myndighetene gradvis har bygget opp i det nye overvåkingssamfunnet. Disse apparatene for sikkerhet inkluderer helsesystemer, systemer for utdanning og andre praksiser og institusjoner som må til for å sikre en best mulig ivaretakelse av økonomiske, vitale og sosiale prosesser i en befolkning. I tillegg inkluderes maktinstansene i samfunnet, nemlig PST og Etterretningstjenesten (Dean, 2010). Empirien belyser hvordan samfunnet er preget av sikkerhetsapparater som nevnt ovenfor. For å kunne optimalisere en befolkning er det nødvendig at det eksisterer ulike systemer for å ivareta befolkningen, både når det kommer til befolkningens velferd og sikkerhet, men også deres egenskaper. For at denne formen for styring skal fungere, med optimalisering av befolkningens egenskaper, innføres det dermed inngripende midler for å passe på at det går i riktig retning.

Preaktiv strafferett er også en lovendring som trådte i kraft som en reaksjon på risikoen for terrorangrep i samfunnet. Gjennom denne lovendringen senkes terskelen for straff og overvåkning, og oppmerksomheten gjelder ikke lengre kun konkrete handlinger, men også tankevirksomhet (Engene, 2013). Her ligger det et stort potensial for mye mer overvåking fra myndighetene enn det som har vært politisk akseptert i Norge i årene etter Lund-kommisjonen. Ved innføringen av lovforslag som dette, synliggjøres også prinsippet om panoptikon og den panoptiske disiplin. Foucault mente at panoptisk disiplin var mønsteret bak en ny form for maktmekanisme i samfunnet, og at dette gradvis bidro til å forme det nye overvåkingssamfunnet. Ved at man vet at det er mulig at noen overvåker deg, vil man oppføre seg deretter. Et panoptikon kan i stor grad gjøre befolkningen 'disiplinert', på bakgrunn av at man vet at man kan bli sett. På denne måten blir makten relasjonell og vil fungere automatisk (Nortvedt & Grimen, 2004). Her kan det argumenteres for at samfunnet vi lever i kan regnes som et slags moderne panoptikon. Vi sitter ikke i et tårn med voktere som følger med på oss, men det eksisterer en usynlig overvåking. Snowden-avsløringene tydeliggjorde dette. Foucault beskriver at det foreligger en tett relasjon mellom kunnskap og makt, noe som illustreres i empirien ved at myndighetene stadig forsøker å innhente mer informasjon om befolkningen. At man vet at noen kan følge med på det du foretar deg, kan medføre en frykt for at noen følger med på deg til enhver tid, og kan føre til en nedkjølingseffekt i samfunnet. Dette blir videre belyst i kapittel 6.3.

6.1.3 Delkonklusjon

I lys av diskusjonen ovenfor ønsker jeg å trekke frem at risikobildet i Norge har hatt en utvikling mot det mer komplekse. Verdier, trusler og sårbarheter i samfunnet har økt, noe som gjør at myndighetene ønsker å øke forebyggende sikkerhet for terrorangrep i samfunnet. Ved bruk av trefaktormodellen kan man se hvordan verdier, trusler og sårbarheter kan bidra til å påvirke risiko, og dermed bidra til bevisstgjøring rundt hvilke sikkerhetstiltak som vil være nødvendig for en god styring av en befolkning. Målet til myndighetene er å møte truslene, selv om de er i konstant utvikling. Dette gjennomføres ved forsøk på utvikling av lovverk og utvidelse av fullmakter. Foucault sin teori om governmentality bidrar til å belyse hvordan myndighetene styrer og former befolkningen, gjennom bruk av ulike praksiser. Overvåking som sikkerhetstiltak er en av styringsmetodene til myndighetene. At befolkningen tror at risikoen for terrorangrep mot staten er høy bidrar også til selvstyring ved at de godtar større grad av inngripen ovenfra. Dette tydeliggjøres ved hvordan risikopersepsjonen i samfunnet har endret seg de siste årene.

Myndighetene ønsker i all hovedsak en forvaltning av egenskapene til befolkningen, slik at befolkningen kan leve i et samfunn preget av god økonomi, velferd, helse og utdanning. Dette styres i stor grad av risiko, sammen med lovverk – suveren makt, og regulering av dette – disiplinær makt. Ved innføringen av apparater for sikkerhet kan styringsmyndighetene i tillegg forme befolkningen til å bli den mest optimaliserte versjonen av seg selv, ved blant annet å følge med på befolkningen og hva de foretar seg. Å se på samfunnet som et slags moderne panoptikon er dermed en passende beskrivelse av typen overvåkingssamfunn vi lever i i dag.

6.2 Hvordan har statssikkerhet og samfunnssikkerhet endret seg i forhold til utviklingen til overvåking?

Empirien belyser hvordan statssikkerhet og samfunnssikkerhet har endret seg i tråd med utviklingen av overvåking, både når det gjelder begrepsbetydning, og hvordan dette har påvirket aktørene ansvarlig for å opprettholde disse formene for sikkerhet. Funnene skisserer at gråsonen mellom PST og Etterretningstjenesten vokser i takt med utviklingen av teknologien og det nasjonale risikobildet, og at ansvarsområdene til tjenestene overlapper i

mye større grad enn tidligere. Dette, knyttet opp mot risikopersepsjon, tillit og mistillit, samt frihet versus sikkerhet utgjør den videre drøftingen i kapittelet.

6.2.1 Begrepsbetydning

Som belyst i empirien har sikkerhetsbegrepene forandret seg i løpet av årene og begrepene innebærer i dag andre ting enn de gjorde på slutten av 90-tallet. Sikkerhet er et essensielt begrep når det kommer til hvordan sikkerhetstiltak og metoder for overvåking, samt nye forslag til terrorlovgivning utarbeides av myndighetene. Empirien viser også hvordan det tradisjonelt sett foreligger et skille mellom statssikkerhet og samfunnssikkerhet. Mens statssikkerhet i all hovedsak har vært forankret i maktpolitiske tradisjoner og er forbundet med forsvars- og sikkerhetspolitikk, har samfunnssikkerhet i større grad vært rettet mot det norske rettsapparatet og befolkningens velvære.

Det kan argumenteres for at samfunnets forståelse av begrepene har gått fra å omfatte et objektivt og realistisk perspektiv på risiko til å innebære en mer subjektiv, konstruktivistisk forståelse av begrepene. En slik forståelse innebærer at risiko i større grad blir formet gjennom sosiale interaksjoner, kultur og inntrykk (Clarke & Short, 1993), noe som dermed har bidratt til fokusendringen som har forekommet. Samfunnssikkerhetsbegrepet har nemlig vært formen for sikkerhet som har vært mest i fokus de siste 10 årene. Olsen et al. (2007) argumenterer for at en av årsakene til dette er at en stat er avhengig av et samfunn for å eksistere. En stat på sin side kan forsvinne, men samfunnet vil fremdeles fortsette å eksistere uavhengig. Samfunnssikkerhet blir dermed ansvarlig for å håndtere politikk og tiltak som skal sikre at kritiske samfunnsfunksjoner opprettholdes, og blir dermed ansett som stadig mer relevant.

Som vist i kapittel 6.1 har befolkningens frykt for terrorangrep økt, i takt med det økende risikobildet og det sikkerhetspolitiske landskapet. I arbeidet med å identifisere risikoen for terrorangrep er det nødt til å gjennomføres verdi-, sårbarhets- og trusselvurderinger for å se hvor mye ressurser som burde tas i bruk for å redusere risikoen for terrorangrep. Her er det helt nødvendig at myndighetene er klar over at det alltid vil foreligge en restrisiko, slik at inngrepene ikke blir for ekstreme i kampen mot et risikofritt samfunn. Myndighetene er her nødt til å ta den konstruktivistiske oppfatningen av risiko for terrorangrep i betraktning. Som tidligere beskrevet kan sannsynligheten for maktmisbruk fra myndighetene øke om risikopersepsjonen til befolkningen er høyere enn den faktiske risikoen for terrorangrep. På en

annen side – innfører ikke myndighetene noen form for sikkerhetstiltak kan dette i verste fall føre til fremkomsten av mistillit til myndighetene. Det vil dermed være nødvendig å finne en balanse mellom innføringen av overvåking som sikkerhetstiltak og risikopersepsjonen til befolkningen.

Terrorisme i seg selv kan alene anses som en trussel for menneskerettighetene. Det handler ikke kun om de fysiske konsekvensene av handlinger, men også hvilke psykologiske effekter et terroranslag kan ha på en befolkning. En av myndighetenes viktigste oppgaver når det kommer til sikkerhetstiltak mot terrorisme er dermed å øke befolkningens tillit. Blir risikoen i samfunnet for stor eller oppfattelsen av denne, vil dette påvirke tilliten. For at demokratiske prosesser skal kunne forekomme i et samfunn er tillit et helt essensielt konsept, ettersom det er grunnsteinen i et hvert velfungerende demokrati (Bergsjø et al., 2020). Empirien viser at befolkningen i Norge har svært høy tillit til myndighetene, sammenlignet med resten av Europa. Foucault mente at liberale demokratiske samfunn i stor grad var hyklerske ettersom at samfunnet er bygget på en mistillit til befolkningen, som kommer til syne ved myndighetenes bruk av systematisk overvåking og kontroll (Nortvedt & Grimen, 2004). Men, ettersom tillit og mistillit kan sies å ha en gjensidig avhengighet når det kommer til hvordan de er institusjonalisert i samfunnet, kan dette tolkes som at innføring av sikkerhetstiltak også kan øke tilliten en befolkning har til myndighetene ved at befolkningen føler seg ivaretatt. Her er det nødt til å bli identifisert en fin balanse. På en side – høy risiko for terrorangrep og fravær av sikkerhetstiltak kan føre til en mistillit fra befolkning til myndigheter. På en annen side kan for strenge sikkerhetstiltak også medføre mistillit, ved eksempelvis brudd på menneskerettigheter eller begrensninger i frihet. Begge sider kan på hver sin måte medføre negative konsekvenser for demokratiet. At et samfunn har høy tillit til sine myndigheter kan dermed gjør tillitsgiveren sårbar for maktmisbruk, og dermed er et klart regelverk og tydelig ansvarsområder hos de ulike maktinstansene å anse som helt nødvendig.

6.2.2 Ansvarsområder

Når det forekommer ulike sikkerhetsutfordringer for et samfunn rettferdiggjør myndighetene bruken av ekstraordinære midler for å håndtere dem. Utviklingen av sikkerhet som konsept kan dermed på et vis være årsaken til bruken av ekstreme maktmidler for å håndtere truslene som forekommer. Ved å bruke begreper som sikkerhet i sammenheng med en nødsituasjon hevdes dermed retten til å bruke hva som helst av nødvendige midler for å blokkere en hvilken som helst truende utvikling (Buzan et al., 1998).

For mange liberale, demokratiske samfunn begynner beskyttelsen av eget land å smeltes sammen til én kategori, med alt det innebærer. Stats- og samfunnssikkerhet flyter stadig mer over i hverandre og danner en gråsone, og ansvarsområdene til PST og Etterretningstjenesten overlapper i mye større grad enn tidligere. Grunnet den nye formen for komplekse, digitale trusler er det ikke lengre klart hvem som har jurisdiksjon når det kommer til ulike typer angrep mot landet. Det tradisjonelle skillet kan sies at i hovedsak går ut på det militære versus det sivile og hvordan de ulike apparatene rettferdiggjør bruk av ekstreme maktmidler for å håndtere en sikkerhetsutfordring (Buzan et al., 1998). Tidligere har den militære sektoren i stor grad blitt ansett som aktøren som tar i bruk ekstreme maktmidler. Ettersom den digitale utviklingen medfører at skillet blir mer utydelig, angår dette også i større grad den sivile sektoren og politietaten. Lovforslagene som gjelder for den sivile sektoren tyder på et ønske om flere fullmakter til bruk av mer ekstreme sikkerhetstiltak. Dermed gjelder ikke et slikt tvangsbruk lengre kun den militære sektoren. Samfunnssikkerhet har i utgangspunktet vært innenfor ansvarsområdet til den sivile sektoren, og innebærer en opprettholdelse av trygghet og ivaretakelse av befolkningen i et samfunn (Kveberg & Johnsen, 2013). Ved at det tas i bruk ekstreme maktgrep for å sikre tryggheten til individene i en befolkning kan det dermed argumenteres for at friheten deres blir begrenset.

I kapittel 3 redegjøres det for frihet som en verdi, og det blir regnet som en av verdiene som blir høyest verdsatt i liberale demokratiske samfunn. Det blir allikevel gjort flere inngrep i den individuelle, negative friheten i samfunnene med slike regjeringsregimer til en hver tid. Som nevnt i teorikapittelet er eksempelvis trafikkregler en pålagt begrensning for hva individene i et samfunn kan gjøre. Myndighetene innfører lover og regler som dette for å redusere den eksisterende risikoen i samfunnet. Argumentet ovenfor kan dermed sees fra to perspektiver, der sikkerhet også kan sees på som en bidragsyter til vår frihet (Engen et al., 2016). Ved at befolkningen godtar mer inngripen fra myndighetene, og godtar at overvåking som sikkerhetstiltak blir tatt i bruk av maktinstansene, oppnås det frihet fra kaos. Om det blir gjennomført et terroranslag kan det forventes at det forekommer kaos for en del av befolkningen, og oppnår man frihet fra dette kan dermed sikkerhet betraktes som en bidragsyter til befolkningens individuelle frihet.

Spørsmålet som blir stilt er dermed hvor mye sikkerhet som kan etableres, samtidig som friheten til befolkningen blir opprettholdt. En av utfordringene som oppstår ved innføring av

sikkerhetstiltak mot terrorisme er at befolkningen ikke har noen sjanse for å forutse slike angrep selv. Risikoen for slike hendelser vil dermed være umulig for individer å kontrollere, og medfører at befolkningen lettere vil godta tiltak som myndighetene ønsker å innføre (Engen et al., 2016). Som nevnt i kapittel 6.1 kan samfunnet sees på som et slags moderne panoptikon. Det er ingen fysiske voktere som ser på deg, men overvåkingen forekommer og vil i all hovedsak være usynlig. Konsekvenser av sikkerhetstiltakene vil dermed ikke ramme oss direkte, da vi ikke kan se de. Dette danner en god grobunn for en overvåkingskultur i samfunnet, og vil gi tiltak som dette en større gjennomføringskraft.

For å forstå Foucault sin teori om governmentality påpekes det at det liberalistiske fokuset på det frie individet er en helt essensiell del av teorien, og han mente at ettersom individet som styres er en aktør, vil dermed aktøren besitte en grunnleggende frihet (Foucault, 2007). Dean (2010) påpeker den ambivalensen som dermed oppstår mellom et fritt individ og styringsmaktene i et liberalt regjeringsregime. Ettersom styringsmaktene bidrar til å forme og organisere forholdene som er nødvendige for at et individ kan være fritt, vil dermed individet samtidig være styrt. «In order to act freely, the subject must first be shaped, guided and molded into one capable of responsibly exercising that freedom through systems of domination» (Dean, 2010, s. 193).

6.2.3 Delkonklusjon

Både stats- og samfunnssikkerhet har gjennomgått store endringer siden slutten av 90-tallet. I tiden da Lund-kommisjonen eksisterte var det enda ikke kastet lys på samfunnssikkerhet i Norge, som de siste 10 årene er formen for sikkerhet som har fått mest fokus. Ved at man ser sikkerhetsbegrepene og hvordan de forstås i lys av befolkningens risikopersepsjon og deres trygghet kan det dannes forståelse for hvor nødvendig det er å ta deres perspektiv i betraktning. Innfører ikke myndighetene noen form for sikkerhetstiltak om risikopersepsjonen for terrorangrep er høy kan dette føre til mistillit hos befolkningen, men dette kan også forekomme hvis sikkerhetstiltakene blir for strenge, der begge deler i verste fall kan ha konsekvenser for demokratiet.

Ansvarsområdene til PST og Etterretningstjenesten har også forandret seg når det kommer til overvåking. Ved samfunnets stadige digitalisering har truslene blitt mer komplekse og grenseoverskridende. Det vil dermed være utfordrende for tjenestene å håndtere samme hendelse når de selv har ulike oppgaver og hjemmelsgrunnlag. Utviklingen kan tyde på at

begge sektorene har gått over i hverandres tradisjonelle ansvarsområder der den militære i større grad ønsker å operere innenlands, mens den sivile vil ha fullmaktsutvidelser for bruk av ekstreme maktmidler. Ettersom samfunnssikkerhet skal verne befolkningen mot hendelser som truer grunnleggende verdier, kan slike ekstreme maktgrep for å sikre denne tryggheten føre til en begrenset frihet hos befolkningen. Sikkerhetstiltak kan dermed på en side sees på som noe som begrenser befolkningens individuelle frihet, men kan på en annen side også sees på som en bidragsyter til frihet ved at det fritar befolkningen fra kaos. At befolkningen godtar inngrep i friheten sin kan legge til rette for en overvåkingskultur i samfunnet, som også vil gi lovforslag om ulike sikkerhetstiltak for terrorisme en større gjennomføringskraft. Spørsmålet blir dermed hvor balansegangen mellom frihet og sikkerhet skal gå – en utfordring som kompliseres med uklare skiller mellom maktinstansene i samfunnet.

6.3 Hva er utfordringer med denne utviklingen i forhold til personvern?

Personvern regnes som en veldig viktig demokratisk verdi. Ved at samfunnet stadig utvikler seg når det kommer til teknologi og globalisering medfører dette også at det trengs nye former for sikkerhetsmekanismer, noe som kan skape utfordringer for verdier som nettopp personvernet. Empirien brer over personvern som et ideal, innføringen av skjulte tvangsmidler for å møte dagens komplekse trusselbilde, befolkningens syn på personvern og utfordringer en slik utvikling kan ha. Videre vil drøftingen fokusere på særlig to utfordringer som gjør seg gjeldende når det kommer til personvern: bruk av skjulte tvangsmidler og nedkjølingseffekten som kan forekomme ved overvåking, i tillegg til en avsluttende drøfting rundt myndighetenes intensjon og effekt av tiltak.

6.3.1 Skjulte tvangsmidler

Personvern regnes som et av liberale demokratiers hovedidealer, men personvernet er ikke absolutt. EMK art. 8 (1) legger vekt på at alle har rett på sitt eget privatliv. Samtidig påpeker også konvensjonen art. 8 (2) at personvernet nettopp ikke er absolutt, ved at inngrep i personvernet kan skje, dersom det er nødvendig med hensyn til den nasjonale sikkerheten, offentlig trygghet eller landets økonomiske velferd (Personopplysningsloven, 2018). Dermed vil det kunne innføres bruk av skjulte tvangsmidler til tross for det eksisterende europeiske lovverket som skal sikre våre menneskerettigheter og demokratiske verdier. Om bruk av skjulte tvangsmidler blir lovlig kan dette medføre ulike konsekvenser. Ved at lovlige, skjulte etterretnings- og etterforskningsmetoder blir utvidet går dette hånd i hånd med en utvidelse av

statens makt overfor den enkelte borger og de vil da fratas deler av sine rettigheter og friheter (NOU 2015: 13). Bruken av skjulte tvangsmidler vil som nevnt medføre inngrep i enkeltmenneskers personvern, men også selve eksistensen av regler som åpner for slikt tvangsmiddelbruk kan medføre inngrep overfor alle som kan rammes av dem, uavhengig av om reglene faktisk brukes.

Wessel-Aas (2012) påpeker at jo mer av befolkningens atferd som blir regulert, med argumentasjon i økt trygghet og samfunnsvern, jo mindre spillerom blir det for borgerne til å utfordre makten om nødvendig. Foucault (2007) ville ansett dette som en del av governmentality, der regulerte atferdsmønstre hos befolkningen etter hvert vil bli sett på som en egeninteresse hos individene. Om samfunnets risikopersepsjon innebærer at terrortrusselen mot samfunnet er stor, vil dette føre til en tro om at sikkerhetstiltak fra myndighetene er en nødvendighet for egen sikkerhet. På samme måte vil en befolkning tro at inngripen i eget personvern er en nødvendighet, og dermed opptre disiplinært i forhold til myndighetenes ønsker.

6.3.2 Nedkjølingseffekt

Myndighetene sitter på stadig mer informasjon vedrørende sine borgere, og personvernets rolle omhandler i stor grad forhindring av maktmisbruk ovenfra og ned. Foucault (2007) la som nevnt mye av fokuset fra sin analyse på kunnskap og makt. Jo mer kunnskap og informasjon man besitter, jo mer makt vil kunne misbrukes overfor andre. Foucault argumenterte for at det eksisterer to fremstillinger av makt som kan anses som relevante for moderne styringsformer. Den første omhandler nettopp dette, relasjonen mellom kunnskap og makt. Han argumenterte for at den panoptiske disiplinen, som han regnet som en ny form for maktmekanisme, spredte seg til alle samfunnets institusjoner og arkitektur og dermed gjennomsyret samfunnet. I dag kan det heller sies at vi lever i et slags moderne panoptikon. I motsetning til panoptikon slik Foucault beskriver det eksisterer det ikke lengre fysiske voktere som følger med på alt du gjør, men i stedet en usynlig overvåking basert på samme prinsipp. For å kunne utøve en slik makt er dermed kunnskap om individene makten skal utøves overfor helt essensielt (Nortvedt & Grimen, 2004).

Nedkjølingseffekt kan som nevnt i kapittel 6.1 knyttes til en form for panoptisk makt i samfunnet. En nedkjølingseffekt omhandler nettopp at folk holder seg fra å ytre meninger

eller foreta valg de ellers ville tatt om de ikke trodde de ble overvåket. En slik effekt kan dog være vanskelig å måle. Ut fra personvernundersøkelsene presentert i empirien kan det forstås som at nedkjølingseffekten i samfunnet er tilsynelatende svak. Allikevel kommer det frem at hele 16% har unnlatt å gjøre enkelte handlinger på nett fordi de er redde for at noen følger med på hva de gjør, noe som er et høyt antall til å være i et liberalistisk demokrati. At det blir vanligere med en skjult overvåking som sikkerhetstiltak mot terror kan medføre en slik nedkjølingseffekt i samfunnet, som også kan tolkes for å være en form for selvstyring hos individene i befolkningen. Myndighetene etablerer på et vis en styringskultur og etablerer på denne måten ulike måter å tenke og handle på. Dette gjelder alle normale, 'disiplinære' handlinger i samfunnet, som å gå på skole, spise sunt, bruke prevensjonsmidler osv., og disse styrte tankemåtene og handlingene blir ansett som egeninteresse hos individene i befolkningen (Dean, 2010).

6.3.3 De gode borgerne

Ved å ta i bruk Foucault sitt maktbegrep er det nødvendig å kaste lys på det andre aspektet av makt Foucault la mye fokus på, nemlig den produktive makten. Denne formen ser på, som navnet tilsier, hvordan makt også kan være produktiv, heller enn å kun sette grenser for hva som kan gjøres (Grimen, 2010). Begrepet innebærer hvordan myndighetene kan styre gjennom å forme sinn og atferdsmønstre hos befolkningen. Det er vanskelig å forutse alle implikasjoner ulike tiltak kan ha. Tiltak kan ha både positive og negative effekter, i tillegg til at de kan være innført med både gode og dårlige intensjoner. Bruk av overvåking i samfunnet kan alltid diskuteres om er ment i befolkningens beste velgående, for å sikre individene fra utenforstående trusler, eller om det i større grad handler om kontroll. I kapittel 3 ble den produktive makten eksemplifisert ved hvordan individer ble drillet til å bli «gode pasienter» i møte med diabetes og selvbehandlingsregimet som medfølger. Dette kan sammenlignes med hvordan individene i en befolkning kan bli «gode borgere» ved å bry seg om sin egen sikkerhet, og dermed godta større inngripen fra myndighetene. Hausken et al. (2014) påpeker i sin bok at det har forekommet en utvikling fra at det søkes beskyttelse i menneskerettighetene fra myndighetene til at det søkes beskyttelse i menneskerettighetene hos myndighetene, noe som sammenfaller med empirien presentert i kapittel 5.3.3. Befolkningen ønsker i større grad at myndighetene skal bidra til beskyttelse mot andre borgere og retten til sikkerhet. Foucault poengterer at denne tendensen har med at befolkningens atferdsmønstre har blitt formet av myndighetene å gjøre. Denne utviklingen

tyder dermed på at villigheten for inngrep er større, da fokus på sikkerhet blir viktigere enn fokus på personvern.

6.3.4 Delkonklusjon

Det forekommer hovedsakelig to hovedutfordringer med denne utviklingen i forhold til personvern: maktmisbruk fra myndighetene og nedkjølingseffekt hos befolkningen. Foucault sin teori om governmentality bidrar til å belyse hvordan myndighetene ikke kun styrer befolkningen via en disiplinær og suveren form for makt, men i større grad manipulativt former befolkningen til å tro at valg de tar er egeninteresser, og kan sees på som en annen form for maktmisbruk fra høyere hold. Dette fremstår som en utfordring grunnet at personvernets rolle i stor grad handler om å forhindre et slikt maktmisbruk. Videre diskuteres makt opp mot kunnskap, og hvordan en konstant datainnsamling hos befolkningen kan medføre en nedkjølingseffekt i samfunnet. Denne effekten kan knyttes opp til en panoptisk disiplin. Konsekvenser av dette kan være nettopp en slik form for selvstyring eller selvkontroll, der folk unngår å utføre handlinger i frykt for å bli overvåket. Hvilke intensjoner myndighetene har og hvilke implikasjoner tiltak kan ha er vanskelig å svare på sikkert, da både intensjoner og tiltak kan overlappe seg selv og hverandre. Det utviklingen tyder på er derimot at befolkningen stadig søker mer sikkerhet hos myndighetene, som kan antas at vil føre til en større aksept for inngrep i eget privatliv og personvernet til befolkningen.

Kapittel 7. Konklusjon

I dette kapittelet avsluttes masteroppgaven. Kapittelet skal bidra til å svare på problemstillingen:

Hvilke implikasjoner har utviklingen av overvåking som sikkerhetstiltak hatt for personvernet de siste 25 årene?

Oppgavens problemstilling tar stilling til en lang tidsperiode og den gir helt klart et sammensatt årsaksbilde til hvordan situasjonen er og har forandret seg i løpet av perioden. I det ovenstående er det kun trukket frem et utvalg av relevante endringer som følge av de siste 25 års terrorbekjempelsespolitikk. Funnene fra oppgaven viser at utviklingen har medført ulike implikasjoner for personvern som demokratisk verdi. Nedenfor blir det presentert flere av funnene som anses som særlig relevante for å bidra til å svare på oppgavens problemstilling.

Personvernet har gått gjennom et betydelig rolleskifte de siste 25 årene, grunnet faktorer som teknologisk utvikling, globalisering og et økende ønske om kriminalitetsbekjempelse hos maktinstansene i samfunnet. Det økte trusselnivået i samfunnet, samt utviklingen av angrepsmetodikken tatt i bruk, er også naturlige årsaker til ønsket om å innføre mer inngripende tiltak for å beskytte befolkningen. Dette medfører at myndighetene stadig griper seg lengre inn i individenes private sfærer, ved utformingen og bruk av skjulte tvangsmidler som overvåking. Overvåking kan på flere måter oppfattes som at myndighetene sitter på en implisitt mistillit til befolkningen og dermed har behov for å følge med på hva de foretar seg. Befolkningen må dermed legge sin lit til at myndighetene ikke misbruker makten de erverver. Idealet om et liberalistisk demokrati, der befolkningen først og fremst skal ha kontroll med myndighetene, blir på denne måten ikke levd opp til.

Frihet og individualitet i et samfunn er også det som gjør samfunnet sårbart. Det er dermed et inngravert spenningsfelt mellom myndighetenes behov for kriminalitetsbekjempelse og individets rettigheter i et samfunn. Myndighetene har et syn på at inngripende tiltak er nødvendig for å ivareta stats- og samfunnssikkerheten, men da delvis på bekostning av individenes personvern. På dette vis tolkes myndighetenes oppgave om å beskytte befolkningen på forskjellige måter; enten individorientert eller til fellesskapets beste.

Individorientert innebærer da et større fokus på vern av individenes private sfære, mens det fellesskapsorienterte perspektivet handler om frihet fra kaos, og dermed en innføring av stadig mer alvorlige sikkerhetstiltak.

Funnene fra studien viser noen tydelige konsekvenser av hvordan en slik innføring har påvirket personvern. Ved å se på personvernundersøkelsene kom det frem at nedkjølingseffekten har begynt å slå rot i samfunnet. Selv om en effekt som denne ikke har vært synlig i stor skala for befolkningen de siste 25 årene indikerer funnene at dette vil bli et større problem i tiden fremover, noe som i et fremtidsperspektiv kan medføre alvorlige, negative konsekvenser. Det er derimot viktig å påpeke at selv om noe har en negativ effekt ikke nødvendigvis betyr at det ikke kan medføre noe positivt i tillegg. Ved å se dette i sammenheng med sikkerhetsbekjempelse kan en nedkjølingseffekt potensielt også hindre mennesker i å utføre ulovlige handlinger, som i et fellesskapsorientert perspektiv kan oppfattes som noe positivt.

Maktinstansene i samfunnet har tydelig jobbet iherdig for å modne sin tilnærming til styring av risiko for alvorlig kriminalitet de siste 25 årene. Utvidelser av ulike kriminalitetsbekjempende metoder angår både samfunnet som helhet, men også det enkelte individ, og dermed kreves det også en annen form for lovendringsarbeid for å sikre at hensyn utover myndighetenes egne, blir ivaretatt på en forsvarlig måte. Dette arbeides kontinuerlig med. Ivaretakelsen av personvern er, i tillegg til at det er nedfelt i Grunnloven § 102, forankret i EMK, art. 8 og personopplysningsloven, og nytt lovverk skal dermed være godt argumentert for på en nøyaktig måte for å bli vedtatt og innført. Ved at raten for terrorangrep i vestlige land har økt og medført dette fokuset på sikkerhet i samfunnet, har dette også medført et økende fokus på personvern, noe GDPR er et godt eksempel på. Å ha åpen dialog mellom myndigheter og befolkning kan medføre en større forståelse for hva som er behovet i samfunnet og mål man ønsker å oppnå. Dette er et stort fremskritt fra da Lund-kommisjonen ble dannet for å avdekke maktmisbruket av ulovlige overvåkingsmetoder, oppsummert i Lund-rapporten fra 1996, og illustrerer hvordan negative konsekvenser også kan ha positive sider.

Med formål om å undersøke hvilke implikasjoner utviklingen av overvåking som sikkerhetstiltak har hatt for personvernet de siste 25 årene, kan funn i denne studien peke mot at utviklingen av overvåking har medført ulike negative implikasjoner for personvernet, men

at deler av utviklingen også har hatt positive effekter på samfunnet som helhet. Ved et økt fokus på hjemmelsgrunnlaget til myndighetene, vil det bli lettere for befolkningen å opprettholde en kontroll med myndighetene. På denne måten vil det og bli vanskeligere med maktmisbruk ovenfra og ned. Resultatene tyder også på at nedkjølingseffekten i samfunnet øker, men som beskrevet er dette en utrolig vanskelig faktor å måle. Åpenhet innenfor sektorene er dermed helt essensielt for at samfunnet fremover beveger seg i riktig retning.

7.1 Videre forskning

Denne oppgaven har belyst ulike utfordringer som er knyttet til temaet for oppgaven, nemlig personvern og overvåking. Bruk av slike inngripende sikkerhetstiltak og demokratiske prinsipper er emner som antas å ta stadig større plass i både den nasjonale og internasjonale sikkerhetspolitikkdebatten i årene som kommer og det vil dermed være nødvendig med mer forskning på temaet. Nedkjølingseffekt er en av effektene som jeg mener viktig å sette ekstra fokus på i årene som kommer, selv da en slik effekt i samfunnet er vanskelig å måle. Det kan antas at jo mer overvåking og kontroll som innføres fra myndighetene, jo sterkere vil en slik effekt bli. Dette kan dermed medføre store konsekvenser for et åpent demokrati, basert på ytringsfrihet, rettssikkerhet og personvern, som de demokratiske prosessene er helt avhengig av at fungerer.

I sammenheng med overvåking i forhold til demokratiske prinsipper vil det også være spennende å forske videre på hvordan sosiale medier blir tatt i bruk til etterretningsformål. Sosiale medier er opprettet for at individer skal kunne formidle frie ytringer og intern kommunikasjon i grupper. Ved å benytte åpen etterforskning via disse mediene til etterretningsformål vil dette kunne bryte med ytringsfriheten. Dermed ville det vært interessant å videre undersøke hvilke konsekvenser dette kan medføre for liberale demokratier, som eksempelvis Norge.

Referanseliste

Andreassen, T. A. (2013, 26. oktober). Her er Edward Snowdens mest omtalte avsløringer. *Aftenposten*. https://www.aftenposten.no/verden/i/bKV6l/her-er-edward-snowdens-mest-omtalte-avsloeringer

Aven, T. (2019, 26. september). Risiko. I *Store norske leksikon.* https://snl.no/risiko

Aven, T., Boyesen, M., Njå, O., Olsen, K. H., & Sandve, K. (2004). *Samfunnssikkerhet*. Universitetsforlaget.

Bergsjø, H., Windvik, R., & Øverlier, L. (2020). *Digital sikkerhet. En innføring.* Universitetsforlaget

Blaikie, N., & Priest, J. (2019). *Designing social research*. Polity Press.

Busmundrud, O., Maal, M., Kiran, J. H., & Endregard, M. (2015). *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger* (00923). https://publications.ffi.no/nb/item/asset/dspace:2503/15-00923.pdf

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security. A new framework for analysis*. Lynne Rienner Publishers.

Clarke, L., & Short, J. F. J. (1993). Social Organization and risk: Some current controversies. *Annual review of sociology, 19*, 375-399.

Datatilsynet. (2014). *Personvernundersøkelsen. Samlerapport fra personvernundersøkelsen 2013/2014*. https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/rettigheter-og-plikter/rapporter/personvernundersokelsen/samlerapport-personvernundersokelsen.pdf

Datatilsynet. (2018, 30. oktober). *Iverksette styringssystem for informasjonssikkerhet*. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/iverksette-styringssystem-for-informasjonssikkerhet/

Datatilsynet. (2019a, 17. juli). *Hva er personvern?* https://www.datatilsynet.no/rettigheter-og-plikter/hva-er-personvern/

Datatilsynet. (2019b, 29. mai). *Om personopplysningsloven med forordning og når den gjelder*. https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/om-personopplysningsloven-og-nar-den-gjelder/

Datatilsynet. (2020). *Personvernundersøkelsen 2019/2020*. https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/personvernundersokelser/personvernundersokelsen-20192020/

Datatilsynet og teknologirådet. (2014). *Personvern. Tilstand og trender*. https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/rettigheter-og-plikter/rapporter/persovern_tilstandogtrender_2014.pdf

Dean, M. (2010). *Governmentality. Power and rule in modern society* (2. ed.). Sage Publications.

Digitaliseringsdirektoratet. (2020). *Internkontroll i praksis - informasjonssikkerhet. Sikkerhetstiltak.* (Versjon 1.5). https://internkontroll-infosikkerhet.difi.no/godt-vite/risikohandtering/sikkerhetstiltak

Douglas, M., & Wildavsky, A. (1982). *Risk and culture: An essay on the selection of technological and environmental dangers*. University of California Press.

DSB. (2019). *Analyser av krisescenarioer 2019*. Direktoratet for samfunnssikkerhet og beredskap. https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf

Dæhlen, M. (2017, 20. juli). *Den femte digitaliseringsbølgen - fra data til innsikt*. Titan.uio.no. https://titan.uio.no/forskning-og-vitenskap-informatikkikt-innovasjon-utdanning-blogg-blogg-blogg/2017/den-femte-digitaliseringsbolgen-fra-data-til-innsikt

Ekspertgruppen for Forsvaret av Norge. (2015). *Et felles løft*. Forsvarsdepartementet. https://www.regjeringen.no/globalassets/departementene/fd/dokumenter/et-felles-loft-webversjon.pdf

Eliassen, I. (2014). Varsleren som jages som spion. *Stavanger Aftenblad*. https://www.aftenbladet.no/utenriks/i/v1a0l/varsleren-som-jages-som-spion

Engen, O. A. H., Kruke, B. I., Lindøe, P. H., Olsen, K. H., Olsen, O. E., & Pettersen, K. A. (2016). *Perspektiver på samfunnssikkerhet*. Cappelen Damm akademisk.

Engene, J. O. (2013). Mer overvåkning, mer kontroll - noen utviklingstrekk etter 22. juli 2011. *Tidsskrift for samfunnsforskning, 54*(2), 233-244. https://www.idunn.no/tfs/2013/02/mer_overvaaking_mer_kontroll_-_noen_utviklingstrekk_etter_2

EOS-utvalget. (u.å.). *Hva kontrollerer vi?* https://eos-utvalget.no/hjem/om-eos/hva-kontrollerer-utvalget/

Epinion. (2016). *Befolkningsundersøkelse om risikopersepsjon og beredskap i Norge*. Direktoratet for samfunnssikkerhet og beredskap. https://www.dsb.no/globalassets/dokumenter/nyheter/rapport_bu_2016.pdf

Etterretningstjenesteloven. (2020). *Lov om etterretningstjenesten*. LOV-2020-06-19-77. Hentet fra https://lovdata.no/dokument/LTI/lov/2020-06-19-77

Etterretningstjenesten. (2015). *FOKUS 2015*. https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/rapporter/Fokus%202015.pdf/_/attachment/inline/4a07a5a6-9994-4e28-96ea-c22b7d364a00:4ea88245ef7a52d712a0ff850de0402918ed521a/Fokus%202015.pdf

Flotz, B. C. (2004). Cyberterrorism, computer crime, and reality. *Information management & computer security, 12*(2), 154-166. https://doi.org/10.1108/09685220410530799

Forsvarsdepartementet og Justis- og beredskapsdepartementet. (2018). *Støtte og samarbeid. En beskrivelse av totalforsvaret i dag*. https://www.regjeringen.no/contentassets/5a9bd774183b4d548e33da101e7f7d43/stotte-og-samarbeid-en-beskrivelse-av-totalforsvaret-i-da.pdf

Foucault, M. (2007). *Security, territory, population: Lectures at the Collège de France, 1977-78*. Palgrave Macmillan.

Friis, K., & Hansen, V. V. (2020). Det haster med ny etterretningslov. *Aftenposten*. https://www.aftenposten.no/meninger/kronikk/i/VbmVbd/det-haster-med-ny-etterretningslov-karsten-friis-og-vegard-valther-h

Graver, H. P., & Hardborg, H. (2015). *Datalagring og menneskerettighetene: Utredning til Justisdepartementet og Samferdselsdepartementet*. https://www.regjeringen.no/contentassets/93528bcf984a48a2a89c89cf757b35ef/utredningdldsdjd2015.pdf

Grimen, H. (2010). Michel Foucault - styring, makt og motstand. I J. Pedersen (Red.), *Moderne politisk teori*. Pax Forlag.

Grunnloven. (1814). *Kongeriket Norges Grunnlov*. FOR-2020-05-29-1088. Hentet fra https://lovdata.no/dokument/NL/lov/1814-05-17

Gulløy, E. (1997). *Undersøkelse om personvern: Holdninger og erfaringer 1997*. Statistisk sentralbyrå. https://www.ssb.no/a/histstat/not/not_9748.pdf

Hamnes, L. (2010). - *Stuxnet er et militært våpen*. Teknisk Ukeblad. https://www.tu.no/artikler/stuxnet-er-et-militaert-vapen/234018

Haugsgjerd, A., & Segaard, S. B. (2020). *Politisk tillit, lokaldemokrati og legitimitet. Kunnskapsstatus og utviklingstrekk* (2020: 6). Institutt for samfunnsforskning. https://www.regjeringen.no/contentassets/9d84337e0d2541749f13aa8c7e942b04/politisk_tillit_lokaldemokrati_og_legitimitet.pdf

Hausken, L., Yazdani, S. R., & Haagensen, T. K. (2014). *Fra terror til overvåking: Overvåking i Norge, et kritisk prospekt*. Vidarforlaget.

Honneth, A. (2015). *Freedom's right. The social foundations of democratic life*. Columbia University Press.

Instruks for Politiets sikkerhetstjeneste. (2005). *Instruks for Politiets sikkerhetstjeneste*. FOR-2013-09-27-1139. Hentet fra https://lovdata.no/dokument/INS/forskrift/2005-08-19-920

Ipsos. (2020). *Befolkningsundersøkelse om norske husholdningers bevissthet og adferd knyttet til egenberedskap*. Direktoratet for samfunnssikkerhet og beredskap. https://www.dsb.no/globalassets/dokumenter/rapporter/andre-rapporter/rapport---befolkningsundersokelse-om-husholdningers-egenberedskap-2020.pdf

ISE Bloggers. (2017). *Unpacking cyber terrorism*. Office of the director of national intelligence. https://www.dni.gov/index.php/careers/careers-features/129-uncategorised/2497-unpacking-cyber-terrorism

Johannesen, A., Christoffersen, L., & Tufte, P. A. (2016). *Introduksjon til samfunnsvitenskapelig metode*. Abstrakt.

Joseph, J. (2009). Governmentality of what? Polulations, states and international organisations. *Global Society, 23*(4), 413-427. https://doi.org/10.1080/13600820903198685

Justis- og beredskapsdepartementet. (2012). *Høring –kriminalisering av forberedelse til terrorhandling, utvidet adgang til tvangsmiddelbruk, og endringer i straffeloven 1902 § 60 a*. Regjeringen. https://www.regjeringen.no/contentassets/c0e54a810414447384bc2468b82ed41d/horingsnotat.pdf

Kleven, Ø. (2016). *Samfunnsspeilet* (2/2016). Statistisk sentralbyrå. https://www.ssb.no/kultur-og-fritid/artikler-og-publikasjoner/_attachment/269579?_ts=1555305a1f0

Kveberg, T., & Johnsen, S. T. (2013). *Cyberdomenet, cybermakt og norske interesser* (FFI-rapport 2013/02712). https://publications.ffi.no/nb/item/asset/dspace:2390/13-02712.pdf

Lyon, D. (2003). *Surveillance after September 11*. Polity Press.

Lyon, D. (2007). *Surveillance studies: An overview*. Polity Press.

Lyon, D. (2015). *Surveillance after Snowden*. Polity Press.

Lysne II-utvalget. (2016). *Digitalt grenseforsvar (DGF)*. Forsvarsdepartementet. https://www.regjeringen.no/globalassets/departementene/fd/dokumenter/lysne-ii-utvalgets-rapport-2016.pdf

Mathisen, G. (2013). Samler seg om sikring mot cyberterror. *Forskning.no* https://forskning.no/krig-og-fred-kriminalitet-internett/samler-seg-om-sikring-mot-cyberterror/588974

Meld.St. 10 (2016-2017). *Risiko i et trygt samfunn. Samfunnssikkerhet.* Justis- og beredskapsdepartementet.

https://www.regjeringen.no/contentassets/00765f92310a433b8a7fc0d49187476f/no/pdfs/stm201620170010000dddpdfs.pdf

Meld.St. 17 (2001-2002). *Samfunnssikkerhet. Veien til et mindre sårbart samfunn.* Justis- og politidepartementet. https://www.regjeringen.no/contentassets/ee63e1dd1a16409fa0bb737bfda9279a/no/pdfa/stm200120020017000dddpdfa.pdf

Meld.St. 29 (2019-2020). *Politimeldingen - et politi for fremtiden.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/3fab938bb49b434f946bdd0b6fe6db13/no/pdfs/stm201920200029000dddpdfs.pdf

Menneskerettsloven. (1999). *Lov om styrking av menneskerettighetenes stilling i norsk rett*. LOV-1999-05-21-30. https://lovdata.no/dokument/NL/lov/1999-05-21-30/*#KAPITTEL_emk

Miller, P. B., & Rose, N. (1986). *The power of psychiatry*. Polity.

Mythen, G., & Walklate, S. (2006). Criminology and terrorism. Which thesis? Risk society or governmentality? *The british journal of criminology, 46*(3), 379-398. https://www.jstor.org/stable/23639354?seq=9#metadata_info_tab_contents

NHO. (2018). *Verden og oss: Næringslivets perspektivmelding 2018*. Næringslivets hovedorganisasjon. https://www.nho.no/siteassets/publikasjoner/naringslivets-perspektivmelding/pdf-er-sept18/nho_perspektivmeldingen_5_digitalisering.pdf

Nortvedt, P., & Grimen, H. (2004). *Sensibilitet og refleksjon. Filosofi og vitenskapsteori for helsefag*. Gyldendal Akademisk.

NOU 1999: 27. (1999). *«Ytringsfrihed bør finde Sted». Forslag til ny Grunnlov § 100*. Justis- og politidepartementet. https://www.regjeringen.no/contentassets/026a9879891a4972b019ce10f20561fe/no/pdfa/nou199919990027000dddpdfa.pdf

NOU 2000: 24. (2000). *Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*. Justis- og politidepartementet. https://www.regjeringen.no/contentassets/1c557161b3884335b4f9b89bbd32b27e/no/pdfa/nou200020000024000dddpdfa.pdf

NOU 2006: 6. (2006). *Når sikkerheten er viktigst*. Justis- og politidepartementet. https://www.regjeringen.no/contentassets/c8b710be1a284bab8aea8fd955b39fa0/no/pdfs/nou200620060006000dddpdfs.pdf

NOU 2009: 15. (2009). *Skjult informasjon - åpen kontroll*. Justis- og politidepartementet. https://www.regjeringen.no/contentassets/ac3de9f4288f481e8d6b7971a82310d1/no/pdfs/nou200920090015000dddpdfs.pdf

NOU 2012: 14. (2012). *Rapport fra 22. juli-kommisjonen* https://www.regjeringen.no/contentassets/bb3dc76229c64735b4f6eb4dbfcdbfe8/no/pdfs/nou201220120014000dddpdfs.pdf

NOU 2015: 13. (2015). *Digital sårbarhet - sikkert samfunn.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

NOU 2016: 19. (2016). *Samhandling for sikkerhet. Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid.* Forsvarsdepartementet. https://www.regjeringen.no/contentassets/816d557c6ab24493a1101837cc2e1cf8/nou-2016-19-samhandling-for-sikkerhet.pdf

NOU 2017: 9. (2017). *Politi og bevæpning. Legalitet, nødvendighet, forholdsmessighet og ansvarlighet*. Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/1a1e793002264d9cb5b940e673622984/no/pdfs/nou201720170009000dddpdfs.pdf

NOU 2018: 14. (2018). *IKT-sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet*. Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/0d408600df2f4738a9bbb85040b02b59/no/pdfs/nou201820180014000dddpdfs.pdf

NOU 2020: 4. (2020). *Straffelovrådets utredning nr. 1 - Kriminalisering av deltakelse i og rekruttering til kriminelle grupper*. Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/b73bc67eae2b4de29af8e3a45f5b8999/no/pdfs/nou202020200004000dddpdfs.pdf

NSM. (2003). *Risikovurdering 2003*. https://nsm.no/getfile.php/133792-1592988787/Demo/Dokumenter/Rapporter/rst_2003.pdf

NSM. (2005). *NSMs risikovurdering 2005, ugradert versjon*. https://docplayer.me/7354719-Nsms-risikovurdering-2005-ugradert-versjon.html

NSM. (2010). *Rapport om sikkerhetstilstanden 2010*. https://nsm.no/getfile.php/133768-1592988366/Demo/Dokumenter/Rapporter/rst_2010.pdf

NSM. (2015). *Sikkerhetsfaglig råd*. https://www.regjeringen.no/globalassets/departementene/fd/dokumenter/rapporter-og-regelverk/nsm-sikkerhetsfaglig_raad_2015_web.pdf

NSM. (2020). *Helhetlig digitalt risikobilde 2020*. Nasjonal sikkerhetsmyndighet. https://nsm.no/getfile.php/134267-1601027852/Demo/Dokumenter/Rapporter/NSM_IKT-risikobilde_2020_1609_LR.pdf

NSM. (2021). *Risiko 2021. Helhetlig sikring mot sammensatte trusler*. https://nsm.no/getfile.php/136419-

1616673370/Demo/Dokumenter/Rapporter/NSM_Risiko_2021_web_enkeltside_1203.pdf

O'Malley, P. (1992). Risk, power and crime prevention. *Economy and Society, 21*(3), 252-275. https://doi.org/10.1080/03085149200000013

O'Malley, P. (2016). Governmentality and the analysis of risk. In A. Burgess, A. Alemanno, & J. O. Zinn (Eds.), *Routledge Handbook of Risk Studies*. Routledge.

Olsen, O. E., Kruke, B. I., & Hovden, J. (2007). Societal safety: Concept, borders and dilemmas. *Journal of contingencies and crisis management, 15*(2), 69-79.

Personopplysningsloven. (2018). *Lov om behandling av personopplysninger*. LOV-2018-12-20-116. https://lovdata.no/dokument/NL/lov/2018-06-15-38

Politiloven. (1995). *Lov om politiet*. LOV-2021-04-16-18. https://lovdata.no/dokument/NL/lov/1995-08-04-53

Power, M. (1997). *The Audit Society. Rituals of verification*. OUP Oxford.

Prop. 1 S (2020-2021). *For budsjettåret 2021.* Forsvarsdepartementet. https://www.regjeringen.no/contentassets/5695ead7edfc43ebb03a581d75cfa674/no/pdfs/prp202020210001_fddddpdfs.pdf

Prop. 6. L. (1998-1999). *Om midlertidig lov om begrenset innsyn i overvåkingspolitiets arkiver og registre (innsynsloven).* Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/otprp-nr-6-1998-99-/id159331/?ch=2

Prop. 66 L. (2019-2020). *Endringer i straffeloven mv. (avvergingsplikt, utenomrettslig tvangsekteskap, diskrimineringsvern, skyting mot politiet mv.)* Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/prop.-66-l-20192020/id2696290/?ch=3

Prop. 68 L. (2015-2016). *Endringer i straffeprosessloven mv. (skjulte tvangsmidler).* Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/d2bd4dc7fdb44d90b0d094f4d415b981/no/pdfs/prp201520160068000dddpdfs.pdf

Prop. 73 S. (2011-2012). *Et forsvar for vår tid.* Forsvarsdepartementet. https://www.regjeringen.no/contentassets/e6b0d7ef3c26457ab6ef177cd75b5d32/no/pdfs/prp201120120073000dddpdfs.pdf

Prop. 80 L. (2019-2020). *Lov om Etterretningstjenesten.* Forsvarsdepartementet. https://www.regjeringen.no/no/dokumenter/prop.-80-l-20192020/id2698600/?ch=8

Prop. 131. L. (2018-2019). *Lov om informasjonstilgang m.m. for Partnerdrapsutvalget.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/prop.-131-l-20182019/id2654885/?ch=4

PST. (2004). *Trusselvurdering 2004*. https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2004/#h5sectionTitleAnchor1

PST. (2007). *Trusselvurdering 2007*. https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2007/

PST. (2008). *Trusselvurdering 2008*. https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2008/

PST. (2009). *Trusselvurdering 2009*. https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2009/

PST. (2010). *Trusselvurdering 2010*. https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2010/

PST. (2012). *Trusselvurdering 2012*. https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2012/

PST. (2013). *Trusselvurdering 2013*. https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2013/

PST. (2014). *Trusselvurdering 2014*. https://www.pst.no/globalassets/artikler/trusselvurderinger/trusselvurdering-2014.pdf

PST. (2015). *Trusselvurdering 2015*. https://www.pst.no/globalassets/artikler/trusselvurderinger/trusselvurdering-2015.pdf

PST. (2017). *Trusselvurdering 2017*. https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2017.pdf

PST. (2019). *Trusselvurdering 2019*. https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2019.pdf

PST. (2020). *Nasjonal trusselvurdering 2020*. https://www.pst.no/globalassets/artikler/utgivelser/2020/pst_trusselvurdering_2020.pdf

PST. (2021). *Nasjonal trusselvurdering 2021*. https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/

Ravlum, I.-A. (2005). *Setter vår lit til Storebror … og alle smøbrødre med? Befolkningens holdning til og kunnskap om personvern* (TØI rapport 789/2005). Transportøkonomisk institutt. https://www.toi.no/getfile.php/13913-1134051811/Publikasjoner/T%C3%98I%20rapporter/2005/789-2005/789-2005.pdf

Regjeringen. (2014). *Digitalisering i offentlig sektor*. https://www.regjeringen.no/no/tema/statlig-forvaltning/ikt-politikk/digitaliseringen-i-offentlig-sektor/id2340245/

Regjeringen. (2016, 9. september). *Nye regler om dataavlesning trer i kraft*. https://www.regjeringen.no/no/aktuelt/nye-regler-om-dataavlesing-trer-i-kraft/id2510826/

Regjeringen. (2020, 11. juni). *Ny etterretningstjenestelov er vedtatt i Stortinget*. https://www.regjeringen.no/no/aktuelt/ny-etterretningstjenestelov-er-vedtatt-i-stortinget/id2705969/

Sanger, D. E., & Perlroth, N. (2019). U.S. escalated online attacks on Russia's power grid. *The New York Times*. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

Schartum, D. W. (2010). *Overvåking i en rettsstat*. Fagbokforlaget.

Skjevestad, H. (2020, 24. november). Venter med del av lov som omhandler digitalt grenseforsvar. *Advokatbladet*. https://www.advokatbladet.no/arstalen-2017/venter-med-del-av-lov-som-omhandler-digitalt-grenseforsvar/155342

Soesanto, S. (2020). *Cyber terrorism: Why it exists, why is doesn't, and why it will* (ARI 47/2020). http://www.realinstitutoelcano.org/wps/wcm/connect/cb64e29a-a980-425b-bccd-90dd699b55d0/ARI47-2020-Soesanto-Cyber-Terrorism-Why-it-exists-why-it-doesnt-and-why-it-will.pdf?MOD=AJPERES&CACHEID=cb64e29a-a980-425b-bccd-90dd699b55d0

St.prp. nr. 42 (2003-2004). *Den videre moderniseringen av Forsvaret i perioden 2005-2008.* Forsvarsdepartementet. https://www.regjeringen.no/contentassets/4648088bb28649bc8458f1484d9cbe06/no/pdfs/stp200320040042000dddpdfs.pdf

St.prp. nr. 48 (2007-2008). *Et forsvar til vern om Norges sikkerhet, interesser og verdier* Forsvarsdepartementet. https://www.regjeringen.no/contentassets/93a935d7abc149509595f5e873a38041/no/pdfs/stp200720080048000dddpdfs.pdf

Staksrud, E., Steen-Johnsen, K., Enjolras, B., Gustafsson, M. H., Ihlebæk, K. A., Midtbøen, A. H., Sætrang, S., Trygstad, S. C., & Utheim, M. (2014). *Status for ytringsfriheten i Norge. Resultater fra befolkningsundersøkelsen 2014*. Oslo Fritt Ord, ISF, IMK, & FAFO. https://samfunnsforskning.brage.unit.no/samfunnsforskning-xmlui/bitstream/handle/11250/2389658/Rev_Ytringsfrihet%20i%20Norge%20Holdninger%20og%20erfaringer%20rev2.pdf?sequence=4&isAllowed=y

Standard Norge, NS 5830. (2012). Samfunnssikkerhet: Beskyttelse mot tilsiktede uønskede handlinger. Terminologi.

Størdal, J.-M. (2016, 16. mars). *FFIs samfunnssikkerhetsstrategi*. https://www.ffi.no/om-ffi/styringsdokumenter/ffis-samfunnssikkerhetsstrategi

Sveinbjørnson, S. (2013). *Sverige overvåker norsk mobiltrafikk*. Digi.no. https://www.digi.no/artikler/sverige-overvaker-norsk-mobiltrafikk/288168

Syvertsen, T. (1998). *Dokumentanalyse i medievitenskapen: Tilgang, kildekritikk og problemstillinger*. https://www.hf.uio.no/imk/personer/vit/trinesy/dokumentanalyse_i_medievitenskapen_tilga.pdf

Sæbø, J. R., & Gisle, J. (2019, 15. august). Datalagringsdirektivet. I *Store norske leksikon.* https://snl.no/datalagringsdirektivet

Thagaard, T. (2018). *Systematikk og innlevelse. En innføring i kvalitativ metode*. Fagbokforlaget.

Tjora, A. (2017). *Kvalitative forskningsmetoder i praksis*. Gyldendal.

UNIT. (2020, 24. april). *Informasjonssikkerhet og personvernforordningen (GDPR)*. https://www.unit.no/informasjonssikkerhet-og-personvernforordningen-gdpr

Wessel-Aas, J. (2012). Krigen mot terror og den norske rettsstaten. *Internasjonal politikk, 70*(1), 114-121. https://www.idunn.no/file/pdf/52709311/art13.pdf

Aakre, S. (2020). Hvilket trusselbilde står norske virksomheter overfor, og hvordan kan åpenhet bidra til å forstå cyberrisiko? *Magma*(2), 37-45. https://www.magma.no/hvilket-trusselbilde-star-norske-virksomheter-overfor-og-hvordan-kan-apenhet-bidra-til-a-forsta-cyberrisiko

Vedlegg

Vedlegg 1: Dokumenter.

Utgiver	Utgivelsesår	Tittel
Nasjonal sikkerhetsmyndighet	2003	Risikovurdering 2003
Nasjonal sikkerhetsmyndighet	2005	NSMs risikovurdering 2005, ugradert versjon
Nasjonal sikkerhetsmyndighet	2010	Rapport om sikkerhetstilstanden 2010
Nasjonal sikkerhetsmyndighet	2021	Risiko 2021. Helhetlig sikring mot sammensatte trusler
Politiets sikkerhetstjeneste	2004	Trusselvurdering 2004
Politiets sikkerhetstjeneste	2007	Trusselvurdering 2007
Politiets sikkerhetstjeneste	2008	Trusselvurdering 2008
Politiets sikkerhetstjeneste	2009	Trusselvurdering 2009
Politiets sikkerhetstjeneste	2010	Trusselvurdering 2010
Politiets sikkerhetstjeneste	2012	Trusselvurdering 2012
Politiets sikkerhetstjeneste	2013	Trusselvurdering 2013
Politiets sikkerhetstjeneste	2014	Trusselvurdering 2014
Politiets sikkerhetstjeneste	2015	Trusselvurdering 2015
Politiets sikkerhetstjeneste	2017	Trusselvurdering 2017
Politiets sikkerhetstjeneste	2019	Trusselvurdering 2019
Politiets sikkerhetstjeneste	2020	Nasjonal trusselvurdering 2020
Politiets sikkerhetstjeneste	2021	Nasjonal trusselvurdering 20201
Etterretningstjenesten	2015	FOKUS 2015
Justis- og politidepartementet	1999	NOU 1999: 27 - «Ytringsfrihet bør finde Sted». Forslag til ny Grunnlov § 100

Justis- og politidepartementet	2000	NOU 2000: 24 – Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet
Justis- og politidepartementet	2001-2002	Meld. St. 17 (2001-2002) – Samfunnssikkerhet. Veien til et mindre sårbart samfunn
Justis- og politidepartementet	2006	NOU 2006: 6 – Når sikkerheten er viktigst
Justis- og politidepartementet	2009	NOU 2009: 15 – Skjult informasjon – åpen kontroll
Justis- og beredskapsdepartementet	2012	Høring – kriminalisering av forberedelse til terrorhandling, utvidet adgang til tvangsmiddelbruk, og endringer i straffeloven 1902 § 60 a
Justis- og beredskapsdepartementet	2014 (org. 1999)	Menneskerettsloven. Lov om styrking av menneskerettighetenes stilling i norsk rett
Justis- og beredskapsdepartementet	2015	NOU 2015: 13 – Digital sårbarhet – sikkert samfunn
Justis- og beredskapsdepartementet	2015-2016	Prop. 68 L. (2015-2016). Endringer i straffelovsprosessloven mv. (skjulte tvangsmidler)
Justis- og beredskapsdepartementet	2016-2017	Meld. St. 10 (2016-2017) – Risiko i et trygt samfunn. Samfunnssikkerhet

Justis- og beredskapsdepartementet	2017	NOU 2017: 9 – Politi og bevæpning. Legalitet, nødvendighet, forholdsmessighet og ansvarlighet
Justis- og beredskapsdepartementet	2018	NOU 2018: 14 – IKT-sikkerhet i alle ledd
Justis- og beredskapsdepartementet	2019-2020	Meld. St. 29 (2019-2020) – Politimeldingen – et politi for fremtiden
Justis- og beredskapsdepartementet	2019-2020	Prop. 66 L. (2019-2020) – Endringer i straffeloven mv. (averingsplikt, utenomrettslig tvangsekteskap, diskrimineringsvern, skyting mot poltiet mv.)
Justis- og beredskapsdepartementet	2020	NOU 2020: 4 – Straffelovrådets utredning nr. 1 – kriminalisering av deltakelse i og rekruttering til kriminelle grupper
Forsvarsdepartementet	2003-2004	St.prp. nr. 42 (2003-2004) – Den videre moderniseringen av Forsvaret i perioden 2005-2008
Forsvarsdepartementet	2007-2008	St.prp. nr. 48 (2007-2008) – Et forsvar til vern om Norges sikkerhet, interesser og verdier
Forsvarsdepartementet	2011-2012	Prop. 73 S. (2011-2012) – Et forsvar for vår tid
Forsvarsdepartementet	2015	Et felles løft

Forsvarsdepartementet	2016	Digitalt grenseforsvar (DGF)
Forsvarsdepartementet	2016	NOU 2016: 19 – Samhandling for sikkerhet. Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid
Forsvarsdepartementet	2019-2020	Prop. 80. L. (2019-2020) – Lov om etterretningstjenesten
Forsvarsdepartementet	2020-2021	Prop. 1 S (2020-2021) – For budsjettåret 2021
Forsvars- og beredskapsdepartementet	2018	Støtte og samarbeid. En beskrivelse av totalforsvaret i dag
22. juli-kommisjonen	2012	Rapport fra 22. juli-kommisjonen
Justisdepartementet og samferdselsdepartementet	2015	Datalagring og menneskerettighetene
Direktoratet for samfunnssikkerhet og beredskap	2019	Analyser av krisescenarioer 2019
Direktoratet for samfunnssikkerhet og beredskap	2016	Befolkningsundersøkelse om risikopersepsjon og beredskap i Norge
Direktoratet for samfunnssikkerhet og beredskap	2020	Befolkningsundersøkelse om norske husholdningers bevissthet og adferd knyttet til egenberedskap
Statistisk sentralbyrå	1997	Undersøkelse om personvern: Holdning og erfaringer 1997

Transportøkonomisk institutt	2005	Setter vår lit til Storebror… og alle småbrødre med? Befolkningens holdninger til og kunnskap om personvern
Datatilsynet og teknologirådet	2014	Personvern. Tilstand og trender
Datatilsynet	2008	Personvernundersøkelsen 2008
Datatilsynet	2014	Personvernundersøkelsen. Samlerapport fra personvernundersøkelsen 2013/2014
Datatilsynet	2020	Personvernundersøkelsen 2019/2020
Forskning.no	2013	Samler seg om sikring mot cyberterror
Regjeringen	2016	Nye regler om dataavlesning trer i kraft
The New York Times	2019	U.S. escalated online attacks on Russia's power grid
Regjeringen	2020	Ny etterretningstjenestelov er vedtatt i Stortinget
Aftenposten	2020	Det haster med ny etterretningslov
Advokatbladet	2020	Venter med del av lov som omhandler digitalt grenseforsvar

Tabell 3. Dokumenter tatt i bruk i dokumentanalysen.