Høgskolen
i Innlandet

Institutt for organisasjon, ledelse og styring

Kandidatnummer 102 og 150

Masteroppgave

Tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon

- En analyse av høringssvar til endringer i Etterretningstjenesteloven

Offentlig ledelse og styring

MPABR4901

Våren 2023

Forord:

Takk til veileder Mass Soldal Lund for gode innspill og tilbakemeldinger gjennom arbeidet med å skrive denne masteroppgaven. Arbeidet har vært en lærerik og tidkrevende prosess.

Vi vil også takke Forsvarets Høgskole for stipend gjennom prosjektet "Informasjonskrigføring og datadrevne operasjoner".

Eline Riiber & David Christian Frich, Oslo 10. mai 2023

Sammendrag:

Denne masteroppgaven er et dokumentstudie av høringssvarene til endringene til Etterretningstjenesteloven fra 2020. Oppgaven søker å svare på problemstillingen:

"*Hva oppfattes som de største problemstillingene ved tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon i Etterretningstjenesteloven*?"

Oppgaven belyser hva som oppleves som de største problemstillingene tilknyttet innføringen av tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon, som gir Etterretningstjenesten lovlig adgang til å drive innhenting mot all elektronisk kommunikasjon som går inn og ut av Norge. Videre gir oppgaven en gjennomgang av den kontekstuelle rammen for den nye lovgivningen og et innblikk i hva det betyr i praksis at Etterretningstjenesten får denne adgangen. I oppgaven analyserer vi høringssvarene som ble sendt inn i høringsprosessen. Høringssvarene blir analysert ut fra overvåkningsteoretiske perspektiver med sikte på å kartlegge hva som oppleves som de største problemstillingene. Høringssvarene ble sendt inn av en rekke ulike instanser, og vi undersøker om det er noen likheter eller forskjeller i de problemstillingene som blir lansert på tvers av gruppene.

Gjennom analysen ser vi at problemstillingene som blir tatt opp i høringssvarene samsvarer med det teoretiske rammeverket og Macnishs etiske prinsipper. På samme måte som Macnish sine prinsipper gjør seg relevante, blir Stoddarts motargumenter også vel så relevante, da de utgjør to sider av samme sak. Foucaults panoptiske overvåkningsteori har betydning for flere av problemstillingene, særlig når det gjelder journalisters kildevern og avkjølende effekt. Schartums sårbarhetsteori og poengmatrise, samt Marx' teori om konteksten for overvåkning bidrar også til å kaste lys over flere av høringssvarene, selv om andre deler av rammeverket anses som mer relevant. Vår analyse og vurdering av de ulike teoretiske perspektivene i denne oppgaven tilsier at Macnish, Stoddart og Foucault utgjør hoveddelen av rammeverket som treffer problemstillingen, og er best egnet til å si noe om hva som oppleves som de mest problematiske sidene ved tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon.

Vi har identifisert at det er forskjeller i adresserte problemstilling fra de ulike høringsgruppene. Høringssvarene som er utformet fra offentlige etater er mest opptatt av lovtekniske problemstillinger. Disse instansene vil naturlig kunne identifisere problematiske sider ved hvordan en lovtekst er utformet, samt ha evne til å forskuttere og identifisere potensielle implikasjoner ved uklar lovformulering. Arbeidstaker- og interesseorganisasjoner er i høy grad opptatt av lovtekniske problemstilling, samt problemstillinger som går på økonomi, drift og ressurssetting. Privatpersoner er mer bekymret for overvåkning i seg selv og problemstillinger rundt EMK art. 8 som handler om retten til privatliv. Det er naturlig at ingen privatpersoner ønsker å bli overvåket og at retten til privatliv opprettholdes. Private virksomheter har økonomi, drift og ressurssetting som en hovedproblemstilling i tillegg til domstolskontroll. På tvers av alle kategoriene er det flest høringssvar som har problematisert overvåkning og domstolskontroll, uavhengig av type høringssubjekt. Våre funn indikerer at overvåkning av befolkningen, samt svak eller mangelfull domstolskontroll oppleves som det mest problematiske ved tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon.

Abstract:

This master's thesis is a document study of the responses to the changes made to the Norwegian Intelligence Service Act in 2020. The thesis seeks to answer the research question: "What are perceived as the main issues related to the targeted acquisition of cross-border electronic communication in the Norwegian Intelligence Service Act?"

The thesis examines what is perceived as the major issues associated with the introduction of targeted acquisition of cross-border electronic communication, which gives the Intelligence Service legal access to gather all electronic communication entering and leaving Norway. Additionally, the thesis provides an overview of the contextual framework for the new legislation and an insight into what it means in practice for the Intelligence Service to have this access. In the thesis, we analyze the responses submitted during the consultation process. The responses are analyzed from a surveillance theoretical perspective, with the aim of identifying the major issues. The responses were submitted by various organizations, and we investigate whether there are any similarities or differences in the issues raised across the groups.

Through our analysis, we observe that the issues raised in the responses align with the theoretical framework and Macnish's ethical principles. Similarly, Stoddart's counterarguments are equally relevant, as they represent two sides of the same issue. Foucault's panoptic surveillance theory is relevant to several of the issues raised, particularly with regard to journalists' source protection and chilling effects. Schartum's vulnerability theory and point matrix, as well as Marx's theory of the context of surveillance, also shed light on several of the responses, although other parts of the framework are considered more relevant. Our analysis and evaluation of the different theoretical perspectives in this thesis suggest that Macnish, Stoddart, and Foucault constitute the main part of the framework that addresses the research question and are best suited to shed light on what is perceived as the most problematic aspects of targeted acquisition of cross-border electronic communication.

We have identified differences in the issues addressed by the different consultation groups. Responses from public agencies are mostly concerned with legal-technical issues. These agencies

are naturally able to identify problematic aspects of how a legal text is formulated and have the ability to anticipate and identify potential implications of unclear wording. Employee and interest organizations are highly concerned with legal-technical issues, as well as issues related to finance, operations, and resource allocation. Private individuals are more concerned about surveillance itself and issues related to Article 8 of the European Convention on Human Rights, which deals with the right to privacy. It is natural that no private individuals want to be monitored, and the right to privacy is maintained. Private companies consider finance, operations, and resource allocation to be the main issue, in addition to judicial oversight. Across all categories, there are more responses that have problematized surveillance and judicial oversight, regardless of the type of consultation subject. Our findings indicate that the surveillance of the population, as well as weak or inadequate judicial oversight, are perceived as the most problematic aspects of targeted acquisition of cross-border electronic communication.

Innholdsfortegnelse

Innhold

1. Innledning

Siden den første nettsiden ble til i 1991 har verden vært vitne til en digital revolusjon. Ca. 4,7 milliarder mennesker har tilgang til Internett og digitaliseringen de siste 30 årene har gjort at Internett har blitt en avgjørende faktor for både mennesker, myndigheter og næringslivet verden over (Datareportal, 2021; Det kongelige fornyings-, administrasjons- og kirkedepartement 2013, s. 5). I 2023 opplever vi stadig nye digitale løsninger som kan operere mer og mer selvstendig, i tillegg til programvare, sensorer, og komponenter som gjør at internettbaserte løsninger i økende grad knyttes sammen med det fysiske liv. På denne måten er vi mennesker ikke lenger bundet av geografisk nærhet, tid eller andre størrelser som tidligere har vært styrende (Larssen & Dyndal, 2020, s. 196). Denne utviklingen har bidratt til økonomisk vekst, fremgang og optimalisering av både offentlige og private tjenester, ikke minst som kommunikasjonsverktøy og kilde til informasjon.

Bruken, integreringen, og avhengigheten til digitale, internettbaserte løsninger, både fra mennesker, næringsliv og myndigheter har på samme tid gjort oss sårbare for angrep, manipulasjon, spionasje og sabotasje i det digitale rom. Data og informasjon stjeles fra både bedrifter, kunnskapsinstitusjoner og offentlig sektor med ulike hensikter, på samme tid som Internett brukes som kommunikasjonsmiddel til etterretningsoperasjoner og terrornettverk verden over. Stater som Russland og Kina er særlig kjent for å ha tatt i bruk det digitale rom og "cyberspace" som en arena for å nå sine utenriks- eller maktpolitiske målsettinger. I et stadig mer usikkert verdenspolitisk landskap med større skillelinjer mellom Øst og Vest gjør trusselen seg stadig mer gjeldende. Fremmede staters etterretningsoperasjoner i cyberdomenet utgjør i dag en alvorlig og økende trussel mot nasjonale myndigheter og virksomheter, både i omfang og kompleksitet (PST 2023, s. 14). Samtidig innebærer den teknologiske utviklingen, blant annet når det gjelder kommunikasjonsformer, at mulighetene for å innhente informasjon har blitt bedre. Digitaliseringen av samfunnet innebærer at det stadig genereres større datamengder (Datatilsynet, 2018, s.12-13). Dette medfører at Etterretningstjenesten må være i stand til å finne og samle inn relevant informasjon i en stadig økende informasjonsflom. De må kunne sammenstille og analysere informasjonen og gjøre den om til etterretningsprodukter som er relevante for norske beslutningstakere slik at tiltak kan treffes for å beskytte Norge i henhold til sitt mandat.

Etterretningstjenesten har siden 2012 argumentert for viktigheten av tekniske kapasiteter for å samle inn, behandle og analysere slik type informasjon for å holde tritt med trender i trusselbildet, fremveksten av stordata og den teknologiske utviklingen (EOS-utvalget, 2012). Argumentasjonen resulterte etter hvert i økte bevilgninger, og Lysne-II utvalget ble i 2016 satt ned for å utrede hvordan den teknologiske utviklingen påvirker forsvaret av Norge og norsk utenlandsetterretning (Lysne, 2016, s. 7). I 2020 ble ny Etterretningstjenestelov vedtatt, og Forsvarsdepartementet ønsket i § 7 å gi Etterretningstjenesten adgang til å utføre "tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon" i den hensikt forebygge, avdekke og motvirke utenlandske trusler mot Norge og norske interesser (Regjeringen, 2022). I praksis betyr dette at Etterretningstjenesten på nærmere vilkår vil kunne få adgang til å lagre elektronisk kommunikasjon som passerer landegrensene og senere, etter beslutning fra domstol kunne søke i de lagrede metadataene og innhente innholdsdata. §7 ble ikke innført i 2020 da det var knyttet usikkerhet til menneskerettslige og demokratiske prinsipper som nedkjølingseffekt, journalisters kildebeskyttelse, personvern og internasjonal rettspraksis. Videre høstet lovforslaget kritikk om masseovervåkning på den ene siden, mens andre mente at det var på høy tid å gi Etterretningstjenesten fullmakt på lik linje med sammenlignbare staters etterretningsorganisasjoner (Haugsbø og Harkestad 2022; Svendsen 2022). Forslag til endringer for å ivareta usikkerhetsmomentene i § 7 ble sendt på ny høring til høringsinstansene i 2022, og det er disse høringssvarene som er denne masteroppgaven sin kjerne.

1.1 Tema og problemstilling

Lovforslaget om at Etterretningstjenesten skal gis adgang til tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon, aktualiserer en rekke problemstillinger. Dette satt på spissen gjennom overvåkning og personvern på den ene siden, og statssikkerhet og samfunnssikkerhet på den andre siden. Vi mener derfor at temaet er verdt en nærmere studie, og at høringsprosessen gir mulighet for det.

Problemstilling:

Hva oppfattes som de største problemstillingene ved tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon i Etterretningstjenesteloven?

Denne oppgaven er en kvalitativ studie av høringssvar til høringsprosessen "Forslag til endringer i etterretningstjenesteloven". Vi ønsker å undersøke hva de forskjellige høringssvarene uttrykker, identifisere hva som oppfattes som de mest problematiske sidene med tilrettelagt innhenting, se hvilke argumenter som benyttes og analysere dette i lys av overvåkningsteori.

Vi har i oppgaven valgt å anvende et etisk rammeverk som er basert på tradisjonen om rettferdig krigføring, som teoretisk ramme for analyse av høringssvarene. For å supplere det etiske rammeverket har vi også brukt annen teori som beskriver overvåkning. Vår begrunnelse for å anvende dette rammeverket er basert på vår overbevisning om at det er et godt verktøy for å undersøke problemstillingen vi søker å besvare, da det er en rekke etiske sider ved overvåkning som aktivitet og verktøy.

1.2 Avgrensninger

Denne oppgaven handler utelukkende om høringsprosessen som går på forslag til endringer i ny Etterretningstjenestelov, og ikke de foregående prosessene med innføringen av Etterretningstjenesteloven (2020) som helhet. Vi vil konsentrere oss om de mest vesentlige endringene, da de andre endringene er av en mer lovteknisk karakter og vil etter vårt skjønn ikke berike temaet for oppgaven i særlig grad da dette er mer relevant innenfor juridiske domener.

2. Tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon

2.1 Norske borgeres digitale liv og bruk av Internett

Norge er anerkjent som et av de mest digitaliserte landene i verden, både i privat og offentlig sektor (World Economic Forum, 2022). Norge rangerer høyt når det kommer til digitalisering, basert på en rekke faktorer som bredbåndsutbredelse, tilgang til smarttelefoner og datamaskiner, samt generell bruk av Internett og digitale tjenester. De fleste offentlige tjenester og bedrifter i Norge er gjennomgående digitale og tilgjengelige på Internett.

Ifølge Statistisk sentralbyrå hadde 96% av alle personer i Norge mellom 17 og 74 år brukt Internett hver dag de siste 12 mnd. i 2022 (SSB, 2022). Disse tallene forteller oss at mer eller mindre alle norske husstander bruker Internett i det daglige. Den samme kilden forteller oss at bruken av Internett for det meste benyttes til e-post, søk etter informasjon, søk etter varer og tjenester, lese aviser, søke etter helserelatert informasjon, banktjenester, videosamtaler, sende direktemeldinger, deltakelse i sosiale nettverk og streaming (SSB, 2022).

Den kontinuerlige økningen i digitaliseringen gjør det stadig vanskeligere å velge et liv utenfor Internett i Norge. Det er fremdeles mulig å velge et liv utenfor i interaksjon med det offentlige, mens mange tjenester i det private markedet forutsetter tilgang til digitale enheter og Internett (Tilsynet for universell utforming, 2022). På denne måten ser man at den faktiske valgfriheten om hvorvidt man ønsker å bli en del av det digitaliserte samfunnet, stadig blir mindre. Nettopp på grunn av den store utbredelsen og hvordan vi som samfunn stadig blir mer avhengige av digitale løsninger gjør at vi må se på bruken av Internett som en samfunnsressurs, på nær sagt alle områder. Dette fordi Internett har blitt avgjørende for hvordan vi søker og tilegner oss informasjon, hvordan vi kommuniserer og hvordan vi benytter oss av både offentlige og private tjenester.

Bruk av smarttelefon har for store deler av befolkningen blitt et integrert verktøy i hverdagen, og et verktøy som gjør at vi hele tiden er koblet til Internett, enten gjennom 4G/5G-nettet eller WiFi. De siste årene har man også sett utvikling innen “Internet of Things” (IoT), som refererer til

utbredelsen av eksempelvis smarte-hjem løsninger, som varmeregulering, automatiske strømmålere, dørlåser, sensorer eller annet utstyr som i hjemmet eller andre steder er avhengig av Internett for å fungere best mulig, kommunisere med andre enheter, og med brukeren (PwC, 2016). Alle disse momentene har bidratt til at bruken av digitale tjenester og Internett stadig blir en mer integrert del av folk sin hverdag og på den måten produserer vi stadig større datamengder og legger igjen digitale spor som på forskjellige vis er egnet til å si noe om hvem vi er, hva vi gjør, hvem vi kommuniserer med og hva vi er interessert i. På samme tid gjør denne integreringen det norske samfunnet sårbart når det kommer til angrep eller sabotasje i det digitale domenet (Larssen & Dyndal, 2020, s 198).

2.2 Norsk kommunikasjonsstruktur

Det finnes i dag tre kommersielle telekommunikasjonstrukturer i Norge, drevet av Telenor, Telia og ICE. I tillegg finnes det regionale nett, men viktigst er Telenors kjernenett som i store trekk bærer datatrafikken som beveger seg innad i Norge (NOU 2015: 13, s. 107). Videre har vi fiberselskaper som Global Connect og Altibox som rene fiberselskaper for Internett. For at norske telefon- og internettbrukere skal kunne kommunisere med resten av verden, er norsk kommunikasjonsstruktur koblet sammen med utenlandske nettstrukturer via kabler, både på land og gjennom sjøkabler. Per tid går de største delene av norsk kommunikasjon med utlandet gjennom kabler i Sverige, slik at mesteparten av datastrømmene som krysser grensen vil enten oppstå eller slutte i Norge (Lysne, 2016, s. 48). Bruk av kjente tjenester som eies og drives av aktører i utlandet, slik som Google (Gmail), Outlook, og Skype vil dermed passere disse kablene. Det samme vil gjelde sosiale medier som Facebook, Instagram, Twitter og Snapchat, men også meldingstjenester som WhatsApp og Signal. I tillegg vil andre telefonsamtaler, SMS, iMessage og e-poster som sendes mellom Norge og utlandet krysse kablene. Det er ikke nødvendigvis intuitivt, men dersom en tjeneste man benytter seg av har sin server i utlandet vil kommunikasjonen mellom to personer først gå til serveren i utlandet, også tilbake til Norge. Dermed vil informasjonen være grensekryssende.

Det skal også nevnes at informasjon kan krysse landegrensene uten at man nødvendigvis er oppmerksom på, eller har intensjon om det. Eksempelvis er bruk av skytjenester for lagring av

bilder og dokumenter blitt utbredt, samt at sikkerhetskopier av mobiltelefoner og datamaskiner i økende grad oppbevares på Internett. Dette gjør at informasjon som ikke nødvendigvis er "kommunikasjon" i ordets rette forstand, likevel er grensekryssende (Lysne, 2016, s. 48).

Oppsummert kan en se at den digitale infrastrukturen i Norge i store trekk er integrert med utlandet. Det er også grunn til å anta at denne utviklingen vil fortsette å stige i tiden fremover ettersom globale tjenesteleverandører som oftest har sine servere i utlandet og stadig får større markedsandeler i Norge.

2.3 Norsk utenlandsetterretning

Norsk utenlandsetterretning defineres av Forsvarsdepartementet som *"*et sikkerhetspolitisk virkemiddel som skal bidra til å beskytte Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser gjennom å skaffe norske myndigheter informasjon om utenlandske forhold*"* (Forsvarsdepartementet, 2019-2020, s. 15).

Evnen til å varsle om ytre trusler og innhente og analysere relevant informasjon er således en grunnleggende forutsetning i forsvaret av Norge.

Etterretning kan defineres som systematisk innhenting og bearbeiding av informasjon som angår utenlandske forhold, ervervet med åpne og fordekte metoder i en statlig legal ramme. Etterretningsproduktene skal redusere usikkerhet, skape forståelse og har ofte en prediktiv karakter. Mottakere av etterretningsprodukter er beslutningstakere på ulike nivå i statsforvaltningen, og skal bidra til å redusere usikkerhet. Begrepet "etterretning" brukes både om produktet, aktiviteten og organisasjonen som utøver aktiviteten (Forsvaret, 2021, s. 18).

Informasjon som innhentes i etterretningsøyemed er ofte om en motstander, fiende eller mulig fiende med formål om å beskytte nasjonal sikkerhet eller tilrettelegge for en stats politiske eller strategiske intensjoner og målsettinger. Informasjonen som samles inn til etterretningsformål samles vanligvis inn gjennom skjulte metoder, men selve informasjonen trenger ikke være hemmelig eller skjult for at den samlet sett kan ha etterretningsmessig verdi. Etterretning kan for

eksempel omfatte informasjon om militære kapasiteter, politiske intensjoner og økonomiske forhold i fremmede land, samt informasjon om enkeltpersoner eller organisasjoner som kan brukes til motstanderens fordel. Informasjon som samles inn til utenlandsetterretningsformål brukes til å informere beslutningstakere innen nasjonal sikkerhetspolitikk, militær strategi, varsling eller beskytte landet mot spionasje fra andre stater eller utenlandske agenter eller kapasiteter (Forsvaret, 2021, s. 20).

Fordi etterretning som aktivitet har vært drevet i alle tider og i alle samfunn, må etterretningsaktivitet forstås og tilpasses tiden man lever i. Når omstendighetene eller avgjørende faktorer endres, ser man endringer i hvordan etterretningsaktivitet drives. Den teknologiske utviklingen og den digitale hverdagen vi lever i dag er et eksempel på en slik avgjørende og endrende faktor. Informasjonsmengden, hastigheten og informasjonens kompleksitet er de største kjennetegnene (Stenslie, Haugom & Vaage, 2019, s. 20). Denne utviklingen har hatt dramatiske konsekvenser for trusselbildet, og mål i Norge er under stadige angrep (Stenslie, Haugom & Vaage, 2019, s. 53) Dette eksemplifiseres ved at Nasjonal Sikkerhetsmyndighet i 2022 omtalte cyberangrep som "hverdagskost" for norske virksomheter (NSM, 2022).

Den sikkerhetspolitiske utviklingen de siste årene med økt rivalisering mellom stormaktene uttrykker seg på flere nivåer, herunder militært og økonomisk, men viktigst; teknologisk. Den teknologiske utviklingen har bidratt til at mulighetene til å innhente informasjon har blitt bedre og mindre ressurskrevende. Dette har på samme tid gjort oss mer sårbare for spionasje, sabotasje og andre angrep i det digitale rom. Trusselen er økende, og den kommer primært fra statlige aktører, men også ikke-statlige aktører (PST, 2023). Varslingstiden har stadig blitt kortere, og det er vanskeligere å konstatere at en er under angrep, hvem som angriper og hva angriper er ute etter (Stenslie, Haugom & Vaage, 2019, s. 53). Trusselaktørene påvirker forståelsen av problemstillingen og fenomenet gjennom desinformasjon og fornekting, med mål om å skape en fordelaktig posisjon og handlingsrom for seg selv (Forsvarsdepartementet, 2019-2020, s. 16). Den teknologiske utviklingen har gjort at det stadig stilles høyere krav til Etterretningstjenesten, og for at tjenesten skal kunne holde tritt med det endrede trusselbildet ønsker Forsvarsdepartementet at Etterretningstjenesten skal gis adgang til relevant informasjon - der den

finnes. Slik informasjon mener Forsvarsdepartementet at Etterretningstjenesten skal kunne innhente gjennom grenseoverskridende elektronisk kommunikasjon.

I store deler av moderne tid har etterretningstjenester operert i knapphet. Det har historisk vært vanskelig å tilegne seg hemmeligheter, og de virkelige store, verdifulle hemmelighetene har vært sjeldne. Teknologien endret dette drastisk og normaltilstanden med mangel på informasjon ble erstattet med motparten; informasjonsoverflod, ofte generert gjennom teknologiske innsamlingssystemer. Allerede under angrepet på Pearl Harbor i 1941 klarte man ikke å skille de virkelige signalene fra omgivelsenes "støy", og det er denne støyen og informasjonsoverbelastningen som anses som etterretningens største utfordring i det 21- århundre (Andrew, Aldrich & Wark 2009, s. 524).

I all etterretningsvirksomhet er målutvikling viktig for å identifisere trusselaktører eller etterretningsmål. Målutvikling gjøres normalt ved at man gjennom en type inngangsinformasjon og selektor går gjennom historiske data og informasjon. Dette kan for eksempel være en IP-adresse som tidligere er brukt i et cyberangrep eller en e-postadresse som er brukt av en terrorist. Man vil da forsøke å finne ut om trusselaktøren har vært i kontakt med andre, ukjente trusselaktører, eller om aktøren har benyttet andre IP-adresser eller e-postadresser, samt hva aktøren har utvist interesse for. Svaret på flere av disse spørsmålene kan finnes i historisk aktivitet og data, ofte fordi trusselaktører stadig endrer og tar i bruk nye selektorer for å skjule og fordekke sin aktivitet (Lysne, 2016, s. 19). Å produsere rettidig etterretning om dette kan bidra til at norske myndigheter får satt inn sine forebyggende tiltak eller virkemidler til rett tid og på den måten forsvare og forhindre et angrep, enten om det er fra en statlig trusselaktør i cyberdomenet eller en terrorist.

2.4 Trusselbildet

De mest alvorlige truslene mot Norges sikkerhet og selvstendighet er nesten uten unntak trusler med knytninger eller opprinnelse i utlandet. Dette viser både Politiets sikkerhetstjeneste og Etterretningstjenestens siste års trusselvurderinger (PST, 2023; Etterretningstjenesten 2023). Trusselaktørene bruker Internett som selve verktøyet, men også til å kommunisere over landegrensene med avanserte dataverktøy. Dette har gitt både større og mindre stater, så vel som ikke statlige aktører, kapasitet til å ramme Norge på måter de tidligere ikke hadde. Slike digitale etterretningsoperasjoner mot mål i Norge kan pågå over lang tid uten å bli oppdaget, og de kan være både målrettede og effektive (Lysne, 2016, s. 11). Målene kan være politiske, i form av informasjon om norske holdninger eller standpunkt i internasjonale fora, eller forsøk på å påvirke disse. De kan være militære, i form av at de vil forsøke å finne informasjon om norske kapasiteter, strategier eller allianser. De kan være teknologiske i form av at de vil finne informasjon om sensitiv og kritisk teknologi som Norge ikke vil dele med land vi ikke har et sikkerhetssamarbeid med eller økonomiske i form av forretningshemmeligheter eller norske investeringsstrategier (PST, 2022; PST, 2023). Dette er ikke uttømmende.

Elektronisk kommunikasjon via Internett kan benyttes av slike trusselaktører til å planlegge og gjennomføre operasjoner, rapportere hjem om informasjon de har stjålet til sin oppdragsgiver, formidle nye oppdrag eller fremskaffe informasjon om nye mål i Norge. Det finnes en rekke eksempler på hvordan trusselaktører i utlandet har benyttet seg av Internett for å påvirke samfunnsinformasjon eller samfunnsfunksjoner i et annet land.

Kinesiske cyberaktører antas å stå bak cyberangrepet “Operation Aurora”, som ble gjennomført mot flere store teknologiselskaper, inkludert Google, Adobe og Intel i perioden 2009-2010 (MacAfee, 2011). Angrepet medførte at store mengder sensitiv informasjon ble stjålet fra selskapenes datasystemer. Russiske cyberaktører antas å stå bak cyberangrepet “Black Energy” som slo ut strømnettet i store deler av Ukraina i 2015 (Accenture iDefense,2014). Det norske Stortinget ble utsatt for cyberangrep i både 2020 og 2021, hvor analysene viste at førstnevnte angrep var utført av en aktør tilknyttet Russlands militære etterretningstjeneste GRU (PST, 2020) og sistnevnte av en kinesisk aktør (Regjeringen, 2021).

En annen type bruk av Internett som er egnet til å påvirke et annet lands, institusjoner og befolkning finner vi i det amerikanske presidentvalget i 2016, hvor det amerikanske etterretningsmiljøet mener at russiske aktører forsøkte å påvirke valget til fordel for Donald Trump (US Department of Justice, 2018). Det samme ble sett i Storbritannias Brexit-avstemning (Intelligence and Security Committee of Parliament, 2021) samme år, og under det franske presidentvalget i 2017 (The U.S Office of the Director of National Intelligence, 2017). Påvirkningsoperasjonene har vært forskjellig utført, men noen av metodene har blant annet vært sosiale medier-kampanjer hvor trusselaktøren har brukt falske profiler på sosiale medier for å spre desinformasjon, propaganda i den hensikt å øke polariseringen. Dette gjøres ved spredning av bevisst feilaktig eller villedende informasjon i den hensikt å påvirke leserens holdninger og virkelighetsoppfatning. Statsdrevet desinformasjonskampanjer søker gjerne å påvirke eller forsterke konfliktlinjer mellom grupper i et samfunn for å skape best mulig forutsetninger for sine egne mål. Målsetningen trenger nødvendigvis ikke å være å få folk til å tro på noe som er direkte usant, men like gjerne skape tvil, økt oppmerksomhet, usikkerhet eller avledning. Informasjonen som spres kan på den måten være helt eller delvis korrekt, men da gjerne tillagt en annen mening enn den opprinnelige, tatt ut av sammenheng eller kontekst, eller på annen måte fremsatt på en feilaktig eller villedende måte (FFI,2021, s. 11). Slik påvirkningsaktivitet inkluderer oppretting av falske profiler, grupper, sider på sosiale medier, nyheter, samt manipulasjon av diskusjoner og forum på Internett. Andre eksempler er at politiske partier og kandidater, samt organisasjoner og institusjoner knyttet til valg, blir angrepet for å stjele sensitive data og spre desinformasjon. De har også lekket dataene som er stjålet fra politiske partier eller kandidater i den hensikt å så tvil, ødelegge deres troverdighet eller påvirke valgresultatene.

Det kan diskuteres hvorvidt et digitalt angrep mot Norge kan sidestilles med et militært angrep eller ulovlig maktbruk etter folkeretten, men angrepets mål og styrke kan få like alvorlige konsekvenser. Det digitale rom kan på mange måter anses som et nytt domene for mellomstatlig aggresjon, og tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon kan bidra til å styrke norsk forsvarsevne på feltet.

2.5 Hvorfor tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon?

Lysne II-utvalget definerer tilrettelagt innhenting av elektronisk kommunikasjon (tidligere digitalt grenseforsvar) som:

> *Etterretningstjenestens målrettede innhenting og analyse av utenlandsetterretningsrelevant informasjon, basert på aksess til elektronisk kommunikasjon som går inn og ut av Norge, i den hensikt å kartlegge og motvirke mulige ytre trusler mot rikets sikkerhet og selvstendighet og andre viktige nasjonale interesser*

(Lysne, 2016, s. 10).

I proposisjon 80 L (2019-2020) fra Forsvarsdepartementet til Stortinget skriver Forsvarsdepartementet at tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon vil "styrke Norges selvstendige etterretningsevne og vår mulighet til å oppdage og motvirke spionasje, sabotasje, terrorhandlinger og andre trusler mot nasjonale sikkerhetsinteresser" (Forsvarsdepartementet, 2019-2020, s. 9).

Med andre ord handler det om at Etterretningstjenesten skal kunne innhente, bearbeide og analysere utvalgt kommunikasjon som går inn og ut av Norges grenser gjennom sjø- eller landbaserte fiberoptiske kabler med det formål å varsle mot utenlandske trusselaktører. Dette innebærer ikke bare kommunikasjon mellom to eller flere entiteter, men også overføring av lyd, tekst, bilder eller andre data som beveger seg over landegrensene gjennom Internett (Lysne, 2016, s. 10).

Etterretningstjenesten mandat er å samle informasjon og analysere denne i den hensikt å kartlegge og motvirke ytre trusler mot Norges selvstendighet og andre viktige nasjonale interesser (Etterretningstjenesten, 2022). En del av dette oppdraget er å være Norges COMINT-tjeneste (kommunikasjonsetterretning), som betyr å innhente informasjon i kommunikasjonsdomenet, om fremmede stater, organisasjoner eller personer som er relevant for Etterretningstjenestens overordnede mandat. Formålet med tilrettelagt innhenting av

grenseoverskridende elektronisk kommunikasjon er å sikre at Etterretningstjenesten i lys av den teknologiske utviklingen skal ha tilgang til relevant informasjon, der den finnes og der den kommuniseres- på Internett. Dette er viktig for Norges evne til å kartlegge, varsle om og motvirke alvorlige trusler, både i fredstid og under sikkerhetspolitiske kriser (Lysne, 2016, s. 10).

I det verdensomspennende kommunikasjonsnettet utveksles informasjon som det er viktig for norske myndigheter å ha kunnskap om, samtidig som det benyttes til aktivitet som kan utgjøre en ytre trussel mot Norge og nasjonale interesser (Lysne, 2016, s. 11). Eksempler på dette er digital spionasje og cyberangrep. Med Internett som en stadig mer avgjørende komponent i all menneskelig aktivitet antas disse truslene å forsterkes i årene som kommer.

I langtidsplanen for Forsvaret står blant annet:

> *Digitale angrep har i økende grad blitt en integrert del av militære operasjoner. Slike angrep kan forstyrre, påvirke og hindre nasjonale beslutningsprosesser i sikkerhetspolitiske kriser og væpnet konflikt. Evne til å motstå angrep i og gjennom det digitale rom for å sikre egen handlefrihet vil derfor være viktige elementer i et lands forsvar, selv om maktanvendelse gjennom det digitale rom sannsynligvis ikke vil kunne avgjøre mellomstatlige konflikter alene*

(Forsvarsdepartementet, 2015-2016, s. 35).

Oppsummert er de viktigste formålene med tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon å etablere et troverdig forsvar mot cyberangrep og trusler i det digitale domenet, og at Norge kan forsvare seg selv og NATO i et trusselspenn som innbefatter langt mer enn det konvensjonelle forsvaret vi har i dag. Videre vil det gi norske myndigheter tilgang til etterretning relevant for norsk forsvars, utenriks-, og sikkerhetspolitikk, og kunne bidra til å identifisere og avdekke terrorplaner og terrorangrep på norsk jord (Lysne, 2016, s. 12).

Per i dag har Etterretningstjenesten begrenset evne til å fange opp grenseoverskridende kommunikasjon fra utenlandske aktører som kan utgjøre en trussel eller sikkerhetsutfordring. For

eksempel er det begrenset mulighet for å avdekke at en kjent terrorleder i Syria kommuniserer med ukjente personer i Norge. På samme tid er det svært begrensede muligheter for å avdekke at utenlandske aktører driver spionasje mot offentlige eller private virksomheter i cyberdomenet, eller driver påvirkningsoperasjoner. Dette betyr i praksis at slik aktivitet i dag ikke avdekkes eller identifiseres tidlig nok eller før skaden allerede har skjedd (Lysne, 2016, s. 28-29).

Flere stater som i dag bruker kapasiteter tilsvarende tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon innhenting kan sies å ha vært tilbakeholdende med å kommunisere offentlig om at slike kapasiteter benyttes. For å vise at innhentingen er målrettet og underlagt tilstrekkelige rettslige mekanismer har mer detaljert informasjon om reglene med tiden blitt gjort tilgjengelig for offentligheten. Dette for eksempel i Storbritannia hvor den britiske regjeringen offentliggjorde rapporten "Operational Case for Bulk Powers", "Bulk Personal Datasets - Impact Assesment" og "Report of the Bulk Powers Review" i 2016. Dokumentene er entydige når det gjelder verdien av massedatainnhenting. Videre argumenteres det for fortsatt innhenting, og dokumentene hevder at innhentingen ikke innebærer ulovlig masseovervåkning. Det fremkommer også at verdifull etterretning er kommet myndighetene i hende gjennom denne kapasiteten, og at det har bidratt til å redde liv og forhindre angrep med alvorlig skadepotensial. I Dagens Næringsliv i april 2020 argumentere sir David Omand, tidligere sjef for det britiske signaletterretningsorganet Government Communications Headquarters (QCHQ) og gjesteforeleser ved King´s College i London for at det norske samfunnet ikke bør frykte tilrettelagt innhenting, og viste til at tilsvarende system i Storbritannia hadde forhindret 15 terrorangrep i løpet av 18 måneder i 2019-2020. Omand antyder langt på vei at man ved å styrke Etterretningstjenesten med tilrettelagt innhenting vil kunne forvente en økning i vellykkede etterretningsprestasjoner i Norge. Omand skriver i sitt innlegg "Etterretning forutsetter at etterretningstjenester gis denne muligheten regulert i lov. Dette er god etterretning, ikke "masseovervåkning", som vil være ulovlig for enhver stat som har undertegnet den europeiske menneskerettighetskonvensjonen (Omand, 2020).

Sammenlignbare stater som Danmark, Sverige og Finland har allerede tilgang til kapasiteter tilsvarende grenseoverskridende elektronisk kommunikasjon for etterretningsformål

(Forsvarsdepartementet, 2019-2020, s. 87). U.S. Presidential Policy Directive 28 on Signals Intelligence Activities, begrunner slik type innhenting i USA på følgende måte:

> *"Locating new or emerging threats and other vital national security information is difficult, as such information is often hidden within the large and complex system of modern communications. The United States must consequently collect signals intelligence in bulk in certain circumstances in order to identify these threats"*

(The White House - President Barack Obama, 2014).

Per i dag mottar Etterretningstjenesten varsler og informasjon som baserer seg på slik innhenting fra samarbeidende tjenester i andre land, og det kan argumenteres for at det er en rekke problematiske sider ved dette. Varslene kommer gjerne sent, ettersom landene prioriterer trusler mot mål innenfor sine egne grenser først og fremst, og dermed kommer varslene til Norge for sent. Like fullt kan ikke Norge belage seg på at samarbeidende, utenlandske etterretningstjenester skal sette søkelys og arbeide for å motvirke trusler mot Norge (Forsvarsdepartementet, 2019-2020, s. 88).

Det er også en etisk side ved dette dersom Etterretningstjenesten ikke gis adgang til å drive slik innhenting. Norge vil like fullt være avhengig av at samarbeidende tjenester deler sin informasjon om slike trusler- og bruke denne, som i mange tilfeller vil være innhentet gjennom deres egen tilgang til grenseoverskridende elektronisk kommunikasjon (Lysne, 2016, s. 29). Det vil i så fall forbli et paradoks dersom Norge kan bruke slik informasjon til å beskytte seg mot trusler dersom den er innhentet av andre, men ikke innhente den selv.

Uten tilgang til informasjon som sendes over landegrensen med dagens kommunikasjonstjenester vil det bli vanskelig for Etterretningstjenesten å identifisere og varsle om utenlandske trusselaktører. En slik trussel må identifiseres tidlig, og man er avhengig av store datamengder for å klare å skille dem ut (The White House - President Barack Obama 2014). Manglende tilgang til informasjon vil kunne føre til svakere etterretningsprodukter og dermed beslutningsstøtte til norske myndigheter, som igjen kan føre til svakere beslutningsstøtte i

utformingen av norsk utenriks-, forsvars-, og sikkerhetspolitikk. På lengre sikt kan det medføre at Etterretningstjenesten vil få en svakere posisjon i informasjonsutvekslingen med samarbeidende tjenester, som igjen kan føre til at Norge ikke vil motta informasjon om identifiserte trusler som er relevant for Norge. Dette fordi man ikke vil sees på som en relevant samarbeidsaktør i et samarbeidsklima hvor informasjon er selve verdien (Lysne, 2016 s. 31). Med tiden kan dette føre til en betydelig svekkelse i norsk evne til å motvirke trusler fra utenlandske trusselaktører.

Wesley Wark argumenterer for at vi i dagens samfunn må forstå rollen teknologi har spilt- og vil fortsette å spille i utformingen av etterretningspraksis og kapasiteter. Teknologiutvikling var en nøkkeldriver for hvordan etterretningsfaget utviklet seg fra tidlig 1900-tallet og fremover. Dette eksemplifisert i hvordan bruk av radio i første verdenskrig åpnet muligheten for "sanntids" informasjon, og innhentingsdisiplinen SIGINT (signaletterretning) ble født. Videre hvordan luftfartspionerer som brødrene Wright la grunnlaget for IMINT (bildeetterretning) og "eyes in the sky", samt hvordan bruk av datamaskiner og Internett har gitt etterretningstjenestene tilgang til et globalt lager av kunnskap og søkemotorer for offentlig tilgjengelig informasjon gjennom OSINT (open-source intelligence) (Andrew, Aldrich & Wark, 2009, s. 523). Et tilbakeblikk på hvordan etterretningsfaget har utviklet seg historisk forteller at det er nødvendig for Etterretningstjenesten å tilpasse seg den til enhver tid teknologiske tilstanden og utviklingen i verden, med vår tidsepoke med Internett som intet unntak.

Lysne II-utvalget skriver også i sin utredning at de antar at det totale overvåkningstrykket i Norge stadig vil bli større dersom Etterretningstjenesten ikke gis tillatelser til innhenting av grenseoverskridende elektronisk kommunikasjon. Eksempelvis vil Nasjonal Sikkerhetsmyndighet (NSM) måtte overvåke trusselutsatte aktører eller grupper av aktører i mye større grad og Politiets Sikkerhetstjeneste (PST) vil måtte øke sin overvåkning av personer og grupper, samt i større grad dele personopplysninger til utlandet for å kunne avdekke eller forebygge trusler innenfor sine mandater. På samme tid skriver utvalget at økt overvåkning innad i Norge fra PST og NSM sin side etter all sannsynlighet ikke vil evne å avdekke de mest alvorlige truslene fra utlandet som kommuniserer mot personer eller digital infrastruktur i Norge, slik man ville kunnet med tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon (Lysne, 2016, s. 32).

Sett fra et annet perspektiv vil den vanlige norske brukeren av Internett eller digital kommunikasjonstjeneste ikke ha forutsetninger for å vite om datatrafikken en bruker kun går innenlands, eller også utenlands. Mange vil nok tro at dersom en sender e-post eller chatter med en person i Norge, så holder også kommunikasjonen seg innenfor Norges grenser. Spesielt er dette vanskelig all den tid store tjenester som Google, Facebook eller tilsvarende tjenester har servere utenlands, som i praksis gjør at store deler av norske internettbrukere sin datatrafikk vil omfattes av Etterretningstjenestens innhenting. Et viktig poeng her er at store deler av informasjonen som Etterretningstjenesten vil samle inn i store trekk ikke vil være relevant for dem, og den vil omhandle personer de ikke har mandat til å drive etterretningsaktivitet mot. I tillegg vil Etterretningstjenesten potensielt kunne få et omfattende innblikk i den norske befolkningens kommunikasjon og bruk av Internett som sådan. Dette kan oppfattes som problematisk, spesielt i et personvernsperspektiv.

2.6 Metadata og innholdsdata

I forslag til endringer i Etterretningstjenesteloven skilles det mellom metadata og innholdsdata. Det legges opp til at Etterretningstjenesten kan innhente metadata i bulk, og senere søke i innholdsdataene etter beslutning fra retten. Det er derfor relevant å beskrive hva metadata og innholdsdata er, for å forstå hvilken type informasjon som finnes i slike data.

Metadata er enkelt forklart data som beskriver andre data. Dette kan for eksempel være e-postadresser, IP-adresser, filtype, tidspunkt for en sending, herunder klokkeslett og dato, telefonnummer, varighet på samtaler, eller hvilke telefonnummer som ringer til andre telefonnumre. Videre kan metadata være geografisk plassering, tilbyder av kommunikasjonstjenesten som benyttes, IP-adresser og brukernavn. Eksempelvis vil det fra en smarttelefon gå en kontinuerlig datastrøm fra aktive apper, som vil kunne si noe om bruken av applikasjonen på telefonen. I metadataen får man ikke innsikt i selve innholdet i kommunikasjonen, som for eksempel teksten i en chat eller e-post, men informasjon om entitetene som kommuniserer med hverandre. For å trekke dette inn i den fysiske verden kan man se på metadata som adressat på et brev. Vi får altså informasjon om navn og adresse til den som

skal motta brevet og kanskje avsenders navn og adresse på baksiden. Vi får derimot ikke lese brevets innhold og tekst, som er "innholdsdata". Innholdsdata er altså selve informasjonen eller teksten som er skrevet i en e-post eller chat, men kan også være lydklippet av en telefonsamtale (Datatilsynet, 2019, s. 29-30).

Lagring, sammenstilling og analyse av metadata kan for eksempel gi informasjon over alle internettsider en bruker har besøkt i et gitt tidsrom, eller hvem brukeren har kommunisert med per e-post eller annen kommunikasjonstjeneste. Det er på denne måten Etterretningstjenesten ønsker å bruke informasjonen for å avdekke og identifisere trusler mot Norge. Ved å gjøre retrospektive søk i metadata, for eksempel etter en IP-adresse eller e-post kan man få innblikk i rekkevidden av et cyberangrep eller størrelsesorden i et terroristnettverk (Lysne, 2016, s. 25). På en annen side kan man lett tenke seg skadepotensialet som ligger i en slik innsamling, for eksempel i et personvernsperspektiv. Informasjon om at en person har sendt e-post til barnevernet, ringt politiet og legen samme dag kan fortelle mye, uten at man har tilgang til innholdsdata fra samtalene.

Innholdsdata på sin side er informasjonen som er selve innholdet i en fil eller annen digital ressurs, som for eksempel teksten i et dokument, bildet i et fotografi, samtalen i en chattelogg eller teksten i en e-post. Med referanse til den fysiske verden kan metadata være adressat på et brev, mens innholdsdata er brevets innhold, tekst og budskap. Innholdsdata slik det kommuniseres i dag er i grove trekk kryptert informasjon fra tjenesteleverandørens side (Datatilsynet, 2019, s. 29-31).

Dersom man ser innholdsdata i et personvernsperspektiv ser man at innsyn i slik informasjon kan gi tilgang til en person sine private tanker, følelser og privatliv gjennom dens korrespondanse, som treffer rett i kjernen av EMK art. 8 (FN, 1948). Videre vil innholdsdata kunne gi innsyn i en person sin politiske eller religiøse overbevisning, som treffer i kjernen av EMK art. 9 (FN, 1948).

2.7 Personvern

Personvern forstås i denne oppgaven som et bredt spekter av rettigheter og interesser knyttet til beskyttelse av personopplysninger og personlig autonomi. I kjernen er personvern å ha muligheten til å kontrollere tilgangen til, og spredningen av ens egne personopplysninger, samt retten til å ta beslutninger om eget liv uten innblanding. Dette inkluderer retten til å holde ens personopplysninger som navn, adresse eller kommunikasjon med andre konfidensiell, samt rett til å kontrollere hvem som har tilgang til denne og til hvilket formål det kan brukes (Datatilsynet, 2019). Personvernet er nært knyttet opp mot EMK art. 8 og EMK art. 9. Det kan argumenteres for at innsyn i opplysninger som metadata og innholdsdata i grunnen er det samme som personsensitive opplysninger som inngår i personvernet.

Personvern kan også være retten til å være fri fra uønsket oppmerksomhet eller inntrenging, slik som retten til privatliv i ens eget hjem eller personlig kommunikasjon. Personvern står imidlertid ofte i spenning med andre verdier, som sikkerhet, offentlig sikkerhet og retten til informasjon (NOU 2022: 11, s. 29). Som et resultat involverer personvernlover og -forskrifter ofte å balansere disse konkurrerende interessene for å beskytte enkeltpersoners personvern samtidig som det tillater statlig innsamling og bruk av personlig informasjon når det er nødvendig. Dette på lik linje som EMK, hvor det fremgår at slik informasjon som utgangspunkt være fri for inngrep fra myndighetene. Det finnes dog unntak, og det er disse unntakene som legges til grunn når man ønsker å gi Etterretningstjenesten lovlig adgang til metadata og innholdsdata som krysser Norges grense.

3. Høringsprosessen

3.1 Hva er en høring?

Ordet "høring" avledes av verbet å "høre". En betydning av verbet å "høre" er å lytte, og ved en høring signaliseres en vilje til å lytte til andres synspunkter (Språkrådet, 2018.)

Offentlige høringer brukes for å få samfunnets og relevante aktørers innspill på forslag til politiske vedtak. Det er en demokratisk prosess der organisasjoner, samfunnsborgere og næringsliv får ytret sin mening om et forslag til et vedtak før det fattes av forvaltningen eller beslutningstakere. Det er vanlig å ha nye forskrifter og lover ute på offentlig høring (Regjeringen, 2022).

Harold D. Laswell utviklet i 1950 en politisk stegmodell som beskriver politiske prosesser. Denne modellen blir ofte tatt utgangspunkt i når politiske prosesser skal studeres. Modellen består av fem steg: *agendasetting, politikkutforming, beslutning, iverksetting og evaluering* (Vabo, Klausen & Askim, 2020, s. 31-35). I politikkutformingsfasen er det viktig å innhente informasjon som forteller noe om hvordan samfunnet stiller seg til politikken som skal utformes. En måte å få samfunnets tilbakemeldinger på politikk er å bruke høringsprosesser (Vabo et al., 2020, s. 114-115). Høringsprosessen er dermed et ledd i politikkutformingsfasen i stegmodellen.

I dette tilfellet er det Forsvarsdepartementet som sendte endringer i Etterretningstjenesteloven ut på høring. Det er i denne prosessen at organisasjoner, samfunnsborgere og næringslivet har mulighet til å komme med uttalelser til lovforslaget.

En høringsinstans kan omtales som en organisasjon, virksomhet eller privatperson som har fått en invitasjon til å uttale seg om det som er til høring. Det er som regel instanser som jobber innenfor fagfeltet eller er berørt i en eller annen grad av det loven eller forskriften som er på høring omhandler (Tjernshaugen, Berg & Gisle, 2023).

3.2 Introduksjon til høringsprosessen

Med endringer i det sikkerhetspolitiske landskapet så vel som teknologisk utvikling, har det med tiden meldt seg behov for endringer i hvordan Etterretningstjenesten skal utøve sitt mandat. Inntil 1990-tallet var det ingen spesifikk lovregulering for hvordan Etterretningstjenesten skulle utføre sine oppgaver. Den første lovreguleringen kom i 1998, og denne har ikke vært endret frem til ny Etterretningstjenestelov ble vedtatt i 2020 (Sejersted, 2005, s. 121-123).

Den nye Etterretningstjenesteloven fra 2020 er i store trekk en videreføring av den foregående etterretningstjenesteloven fra 1998, imidlertid med noen forslag til endringer. Forsvarsdepartementet har i den nye loven ønsket å legge til lovhjemler for tilrettelagt innhenting. Dette er basert på Lysne II-utvalget sin rapport som argumenterer for at tilrettelagt innhenting vil "styrke Norges selvstendige etterretningsevne og vår mulighet til å oppdage og motvirke spionasje, sabotasje, terrorhandlinger og andre trusler mot nasjonale sikkerhetsinteresser" (Forsvarsdepartementet, 2019, s. 9-11).

EOS-utvalget skrev i melding til Stortinget 17. juni 2016 at Etterretningstjenesteloven fra 1998 burde gjennomgås. EOS-utvalget begrunnet dette i endringer i trusselbildet, teknologiutvikling og lovutvikling, herunder styrkingen av menneskerettighetenes stilling i norsk rett i 1999, samt ny paragraf i Grunnlovens § 102 om retten til privatliv i 2014 (EOS-utvalget, 2016). Stortinget fattet i februar 2017 vedtak der de oppfordret regjeringen til å revidere Etterretningstjenesteloven fra 1998 (Forsvarsdepartementet, 2019, s. 9-12).

Det ble sendt ut høringsnotat til ny Etterretningstjenestelov 12. november 2018. I det reviderte forslaget til loven ble det lagt til lovhjemler som omhandler tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon (Forsvarsdepartementet, 2019, s. 9-12).

Den nye Etterretningstjenesteloven ble vedtatt i Stortinget 11. juni 2020 i Stortinget med ikrafttredelse den 1. januar. 2021, med unntak av kapittel 7 og 8, som fikk ikrafttredelse 1. januar året etter. § 7-3 som omhandler tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon er fremdeles ikke gjort rettskraftig (Stortinget, U.Å).

I etterkant av at loven ble vedtatt ble det offentliggjort at Forsvarsdepartementet i samråd med deltakere fra Justisdepartementet og Utenriksdepartementet med fler ville gjøre en rettslig analyse

av kapittel 7 og 8 for å se om kapitlene i loven var i tråd med gjeldende rettspraksis fra EUs menneskerettighetsdomstol. De nye endringene ville bli sendt ut på ny offentlig høring (Regjeringen, 2022)

Det er i hovedsak foreslått tre endringer i Etterretningstjenesteloven fra 2020, og det er disse endringene som er sendt på høring og som denne oppgaven omhandler. Formålet med endringene er å styrke rettsvernet til journalistiske kilder, tilfredsstille internasjonale forpliktelser og at lovverket er i tråd med menneskerettighetene.

Loven med de foreslåtte endringene ble sendt på høring 19. juni 2022 med høringssvarfrist til 27. september samme år. Det ble anført at alle høringsinstanser som ikke var oppført kunne melde sin interesse. Siden dette var en offentlig høring, hadde også privatpersoner anledning til å sende inn sitt høringssvar (Regjeringen, 2022). Det betyr i praksis at alle som ville kunne sende inn høringssvar.

3.3 Høring - Forslag til endringer i Etterretningstjenesteloven

Det foreslås endringer i forhold til flere av paragrafene i Etterretningstjenesteloven.

Bakgrunnen for å sende deler av Etterretningstjenesteloven ut på offentlig høring var at EU-domstolen 6. oktober 2021 avsa dom i tre saker som sammen er omtalt som "La Quadrature du Net" og en annen som omtales som "Privacy International". Dommene ble brukt til å tolke EU sitt kommunikasjonsdirektiv. Norge er ikke EU-medlem og på den måten ikke forpliktet til å følge alle EU-direktiver slik som fullverdige medlemsstater, men som EØS-medlem er Norge forpliktet til å forholde seg til EUs kommunikasjonsdirektiv.

Videre ble det også avsagt dommer i Den europeiske menneskerettighetsdomstolen i mai 2021. Dette var "Case of Centrum för Rättvisa v. Sweden» og "Case of Big Brother Watch and Others v. The United Kingdom". Den juridiske analysen av dommene falt ned på at Etterretningstjenesteloven var i henhold til menneskerettighetene og kriteriene som ble listet opp i La Quadrature du Net dommen, med unntak av etterretningstjenesteloven § 7-3. Med bakgrunn i den juridiske analysen ble det besluttet at det skulle utformes et nytt lovforslag om hvem som skal beslutte innhenting av kildeidentifiserende materiale til etterretningsformål og hvem som

skal beslutte når det kan iverksettes tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon.

De største forslagene til endring i loven gjelder hvem som har rett til å beslutte bruk av kildeidentifiserende tiltak til etterretningsformål, jf. etterretningstjenesteloven §5-2. I det opprinnelige forslaget var denne beslutningen gitt til sjef for Etterretningstjenesten. I den nye prosessen er det foreslått at det er Oslo tingrett som skal gis slik beslutningsmyndighet. Oslo Tingrett er i dette høringsnotatet satt til å vurdere forholdsmessigheten ved å tillate bruk av kildeidentifiserende tiltak til etterretningsformål. Videre skal det stilles som vilkår at slike tiltak kun kan besluttes dersom det er "strengt nødvendig", og at hensynet til nasjonal sikkerhet overgår kildevernet. Hovedbegrunnelsen for denne endringen er for å styrke rettssikkerhetsgarantiene.

Den andre foreslåtte endringen er å endre § 7-3 i Etterretningstjenesteloven, som er vedtatt, men ikke iverksatt. Slik loven er utformet per i dag er det sjefen for Etterretningstjenesten som har beslutningsmyndighet for iverksettelse av tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon. I høringsnotatet foreslås det at også denne beslutningsmyndigheten skal gis til Oslo tingrett. Det presiseres også at tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon kun skal benyttes i saker som innbefatter en alvorlig trussel mot nasjonens sikkerhet, og kun der mindre inngripende virkemidler ikke er formålstjenlig (Forsvarsdepartementet, 2022 s.4).

4. Overvåkningsteori

4.1 Introduksjon til overvåkning

I introduksjonen til overvåkningsteorien vil vi forklare hva som inngår i begrepet overvåkning og om bruk av overvåkning som tiltak i en etterretningsprosess. En sammenfatning av disse teoriene blir presentert i form av et teoretisk rammeverk som vi vil bruke til analysen og drøftingen av høringssvarene.

Vi vil først gi en introduksjon til fenomenet overvåkning. Den sier noe om hva overvåkning er, og forskjellige typer overvåkning. Litteraturen vi har valgt å ta utgangspunkt i for å forklare overvåkningsbegrepet, er litteratur som tar utgangspunkt i rettsstaten sin overvåkning. Vi mener dette er relevant litteratur ettersom det er Forsvarsdepartementet som har utformet forslaget til loven og at det er Forsvaret, ved Etterretningstjenesten som skal anvende lovverket til tilrettelagt innhenting.

Videre i dette kapittelet vil vi gjøre rede for forskjellige teorier innenfor overvåkning. Teorien vi har valgt som hovedteori er inspirert av tradisjonen rettferdig krig, men er gjort om av forfatteren for å kunne brukes i en overvåkningskontekst. Teorien er ment som et etisk rammeverk for analyse av om det er moralsk å gjennomføre overvåkning, samt om måten det utføres på er moralsk forsvarlig. Vi vil bruke rammeverket til å analysere høringssvarene til lovforslaget.

Tilrettelagt innhenting er å regne som en overvåkningsmetode. Det er viktig å ha med seg at overvåkning i denne sammenhengen vil være et av flere tilgjengelige tiltak i en etterretningsprosess. Forsvaret definerer etterretningsprosessen som "Etterretning er resultatet av statlig sanksjonert innhenting, analyse og vurdering av data og informasjon, som er generert åpent eller fordekt og utarbeidet for å gi fortrinn i beslutningsprosesser" (Forsvaret, 2021, s. 20).

Born og Wetzling skriver at vestlige etterretningstjenester har den paradoksale oppgaven med å jobbe i det skjulte for å forsvare det åpne samfunn. Selv om sikkerhets- og etterretningstjenester underlegges lovverk, argumenterer Born og Wetzling for at etterretningstjenester i de fleste nasjoner blir behandlet som unntak fra resten av statsforvaltningen. Dette fordi de i skjul og hemmelighold er tillatt privilegert adgang til beslutningstakere og politikere, samt gitt spillerom

til å snoke og engasjere seg i ubehagelige aktiviteter som er ansett som upassende for andre offentlige etater. Resultatet av dette er at offentligheten har lite eller ingenting å si om hvilken informasjon som lagres eller sirkulerer rundt blant utøvende myndigheter (Born & Wetzling, 2007, s. 317) Dette kan være grunnlaget for skepsisen som følger i med å gi Etterretningstjenesten ytterligere adganger til å innhente informasjon som mange omtaler som masseovervåkning.

4.2 Overvåkning i et historisk perspektiv

Selv om vi i denne oppgaven ønsker å se nærmere på en svært moderne og digital form for overvåkning, er det lett å få en oppfatning om at overvåkning er et nytt fenomen. Overvåkning er en aktivitet som i forskjellige former har blitt brukt i tusenvis av år. Debatter om retten til bruk av overvåkning og personvern er hyppig omhandlet og dokumentert i litteratur skrevet lenge før det som regnes som den moderne tidsalder. I det gamle testamentet omtales Gud sitt altseende-øye som får med seg alle handlinger gjort av individer på jorden. Dette kan forstås som en form for overvåkning, der de troende vet at alle deres handlinger blir vurdert. Gud kan straffe individene for deres handlinger, men kan også utvise kjærlighet og beskyttelse (Marx, 2015, s. 733).

Dronning Elizabeth den første (1533-1603) uttalte at øyet var et vindu inn til en manns hjerte og dens største hemmeligheter. Hun var opptatt av balansen mellom statens behov for å ha kontroll med lovbrytere, men også å bevare personvernsrettighetene til de individuelle borgerne hun hadde ansvaret for. Hennes syn på overvåkning har store likhetstrekk med diskusjoner som gjøres rundt overvåkning i demokratiske stater den dag i dag (Marx, 2015, s. 733).

På slutten av 1700-tallet ble det laget beskrivelser av hvordan man skulle håndtere pestepidemier. I slike tilfeller ble byen delt inn i kvarterer, hvert kvarter ble holdt under oppsyn av en offentlig tjenestemann omtalt som en "syndig". Alle innbyggerne i hvert kvarter ble satt i karantene. De ville få rasjoner og nok til å overleve, men de hadde ikke lov til å forlate sine bopeler. Tjenestemannen sin oppgave var å låse alle bygårder og å holde oppsyn med kvarteret han hadde ansvaret for. Han kunne be innbyggerne når som helst om å vise seg for registrering. Dersom det var noen som ikke meldte seg, måtte det gjøres rede for. Denne tellingen ble transkribert og overlevert til intendant, en høytstående offentlig tjenestemann som hadde ansvaret for kvarteret.

Disse tellingene ble rapportert til sorenskriveren for kontroll og oversikt. Det ble opprettet sjekkpunkter i byen for å forhindre at innbyggerne forsøkte å forlate byen eller å bevege seg rundt. Dersom den offentlige tjenestemannen forsømte sine oppgaver, eller noen brøt karantenereglene, kunne de bli straffet. I ytterste konsekvens måtte de bøte med livet (Foucault, 1979, s. 195-199).

Jeremy Bentham designet et fengsel som han omtalte som *Panoptikon*. Fengselet hadde et tårn i midten der fangevokteren oppholdt seg. De innsatte var plassert i separate celler rundt tårnet. Tårnet var innrettet med vinduer på en slik måte at fangevokteren hadde anledning til å se de innsatte, uten at de innsatte klarte å se fangevokteren. Det var heller ikke anledning for de innsatte å samle seg i grupperinger eller å kommunisere med hverandre. Fangevokterne kunne aldri ha oppsyn med alle de innsatte samtidig, men siden de innsatte ikke kunne verifisere om de ble observert måtte de alltid ta høyde for at det kunne være tilfelle, men de innsatte kunne til enhver tid se tårnet som en påminner om at de kunne være under oppsyn. Denne anordningen skulle i teorien føre til selvsensur av de innsattes handlinger.

Foucault bruker Panoptikon som en metafor for å forklare hvordan samfunnet har makt ved å konstant overvåke befolkningen. Overvåkningen som beskrevet i det panoptiske fengsel kan også generaliseres og brukes i helsevesenet, skolevesenet, arbeidsplassen m.m. Slik overvåkning foregår overalt i samfunnet og av alle. Den utføres effektivt ved at færre individer trenger å utføre overvåkningen, og uten bruk av tvang. Slik overvåkning overført til andre områder i samfunnet kan ha den samme nedkjølende effekten på samfunnsborgernes livsførsel, slik som det er beskrevet i det Panoptiske fengsel (Foucault, 1979, s. 200-208).

Forskning på overvåkning i moderne tid startet på 1950-tallet. Dette skyldtes flere faktorer, blant annet at mange deler av verden hadde opplevd to verdenskriger, og at det var en periode der politiske ideologier som fascisme og kommunisme så dagens lys. Samfunnene som hadde styresett basert på disse ideologiene og verdisynene, var ofte gjennomsyret av overvåkning, spesielt fra myndighetene. Den styrende eliten i slike stater brukte ofte overvåkning for å kartlegge og luke ut politisk opposisjon og meningsmotstandere i den hensikt å sikre regimet sine maktposisjoner. En annen hendelse som har hatt mye å si for studier på overvåkning er terrorangrepene mot USA og World Trade Center 11. september 2001 (Marx, 2015, s. 734).

4.3 Hva er overvåkning?

I dette kapittelet vil vi ta for oss Dag Wiese Schartums (1956-) perspektiver på overvåkning, som vi mener er nyttige og relevante å bruke til analyse av vår empiri.

Før vi gjennomgår noen av perspektivene til Schartum ønsker vi å gjøre rede for hva overvåkning er. I etymologisk forstand stammer det norske ordet overvåkning fra tyske "überwachen" og betyr å holde oppsikt, passe på, følge nøye med på noe (Naob, u.å.).

Overvåkning kan utføres av myndighetsorganer, men også av private virksomheter eller privatpersoner. For at en aktivitet skal kunne omtales som overvåkning, mener Schartum at den må pågå over tid, være avgrenset og inneholde en viss systematikk. Dersom overvåkningen retter seg mot personer, er det personovervåkning. Det finnes også overvåkning som ikke retter seg mot personer, eksempelvis passive data som samles inn av vegtrafikksentralen for å si noe om belastning på veinettet. Overvåkning kan også utføres maskinelt ved bruk av innretninger som for eksempel kan lese bilskilt automatisk, eller ved bruk av manuelle metoder som spaning (Schartum, 2010, s. 21-22).

Dersom overvåkning som metode blir brukt for mye i et samfunn, kan man ende opp med det som beskrives av Schartum som et overvåkningssamfunn (Schartum, 2010, s. 7)

David Lyon (2001) definerer overvåkning som "any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered" (David Lyon, 2001, s. 2.)

Marx beskriver derimot overvåkning i sin enkleste form, kun som en aktivitet der det samles inn data, som kan analyseres for å gjøre om til informasjon (Marx, 2015, s. 736).

Videre deler Marx opp utførelse av overvåkning inn i to hovedkategorier, kontekst og utførelse. Han beskriver kontekst som hvilken institusjon og organisasjon som er omhandlet, og om hvilke mål, regler og forventninger de er forbundet med. Utførelsen beskriver forventninger i forhold til hvordan overvåkingen gjennomføres. Det kan være regulert av lov eller av mindre formelle forventninger (Marx, 2015, s. 734).

Overvåkning kan sorteres i forskjellige kontekster. Marx deler de forskjellige kontekstene inn i:

Type kontekst	Utføres av
Tvang	Myndigheter
Pleie	Helsevesenet
Kontrakter	Arbeid og konsum
Fri tilgang på tilgjengelig persondata	Det personlige og private innen det offentlige rom

Schartum omtaler to former for kilder til overvåkning. Den første er primærkilden. Det er kilden som er direkte tilgjengelig, som for eksempel politiets spaning mot en mistenkt person i en straffesak. Det samles store mengder data i forskjellige registre om norske borgere. Dette kan for eksempel være deres valutatransaksjoner eller bompasseringer. Denne informasjonen kan gjøres tilgjengelig for politiet ved behov, for eksempel i etterforskningen av en straffesak. Slik type informasjon er ifølge Schartum sekundærkilder (Schartum, 2010, s. 23-24).

Personovervåkning kan videre deles inn i to former. Den ene formen er overvåkning som rettes mot bestemte personer. En annen form er overvåkning som retter seg mot en ubestemt krets av personer. Sistnevnte kan være gjennomsnittsfartsmåling på en vegstrekning, eller vegtrafikksentralen sine kameraer som filmer de store veiaksene i Norge (Schartum, 2010, s. 27). Samfunnsutviklingen påvirker både mulighetene for hvilke typer personopplysninger som er teknisk mulig å samle inn, samt hvilke opplysninger det er ønskelig å samle inn.

Ifølge Schartum er metoden for hvordan informasjonen samles inn, og hvordan den brukes med på å si noe om hvor inngripende en overvåkning er i et personvernperspektiv. Det er vesentlig om dataene som innsamles direkte knytter seg til personer, slik som i en etterforskning, eller om de er selvstendige data som det krever et arbeide å knytte opp mot konkrete personer. Informasjon som

ikke direkte kan knyttes til en person, men der det er mulig i etterkant å identifisere personen det gjelder anses etter Personvernloven fortsatt som personopplysninger (Schartum, 2010, s. 28-30).

For å illustrere hvor inngripende overvåkningen er har Schartum laget en matrise som kan brukes til en slik vurdering.

		Maskinell tilgang	Manuell tilgang
Mulig ID	Vanskelig	1	2
Mulig ID	Lett	3	4
Etablert ID	Beskyttet	5	6
Etablert ID	Ubeskyttet	7	8

(Schartum, 2010, s. 30).

Dersom overvåkningen samler inn informasjon der identitet (ID) ikke er etablert, men er mulig å etablere, er det inndelt i kategorien "lett" og "vanskelig". Det er også et skille på om knytningen kan etableres gjennom en manuell eller en maskinell tilgang. Videre er det to rader i matrisen som beskriver informasjon som innhentes der den som informasjonen omhandler er etablert. Her skilles det også på om den innhentes maskinelt eller manuelt av en person. I matrisen er det et poengsystem fra 1-8, som illustrerer alvorlighetsgraden i lys av personvernet (Schartum, 2010, s. 30-31).

Ved en manuell menneskelig gjennomgang er det en større risiko for at vedkommende ikke har tilstrekkelig kunnskap om regelverket rundt håndteringen og innsynet i personopplysningene. Det

kan også være enkeltpersoner som av forskjellige grunner ikke ønsker å forholde seg til regelverket. Ved å bruke en maskin vil man ikke ha et slikt problem. Den kan programmeres på en måte som gjør at den etterlever regelverket, gitt at den er programmert riktig. Teknologien kan også brukes til å gjøre tilsyn med den manuelle omgangen av personopplysninger. Det kan gjøres ved å lage IKT-systemer som loggfører gjennomføringen og bruken av overvåkingen, slik at personene/myndighetene som gjennomfører overvåkningen kan kontrolleres av kontroll/tilsynsmyndigheter (Schartum, 2010, s. 30-32).

Schartum beskriver mekanismer som kan innføres for å "kontrollere kontrolløren", altså de som gjennomfører overvåkningen og får innsyn i personopplysningene. I tilfeller der det er en manuell tilgang til personopplysninger, kan denne tilgangen gis ved domstolskontroll for å begrense misbruk og urettmessig tilgang og bruk av personopplysningene. Der det brukes maskinell tilgang kan det genereres logger som kan gjennomgås av tilsynsmyndigheter (Schartum, 2010, s. 31).

Selv om det innføres gode mekanismer som skal sørge for at overvåkingen skjer i henhold til formålet gitt av lovverket, bør det tas hensyn til sårbarhetsprinsippet. Det består i å ha en tanke om hva informasjonen man samler inn kan brukes til hvis uvedkommende grupperinger, eller fremmede stater får tak i informasjonen. Det å samle inn store mengder personsensitive opplysninger er sårbart dersom det kommer uvedkommende i hende. Derfor bør det vurderes om den burde samles inn i det hele tatt, og på hvilken måte den sikres (Schartum, 2010, s. 34-35).

Gary T. Marx argumenter for at overvåkning også kan være en måte å beskytte personvernet på. Overvåkning kan brukes til å kontrollere hva som overvåkes, hvem som overvåkes, hvorfor det overvåkes (Marx, 2015, s. 736).

4.4 Kvein Macnishs prinsipper om rettferdig krigføring overført til en overvåkningskontekst

En av teoriene vi har valgt å ta utgangspunkt i vårt teoretiske rammeverk er Kevin Macnish sin artikkel "Just Surveillance? Towards a Normative Theory of Surveillance" (Macnish, 2014, s. 142-153). Teorien er et rammeverk for etisk diskusjon av overvåkningsmetoder. Vi ønsker å analysere høringssvarene ut fra Macnish teori for å se om høringssvarene kan fortolkes ut ifra hans perspektiver for å belyse problemstillingen vår. Macnish sine prinsipper blir presentert i en skjematisk oversikt, hvor vi så går gjennom prinsippene og forklarer disse.

Macnish mener at en etisk diskusjon av bruk av overvåkningsmetoder bør gjøres med prinsippene som finnes innenfor filosofi retningen "rettferdig krigføring", også kjent som *jus ad bellum*. Macnish argumenterer for at andre teoretikere som har forsøkt å lage etiske rammeverk for overvåkning enten har for upresise eller for få prinsipper de vurder ut fra. Macnish mener at prinsippene som finnes innenfor rettferdig krigføring dekker alle aspektene av diskusjonen om overvåkning (Macnish, 2014, s. 142-145). Vi mener derfor den er relevant i analysen av høringssvarene.

Det er åpenbare forskjeller mellom krigføring og overvåkning. I en krig utsettes partene og ofte tredjepart for svært brutale handlinger, som vold, lemlesting, voldtekt og drap. Det er sjelden at begge parter velger å gå til krig frivillig, men noen ganger velger man å overvåke frivillig. Macnish tar her for seg overvåkning som er utført uten samtykke. Han mener at prinsippene fortsatt er gode til bruk for etisk diskusjon og analyse av overvåkning, men med noen tilpasninger. Macnish sin teori er delt i to *Jus ad bellum* og *Jus in Bello*. Jus ad bellum tar for seg argumenter for om det er moralsk forsvarlig å innføre/iverksette overvåkning. Jus in bello tar for seg om selve utførelsen av overvåkningen er moralsk forsvarlig. Det skilles altså mellom iverksettelse av overvåkning og utførelsen av den. Det er syv prinsipper innenfor rettferdig krigføring som er omtalt som jus ad bellum og tre prinsipper innenfor Jus in bello som vil bli presenter skjematisk under (Macnish, 2014, s. 146).

Jus ad bellum:

En verdig sak:

Slik som rettferdig krigføring bør bruk av overvåkning ha et verdig formål. Det bør eksempelvis ikke brukes til fordel for enkeltpersoner i myndighetsappartet eller for personlig vinning eller fordeler for andre.

Et eksempel på et verdig formål er å bruke overvåkning til å beskytte innbyggerne i en stat. Det går også en grensedragning her, mange vil se det som uverdig formål dersom stater overvåker opposisjonspolitikere. Et annet vesentlig spørsmål som bør tas med i vurderingen er om det er et verdig formål er om det er et grunnlag for mistanke om noe straffbart/skadelig som overvåkningen retter seg mot (Macnish, 2014, s 147).

Korrekt intensjon:

Det er viktig at overvåkeren har riktig intensjon og ikke har en annen motivasjon enn det verdige formålet. For eksempel at overvåkningen brukes til et annet formål enn det overvåkningen var tiltenkt mot (Macnish, 2014, s. 148).

Autoritet:

I tradisjonen om rettferdig krigføring er det en forståelse om at det kun er moralsk forsvarlig at en selvstendig stat tar beslutningen om å gå krig. Macnish mener det stiller seg annerledes i forhold til overvåkning og mener at det også kan være moralsk forsvarlig om andre organer utfører overvåkning, som pressen, selskaper med flere. Macnish drar frem at det som er avgjørende er hvordan disse organene håndtere overvåkningsmaterialet. Det er av viktighet om overvåkning er regulert av lov. Hvis overvåkningen ikke er lovregulert, bør det stilles spørsmålstegn ved om det er moralsk forsvarlig å bruke overvåkning (Macnish, 2014, s. 148-149).

Nødvendighet:

Slik som med vurdering av å gå til krig, burde det gjøres en nødvendighetsvurdering før det tas beslutning om å bruke overvåkning. Det burde søkes å bruke lempeligere metoder først. Når slike metoder har vist seg ikke å gi ønsket effekt, kan overvåkning vurderes. Dersom hensikten er

skjult overvåkning må det tas en vurdering av hvilke midler som eventuelt brukes først, ellers kan det avsløre senere bruk av overvåkning (Macnish, 2014, s 150)

Erklæring av overvåkning:

Dette prinsippet er utledet av prinsippet om erklæring av krig. Det å kunngjøre at overvåkning skal brukes, kan være en ulempe dersom overvåkningen er ment til å være skjult. I andre tilfeller kan det være en fordel å kunngjøre at overvåkning er benyttet for å oppnå en avskrekkende effekt. Det kan være et skilt om at et bestemt område er overvåket, for eksempel i butikker som har hatt utfordringer med naskeri, eller farlige veistrekninger der det er ønskelig å redusere hastigheten (Macnish, 2014, s. 150).

Suksess eller mulig måloppnåelse:

Det må være sannsynlighet for å oppnå det oppgitte formålet med overvåkningen. Hvis overvåkning er benyttet for å forebygge kriminelle handlinger, uten at den har den ønskede effekten på overvåkningen, er det utfordrende å vurdere overvåkningen som legitim (Macnish, 2014, s. 150)

Proporsjonalitet:

I likhet med rettferdig krigføring er proporsjonalitet et prinsipp som må tas høyde for når en skal vurdere om overvåkningen er rettferdiggjort. Overvåkningsmetoden bør stå i forhold til det som den skal beskytte mot. Dersom overvåkningen ikke er proporsjonal til problemet, er den ikke legitim (Macnish, 2014, s. 150-151)

Jus in bello:

Prinsippene ovenfor kan brukes til å vurdere om det er moralsk forsvarlig å gå til skrittet å bruke overvåkning som metode. I tradisjonen jus in bello er prinsippene ment å si noe om hvordan krigføringen skal utføres. Macnish argumenter for at prinsippene det kan overføres til overvåkning.

Mala in se:

"Mala in se" er omtalt som virkemidler som er så ekstreme at de må regnes som upassende. I krigføring kan det være bruk av masseødeleggelsesvåpen eller mishandling av krigsfanger. Overført til en overvåkningskontekst kan overvåkning som er svært innskrenkende på uskyldige menneskers privatliv være en analogi. Macnish bruker som et eksempel tankelesing som et mala in se virkemiddel (Macnish, 2014, s. 150).

Proporsjonalitet:

I likhet med prinsippene i *jus ad* bellum, altså om det er rettferdig å gå til krig, er det det også et prinsipp om proporsjonalitet innenfor *jus in bello.* Fremfor en etisk diskusjon om det er riktig å gå til krig, eller dette tilfellet overvåkning, er fokuset dreid over til om overvåkningen står i proporsjonalitet til situasjonen som en befinner seg i. Dersom det i en by er et område der det begås svært mye kriminalitet, kan det være det være etisk forsvarlig å installere overvåkningskameraer i det aktuelle området. Det står i proporsjon til kriminalitetsbildet i området. Det vil trolig ikke være proporsjonalt å installere overvåkningskameraer i hele byen, gitt en slik kontekst. Det ville ikke være proporsjonalt, da man da vil overvåke store områder der det ikke er kjent at det er en høy grad av kriminalitet (Macnish, 2014, s 151).

Diskriminering:

I forståelse av rettferdig krigføring ser man på en som tar til våpen og kjemper som en stridende og som et legitimt mål. Individer som ikke tar til våpen og velger ikke å stride, er ikke legitime mål.

Den samme logikken kan brukes ved vurdering av hvem overvåkning skal rette seg mot. I istedenfor å definere stridende eller ikke stridende, vil man her lage et skille mellom skyldig og ikke skyldig, som respektive legitime og illegitime mål. Hvis man tenker i forhold til kriminalitet ville det ikke ha vært legitimt å bruke overvåkning mot noen som ikke har gjort seg skyldig i trusler mot sikkerhet eller straffbare handlinger. I mange tilfeller er det usikkert om individet er skyldig eller uskyldig. Da vil overvåkning kunne gi et svar på om individet er skyldig eller uskyldig, men Macnish poengterer at før en slik metode brukes, må det foreligge et

mistankegrunnlag mot individet før det kan være moralsk forsvarlig å overvåke det. Det må vurderes om mål/individet er et legitimt eller illegitimt mål for overvåkningen.

I et tilfelle der det er etablert et mistankegrunnlag mot et individ som har dannet et grunnlag for å beslutte å overvåke det, vil det ha vært legitimt selv om det viser seg at denne personen var uskyldig etter at overvåkningen var utført. Dersom det ikke foreligger et mistankegrunnlag mot individet, men overvåkning benyttes for å avdekke om individet er skyldig og resultatet viser at den overvåkede var skyldig, vil det allikevel ha vært et diskriminerende tiltak og ikke ha vært forsvarlig å bruke overvåkning som metode (Macnish, 2014, s. 151).

4.5 Stoddarts kritikk av Macnish sitt etiske rammeverk for bruk til overvåkning

Eric Stoddart skrev et motsvar til Macnish sin artikkel "Just Surveillance? Towards a Normative Theory of Surveillance" (Stoddart, 2014, s. 158-163). Vi mener det er interessant å se på kritikk av teorien til Kevin Macnish sin teori for å få et kritisk perspektiv inn i analysen av empirien i oppgaven vår. I likhet med hvordan Macnish sine prinsipper ble presentert, blir prinsippene i motsvaret også presentert skjematisk.

Stoddart problematiserer bruken av rettferdig krigføring som et etisk rammeverk for å vurdere om overvåkning er moralsk forsvarlig. Hans generelle synspunkter går ut på at Macnish i for stor grad har konsentrert seg om overvåkning fra et etterforskningsperspektiv. I beskrivelsen av prinsippene mener Stoddart at Macnish utilstrekkelig har forklart begrepene intensjon, samtykke og proporsjonalitet.

Stoddart problematiserer at Macnish ikke omfatter sammenstilling av data, dataovervåkning, sousveillance (sous er fransk for under og kan begrepet kan på norsk forstås som undersyn, der observasjonen/overvåkningen utføres av en vanlig borger mot makthavere/autoritetene) gruppeovervåkning med mer (Stoddart, 2014, s. 158).

Videre kritiserer han Macnish for å bruke rettferdig krig teorien som en normativ etikk. Stoddart skiller mellom normativ etikk på førstehånds nivå og annenhånds nivå. Normativ etikk på førstehånds nivå omhandler etikk og moral på et individ nivå. Teorien om rettferdig krigføring er på et annenhånds nivå, da den ikke tar opp direkte om noe er rett eller galt for et individ, men etiske retningslinjer i en krigskontekst. Stoddard mener Macnish sine argumenter er førstehånds

etiske. Macnish skriver i konklusjonen sin følgende om teorien om rettferdig krigføring "Can provide a powerful framework to help in establishing the rights and wrongs of surveillance" (Macnish, 2014, s. 152). Stoddart mener at Macnish ved å fokusere på rett og galt bruker førstehånds nivå (Stoddart, 2014, s. 158).

Jus ad bellum

En verdig sak:

Stoddart mener at Macnish har en mangelfull forklaring på hvordan det store temaet overvåkning skal kunne bli vurdert ut ifra dette prinsippet. Macnish argumenterer for at det må foreligge en undersøkelse som skaffer til veie informasjon som gir grunnlag for overvåkning. Det er ikke problematisert av Stoddart, men han mener overvåkning omfatter så mye at det med Macnish sin beskrivelse av prinsippet blir vanskelig å analysere for eksempel datainnsamling ut fra dette prinsippet (Stoddart, 2014, s. 160).

Korrekt intensjon:

Prinsippet beskriver at overvåkning skal kun utføres med korrekt intensjon. Det skal ikke ligge andre bakenforliggende motiver til grunn for å initiere overvåkning. Stoddart stiller retorisk spørsmål om det finnes noe slik som korrekt intensjon, helt uten hint av andre bakenforliggende årsaker. Det er også problematisk i tilfeller ved gjensidig likemannsovervåkning, eller i tilfeller der en har tilfeller av sousveillance, altså overvåkning nedenfra og opp, typisk borger overvåker myndigheter. Det er i mange tilfeller sivil ulydighet eller i sin ytterste konsekvens ulovlig. Det er da vanskelig å snakke om korrekt intensjon. Stoddart mener at Macnish har fokusert for mye på de mektige og ikke tatt for seg de mindre mektige formene for overvåkning, eksempelvis sousveillance (Stoddart, 2014, s.160).

Autoritet:

Stoddart mener at dette punktet er laget med utgangspunkt i at rett autoritet er en suveren stat/myndighet som tar beslutning om å gå til krig. Han mener at det er vanskelig å overføre det til en overvåknings kontekst og at argumentasjonen som brukes av Macnish fortsatt er for tett bundet opp mot teorien om rettferdig krig (Stoddart, 2014, s. 160).

Nødvendighet:

Macnish beskriver ut fra sin teori at overvåkning må være en siste utvei som kun skal brukes når lempeligere midler har vært vurdert. Stoddart mener at Macnish er for opptatt av etterforsking og en panoptisk forståelse av overvåkning og dermed overser andre felt der overvåkning fint kunne ha vært valgt som et førstevalg. Stoddart eksemplifiserer det med et eksempel fra helsevesenet der det er brukt sporingsbrikker for å ha oversikt over hvor demente befinner seg. I et slikt tilfelle mener han at det er vanskelig å se at overvåkning bør være en siste utvei. (Stoddart, 2014, s.160-161).

Erklæring av overvåkning:

Det handler om å overføre teori til praksis når det gjelder overvåkning. Teorien snakker om en intensjonsforklaring som er viktig i forbindelse med krigserklæring. Men når det kommer til overvåkning, er det ikke like enkelt å bare erklære intensjoner og forvente samtykke fra alle involverte parter. For eksempel tar rettferdig krig teorien ikke hensyn til et samtykke fra den andre staten som blir angrepet. Når det kommer til overvåkning, vil folk flest ikke ønske eller samtykke å bli overvåket uten videre, slik at det å ha en intensjonsforklaring er ikke nok når det gjelder overvåkning. Det må også være samtykke fra alle involverte parter. Hvis ikke kan det føre til alvorlige problemer og konsekvenser (Stoddart, 2014, s. 161).

Suksess/mulig måloppnåelse og proporsjonalitet:

Stoddart slår sammen Macnish sine to siste prinsipper, da han mener de begge går under proporsjonalitetsbegrepet. Det er et uklart begrep som det ikke finnes noen klare definisjoner på. Han mener at Macnish ikke har adressert godt nok hvilke utfordringer som følger med å vurdere proporsjonalitet, selv om Macnish selv vedgår at proporsjonalitet ikke alltid er klart (Stoddart, 2014, s. 161).

Jus in Bello

Proporsjonalitet:

Proporsjonalitetsvurderingen handler om hvilken type overvåkning som skal velges. I rettferdig krigførings teori legges det til grunn at det er en førkrigsfase, en krigsfase og en etterkrigsfase.

Dette kan overføres til enkelte politi- og sikkerhetstjenesters etterforskninger, men det kan ikke overføres til andre former for overvåkning som er mer permanent/evigvarende.

Macnish beskriver proporsjonalitet som noe som kan vurderes ut fra objektive kriterier, men ifølge Stoddart er det ikke mulig å vurdere proporsjonalitet basert på objektive kriterier (Stoddart, 2014, s. 162).

Diskriminering:

I teorien om rettferdig krigføring skal det skilles mellom stridende og ikke stridende. Det er utfordrende å kunne gjøre dette skillet i en krig. Macnish har overført det til en overvåkningskontekst. Det er også vanskelig å skille mellom de overvåkningen skal rette seg mot og de den ikke skal rette seg mot. Det gjelder spesielt former for overvåkning som dataovervåkning, datasammenstilling, og sosial sortering (Stoddart, 2014, s. 162).

4.6 Teoretisk rammeverk

Vårt teoretiske rammeverk forstås som Macnishs teori om prinsipper for overvåkning. Vi vil bruke Stoddards argumenter som en motvekt til Macnishs prinsipper i analysen. I tillegg vil vi bruke Schartums sårbarhetsprinsipp og hans poengmatrise for å beskrive hvor inngripende overvåkningen er, samt Marxs klassifisering av overvåkningskontekster. Videre vil vi se på beskrivelsene gitt i høringssvarene opp mot Foucault sin teori om panoptisk overvåkning.

Samlet gir dette rammene for hvordan vi ser på problemstillingen vår og vi vil analysere empirien vår ut fra dette rammeverket.

Det vil kunne være andre interessante perspektiver og potensielle funn i materialet, men fokuset vil være gitt det teoretiske rammeverket. Funn utenfor dette rammeverket vil ikke tas med i analysen, da vi vil ha søkelys på funn som kan besvare og er relevant for problemstillingen.

5. Metode

5.1 Metodisk fremgangsmåte

I denne delen av oppgaven vil vi legge frem den metodiske fremgangsmåten vi har valgt, beskrive, redegjøre for valg og hvordan vi har gått frem for å forstå og belyse problemstillingen.

Innen forskning har vi to hovedkategorier når det kommer til metode; kvalitative og kvantitative metoder. Kvantitative metoder brukes når man skal beskrive mengder og tall, mens kvalitative metoder er best egnet når man skal bruke ord for å beskrive eller forklare et fenomen eller problemstilling. Kvalitativ metode innebærer derfor at man benytter seg av et ikke-numerisk datamateriale, slik som intervjuer, observasjoner eller skriftlige og visuelle materialer. Målet med kvalitativ forskning er å forstå og tolke erfaringene, perspektivene og betydningen til de som studeres (Bryman, 2021, s. 372). Problemstillingen er derfor avgjørende for om man velger en kvantitativ eller kvalitativ tilnærming.

Dette kvalitative dokumentstudiet har en induktiv tilnærming, hvor formålet er å danne en helhetsforståelse av fenomenet som studeres. Den induktive fremgangsmåten innebærer også at fenomenet studeres uten klare forutsetninger og hypoteser. Det vil si at studiet har en relativt åpen tilnærming til å forstå fenomenet, hvor hensikten er å danne en forståelse av de ulike aspektene ved fenomenet (Halvorsen, 2008, s. 128-129).

Oppgaven er en kvalitativ studie av høringssvar til endringer i Etterretningstjenesteloven. Vi er interessert i å undersøke hva de forskjellige høringssvarene uttrykker, identifisere hva som oppfattes som de mest problematiske sidene med tilrettelagt innhenting, se hvilke argumenter som benyttes og analysere dette i lys av overvåkningsteori.

Asdal og Reinertsen (2020) skriver at vi ved å analysere politiske dokumenter kan forstå endringer og kamper i samfunnet: politiske kamper foregår på politiske arenaer og gjennom politiske prosesser der dokumenter- som høringssvar – står helt sentralt. Kampene foregår nettopp på slike *steder*, i og rundt dokumentene (Asdal & Reinertsen, 2020, s. 36).

For å svare på problemstillingen må vi gå i dybden og analysere informasjonen som ligger i høringssvarene. Det blir derfor naturlig å benytte dokumentanalyse fordi utgangspunktet for studien er skriftlige høringssvar. Dokumentanalyse er studiet av dokumenter eller tekster, og skiller seg fra annen data som samles inn til forskningsformål ved at de er skrevet for et annet formål enn det forskeren skal bruke dem til (Thagaard, 2013, s. 59).

Det er både fordeler og ulemper ved å studere dokumenter. En fordel er at høringssvarene er skrevet på forhånd og av andre, noe som skaper avstand til datamaterialet ved at vi som skal forske på dem ikke kan påvirke utformingen, som for eksempel ved intervju. En annen side ved dette er at vi som forskere ikke har mulighet til å stille oppklarende spørsmål til teksten. I behandlingen av dokumenter er det også avgjørende å være bevisst på at alle dokumenter har ulik oppbygning og struktur, de har forskjellige språklige stiler, ulik argumentasjon og narrativ. Måten en tekst er bygget opp på er viktig for hvordan et tema eller en sak blir presentert, og hvordan den kan bli forstått (Asdal og Reinertsen, 2020, s. 87).

Thagaard (2013) lister opp flere metoder for å samle data ved kvalitativ metode, blant annet analyse av foreliggende tekster (Thagaard, 2013, s. 12-13). Den mest relevante fremgangsmåten for vår oppgave er analyse av foreliggende tekster, som vi heretter vil omtale som dokumentanalyse. Høringssvarene er dokumenter som i utgangspunktet ble skrevet for noe annet enn forskningsformål. På den måten skiller vårt datamateriale betydelig fra datamateriale som eksempelvis er innsamlet gjennom intervjuer. Derfor kan vi ikke bare velge å forholde oss til selve innholdet i dokumentene, men også hvilken kontekst de er skrevet. Høringssvarene som offentlige dokumenter har et klart formål, nemlig gi en tilbakemelding på et høringsnotat som foreslår endringer og justeringer til en vedtatt lov. Høringssvarene er skrevet av organisasjoner eller personer som enten har spesiell kunnskap om temaet eller som på en eller flere måter vil berøres eller engasjerer seg i forslaget, og som vil ytre sine synspunkter. Dette er forhold vi må være bevisst. Allikevel er det en fordel at høringssvarene vil være primærkilder, slik at analysen ikke blir farget av tidligere tolkninger.

På bakgrunn av ovennevnte momenter har vi vurdert at observasjon er en uegnet metode for å besvare vår problemstilling. Det er vanskelig, og kanskje umulig, å observere aktørers holdninger til hva de mener om et lovforslag. Videre har vi vurdert det som utfordrende å intervjue høringsinstansene som i hovedsak er organisasjoner. Høringssvar ble ofte skrevet som et resultat av innspill og på tvers av avdelinger og enkeltpersoner, som ville medført et stort antall intervjuobjekter per høringsinstans. Vi mener at vi ikke ville kunne klare å fange essensen i hva høringsinstansene mener ved å intervjue representanter for høringsinstansene, først og fremst fordi vi hadde måttet hatt flere intervjuobjekter per høringsinstans, men også fordi det totalt sett er så mange høringsinstanser med i prosessen at mengden intervjuer ikke hadde blitt håndterbart for en oppgave på denne størrelsen. Uavhengig av foregående argumentasjon fremstår dokumentanalyse som det mest relevante alternativet ettersom materialet vi skal undersøke er skriftlig, og det eksisterer i skriftlig format.

5.2 Tematisk analyse

Vi har brukt Braun & Clark (2006) sin fremgangsmåte for tematisk analyse (Braun & Clark, 2006, s. 86-93). Tematisk analyse er en kvalitativ dataanalysetilnærming som brukes til å identifisere mønstre og begreper i data. Vi mener dette passer for vår oppgave, ettersom vi skal identifisere hva som oppleves som de største utfordringene med tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon.

I Brymans bok (2021) er tematisk analyse en distinkt tilnærming til kvalitativ dataanalyse som fokuserer utelukkende på analyse og ikke datainnsamling. Bryman (2021) argumenterer for at i motsetning til kritisk diskursanalyse har ikke tematisk analyse et klart definert sett av teknikker. Begrepet brukes ofte i ulike kvalitative dataanalysetilnærminger, som kvalitativ innholdsanalyse, og temaer kan sees på som det samme som koder eller grupper av koder, avhengig av forskerens tolkning. Tematisk analyse innebærer flere stadier: Familiarisering; som inkluderer transkribering av intervjuer, skriving av feltnotater, og undersøke dokumenter. Innledende kodinger; koding for å fange opp nye egenskaper ved dataene, etterfulgt av mer teoretisk koding av relevante begreper. Identifisering av temaer innebærer å sammenligne koder med tidligere koder og teoretiske

begreper. Gjennomgang av temaer kombinerer dem til konstruksjoner av overordnede temaer og undertemaer (Bryman, 2021, s. 537-538).

Å definere temaer i tekstene bidrar til å beskrive deres egenskaper og relasjoner. Til slutt brukes temaene for å underbygge analysen og knytte den til litteratur. Som et resultat er tematisk analyse relevant for vår oppgave fordi det er en kvalitativ dataanalysetilnærming som kan brukes til å identifisere temaer og mønstre i høringssvarene. Ved å bruke tematisk analyse, kan vi identifisere og analysere tilbakevendende temaer og mønstre som dukker opp fra høringssvarene, som gir innsikt i hva som oppleves som de mest problematiske sidene ved tilrettelagt innhenting. I tillegg er stadiene i tematisk analyse, slik som familiarisering, innledende koding, identifisering av temaer og definering av temaer arbeid som kan hjelpe oss å organisere og analysere dataene på en systematisk måte, som til slutt fører til en bedre forståelse av problemstillingen vår. Vi har valgt å gå for en semantisk analyse, som vil si at temaene er definert ut fra det overfladiske meningsinnholdet i dataen. Dette fremfor den latente fremgangsmåten som søker å forklare de underliggende ideene eller bakenforliggende årsakene til funnene (Braun & Clark, 2006, s 84).

5.3 Koding og kategorisering

For å bli fortrolig med innholdet i høringssvarene leste vi gjennom høringssvarene både hver for oss og sammen for å få et inntrykk av hovedtrekkene. Vi gikk gjennom materialet én gang hver for oss, og to ganger sammen.

Når man får nær kontakt med innholdet i dataene vi skal analysere får vi tidlig et grunnlag for å se mønstre og sammenhenger, samt utvikle grunnleggende forståelse for innholdet (Thagaard, 2013, s. 158). Da vi gikk gjennom materialet alene gjorde vi det i den hensikt å se om vi fant mønstre eller temaer vi fant interessante, og noterte dem på lapper. Corbin & Strauss (2008) omtaler denne øvelsen som “open coding” (Corbin & Strauss, 2008, s. 198-199). I praksis betyr dette at vi avgrenset utsnitt i dataene med begreper som gir uttrykk for innholdet i teksten (Corbin & Strauss, 2008, s. 159-165). Når gjennomgangen var gjort hver for oss sammenlignet vi om vi hadde overlappende problemstillinger som kunne slås sammen eller burde splittes, og laget nye

overordnede grupper basert på våre felles kodinger. Den første gjennomgangen var en manuell gjennomgang.

På overordnet nivå krever koding og kategorisering at vi som forskere reflekterer nøye over sammenhengene mellom kodene vi velger å benytte slik at vi bruker begreper som er med på å fremme dataenes meningsinnhold (Thagaard, 2013, s. 159). Ved gjennomgang ble det identifisert at vi hadde flere av de samme, eller overlappende, problemstillinger. Andre var forskjellige, men forskjellene var på nivå heller enn meningsinnhold. Vi hadde som mål å komme til enighet om tre eller fire grupper. Øvelsen resulterte i at vi kom til enighet om tre slike hovedgrupper.

For å kvalitetssikre den manuelle gjennomgangen valgte vi å gjøre en ny gjennomgang i samråd. Vi støttet oss på den gamle kodingen, men valgte denne gangen å gjøre en digital gjennomgang med kode- og analyseverktøyet Nvivo. Programmet brukes for å analysere tekst og større datamaterialer, for eksempel lese dokumenter på tvers, altså systematisk se etter sammenfall eller ulikheter på tvers av dokumentene (Asdal & Reinertsen, 2020, s. 179). Vi gjorde øvelsen to ganger digitalt for å kvalitetssikre. Kvalitetssikringen resulterte kun i mindre justeringer. Problemstillingene vi identifiserte er grunnlaget for modellen vi utarbeidet som skal være utgangspunktet for analysen. Modellen blir presentert senere i analysedelen av oppgaven.

Kvale & Brinkmann omtaler denne fremgangsmåten som "kategorisering av mening" (Kvale & Brinkmann, 2009, s. 211). Kategoriseringen gjør at vi kan identifisere temaer med direkte referanser til problemstillingen vår, hvilke sentrale hovedtemaer som foreligger, samt mønstre i materialet. Videre bidrar kategorisering til at vi må reflektere over hvordan kodene vi har utviklet kan klassifiseres og hvilke betegnelser vi velger å gi dem (Thagaard, 2013, s. 160). Et moment vi var bevisste på i denne prosessen var at vi ved å kategorisere også fremhevet mønstre i dataene, og dermed også lukket døren for andre perspektiver. Et bestemt søkelys på materialet ut ifra visse kategorier gjør at det er andre mønstre som ikke vil observeres. Det var derfor viktig å være tydelig på hvilket perspektiv vi har når vi analyserer materialet (Silverman, 2010, s. 238).

I denne prosessen er vi som forskere bevisst på at kodingen vi velger å gjøre innebærer både beslutninger og tolkninger som har konsekvenser for den videre analysen. Dette fordi hver kode i

datamaterialet representerer enkeltsetninger eller avsnitt, men også en sammenfatning og reduksjon av de opprinnelige dataene (Thagaard, 2013, s. 162). Disse beslutningene og tolkningene baserer seg på vår forforståelse, samt hva vi forstår som de viktige og mindre viktige delene av materialet. Andre som forsker på det samme temaet, vil trolig kategorisere og kode på en annen måte. Vår tolkning av høringssvarene vil antakeligvis bli påvirket gjennom analyseprosessen etter hvert som vi tilegner oss flere perspektiver (Thagaard, 2013, s. 160). Det er derfor viktig at vi gjennom prosessen har et bevisst forhold til dette.

5.4 Analytisk fremgangsmåte

Vi har inndelt analysen i egne kapitler på samme måte som beskrevet i analysemodellen, herunder demokratisk, juridisk og praktisk. I analysen vil vi trekke ut eksempler innenfor hver problemstilling, ofte i form av et representativt sitat fra høringssvaret. Vi vil først analysere problemstillingen opp mot det teoretiske rammeverket, deretter vil vi komme med våre egne betraktninger i en drøftelse. I analysen tilstreber vi å triangulere i form av at vi kombinerer empiri mot teori, og til slutt våre egne vurderinger og betraktninger.

5.5 Forforståelse

Gadamer (1960) skriver at det bare er på bakgrunn av en forståelse som vi allerede har etablert, at vi kan danne oss en mening eller oppfatning (Gadamer, 1960, s. 130-133). Når dokumenter leses, vil leseren møte teksten med en viss forforståelse og forventning. Dette vil farge lesningen og tolkningen av dokumentet. Det er derfor viktig at vi gjennom hele forskningsprosessen er bevisst på vår egen forforståelse og at denne kan endre seg ettersom prosessen skrider fremover. Vi vil eksempelvis kanskje se nye ting eller andre perspektiver i et høringssvar om vi vender tilbake til det flere ganger.

Vår egen forforståelse om tilrettelagt innhenting er blitt preget av det vi har lest og at tematikken har engasjert oss. Forforståelsen har også betydning for hva vi forventet å få ut av studien og hva vi trodde vi kom til å finne. For eksempel hadde vi en antakelse om at personvern vil settes opp mot statssikkerhet, og at mange ville være negative til lovforslaget grunnet personvernhensyn.

Denne antakelsen bygger blant annet på erfaringer vi har gjort oss i arbeidslivet, samt flere endringer vi har observert etter innføringen av personvernforordningen (GDPR) i 2018.

5.6 Etiske vurderinger

Problemstillingen, metoden og datamaterialet som ligger til grunn for oppgaven medfører ingen spesielle etiske problemstillinger. Dokumentene som skal brukes er offentlige dokumenter som er tilgjengelig for alle. Oppgaven handler om å kategorisere høringssvarene og analysere dem på bakgrunn av definerte kategorier i den hensikt å si noe meningsfullt om hva høringsinstansene og privatpersoner opplever som de største utfordringene med innføring av tilrettelagt innhenting. Det ville for eksempel vært knyttet strengere krav til behandling av opplysninger og gjengivelse av intervjuobjekter dersom vi hadde valgt å innhente informasjonen gjennom intervjuer. Uavhengig er det i dokumentanalyse krav om å gjengi informasjonen som kommer frem på en så korrekt og etterprøvbar måte som mulig, og opprettholdelse av objektivitet blir særdeles viktig. Feiltolkninger kan forekomme gjennom ulike fordommer. På samme tid er tolkninger subjektive, og det inkluderer også forfatterne av denne oppgaven. Det blir derfor viktig at vi validerer informasjonen fra høringssvarene for å redusere eventuelle feiltolkninger eller effekten av fordommer (Rønnfeldt, 2005, s. 38-39).

God forskningsetikk handler om et sett av verdier, normer og institusjonelle ordninger som konstituerer og regulerer vitenskapelig virksomhet (Den nasjonale forskningsetiske komité for samfunnsvitenskap og humaniora, 2016, s. 7). En mulig forskningsetisk utfordring er våre egne roller som ansatte i statsforvaltningen. Med bakgrunn i dette kan vi forstås som aktører, dog i begrenset grad ettersom vi ikke har, eller har hatt noen involvering i prosessene. Allikevel kan det være en utfordring for oss å holde avstand til det vi skal studere, fordi vi kan identifisere relevante erfaringer eller ha sterke meninger om visse tema. Dette har vi et bevisst forhold til i arbeidet med oppgaven. Vi har også som statsansatte både bevisst og ubevisst utviklet en forståelse og personlige meninger om tilrettelagt innhenting og hvordan dette bør benyttes. Dette vil for eksempel være formet av tidligere erfaringer, problemstillinger vi har stått ovenfor i arbeidssammenheng kombinert med vårt faglige utgangspunkt. Fagene vi har tatt på Høgskolen i Innlandet og miljøene vi er sosialisert inn i på arbeidsplassen vår er formet av ideologiske

strukturer som også vi er påvirket, og i ulik grad formet av. Dette er en utfordring vi er oppmerksomme på og det er viktig for å kunne opprettholde kredibilitet i analysen.

5.7 Reliabilitet

God henvisningsskikk er en viktig forutsetning for at studien vår skal ha god reliabilitet og ivareta forskningsetiske hensyn. Videre er det viktig at studien ikke generaliserer i større grad enn med bakgrunn i høringssvarene. Høringsinstansene er organisasjoner som i en eller annen grad påvirkes eller har faglig kunnskap innenfor området, og det er naturlig at disse har mer å ytre om temaet enn den generelle befolkningen.

Reliabilitet handler om at studien skal kunne etterprøves. Vil andre kunne komme frem til det samme resultatet ved å gjennomføre den samme studien med de samme betingelsene? For å opprettholde og styrke reliabiliteten til studien vår er det viktig å beskrive forskningsprosessen nøyaktig og begrunne alle valg som er gjort underveis i prosessen (Bryman, 2016, s. 154-155). Vi må derfor være tydelige på hvilke valg vi har gjort og hva som er vurderingen bak valgene. For å sikre at kategoriseringen og kodingen vår er best mulig, har vi gått gjennom dem flere ganger i samråd, men også gjort det hver for oss. Videre har vi kategorisert og laget modell med bakgrunn i funn vi har gjort i kodingen, hvor begrunnelser for valg av kategorier er viktig.

Ettersom vi skal benytte dokumentanalyse som metode får vi fra begynnelsen avstand til datamaterialet. Allikevel er det viktig å være bevisst på hvordan vi kan påvirke forskningsprosessen gjennom våre vurderinger, valg og fortolkninger. Vi vil ha bevisste og ubevisste forutinntattheter om temaet som kan gjøre at vi vurderer subjektivt og ikke objektivt. Vi mener at analysemodellen vil være en motvekt til dette fordi den vil tvinge oss inn i bestemte og forskjellige perspektiver og utgangspunkt når vi analyserer. Videre blir det viktig for oss å begrunne og dokumentere våre egne fortolkninger av høringssvarene underveis. Vi må også være bevisst på hvordan vår egen forforståelse kan påvirke disse fortolkningene og vurderingene.

En trussel mot reliabilitet er et dårlig utvalg. Vi har derfor valgt å ta med alle høringssvar som treffer problemstillingen i form av at de presenterer problemstillinger rundt tilrettelagt

innhenting. Videre har vi tatt ut høringssvar som ikke har et meningsinnhold som det er mulig å analysere. Eksempler på dette er tomme dokumenter eller at det kun er skrevet "nei".

5.8 Utvalg og datamateriale

Det er 38 høringssvar i datamaterialet som danner grunnlaget for empirien i oppgaven. Etter å ha lest alle høringssvarene ble det klart for oss at enkeltindivider og organisasjoner svarer på forskjellige måter. Vi har notert oss at høringsinstansene som er negative til forslaget har til dels omfattende høringssvar, de som er positive eller ikke har anmerkninger velger å ikke komme med et svar, eventuelt meget korte svar. Hovedkategoriene vi har identifisert i høringssvarene er at det er juridiske argumenter, praktiske argumenter og demokratiske argumenter, som også er utgangspunktet for modellen som blir presentert i analysen.

Vi har lastet ned alle innsendte svar som var tilgjengelige på regjeringen sin nettside for høringsprosessen. Høringsprosessen har vært offentlig og det har vært åpent for at alle privatpersoner, virksomheter, foreninger m.m. har anledning til å sende inn høringssvar. Det ble riktignok i forkant sendt ut varsel til identifiserte høringsinstanser. Disse ansees som relevante da flere av høringsinstansene har kunnskap om temaet og faget, og sånn sett kan uttale seg på et kvalifisert, faglig grunnlag. Til tross for dette er det langt fra alle instansene som har svart på høringsnotatet.

Det vil ikke være mulig å generalisere svaret på studien til den øvrige populasjonen i Norge med tanke på det lille antallet svar fordelt på en relativt snever gruppe av virksomheter, organisasjoner, foreninger, privatpersoner med mer. Vi har valgt å skrive en kvalitativ masteroppgave, som heller søker å gå i dybden på en tematikk fremfor å gå i bredden slik et kvantitativ design vil (Oppen, Mørk & Haus, 2020, s.31).

Det kan argumenteres for at høringssvarene gir uttrykk for de sterkeste faglige motpolene i denne debatten, men også privatpersoner som kan tenkes å være spesielt opptatt av tematikken av personlige, ideologiske eller politiske årsaker. Det er for oss nyttig å kunne fange opp slike motsetninger og bruke det til analyse i oppgaven vår. Vi mener det vil kunne gi en pekepinn på hva majoriteten kan mene om tilrettelagt innhenting, men å kunne si noe sikkert om det er umulig

med et slikt utvalg. Flere av høringssvarene er dog velbegrunnede og går i dybden på hva de forskjellige respondentene mener er problemstillingene ved tilrettelagt innhenting. Derfor mener vi at det er et godt empirisk grunnlag.

De innsendte svarene er kategorisert inn i forskjellige kategorier på regjeringens nettsider. Vi har valgt å forholde oss til noen av de samme kategoriene, da vi mener de beskriver godt spennet av forskjellige høringssvar. De er nå gruppert inn i tre forskjellige kategorier: Arbeidstaker- og interesseorganisasjoner, private virksomheter, offentlige etater og privatpersoner.

Vi har valgt å ta vekk høringssvar som er inngitt uten merknader, da slike høringssvar ikke inneholder tekst eller meningsinnhold som kan analyseres. Videre er det flere offentlige etater som har levert høringssvar uten merknad. Dette er PST, Justisdepartementet, Teleplan Globe, Norges Høyesterett, Norsk senter for informasjonssikring, Borgarting lagmannsrett, Domstolsadministrasjonen og IBM. Telenor er også tatt ut da svaret ikke er relevant for problemstillingen. Telenor hadde i sitt høringssvar ingen innsigelser mot lovforslaget og fremstår langt på vei positiv. Ettersom vi skal analysere problemstillingene med lovforslaget, valgte vi å ta ut Telenors høringssvar da vi mente at svaret ikke tilfører analysen relevant innhold.

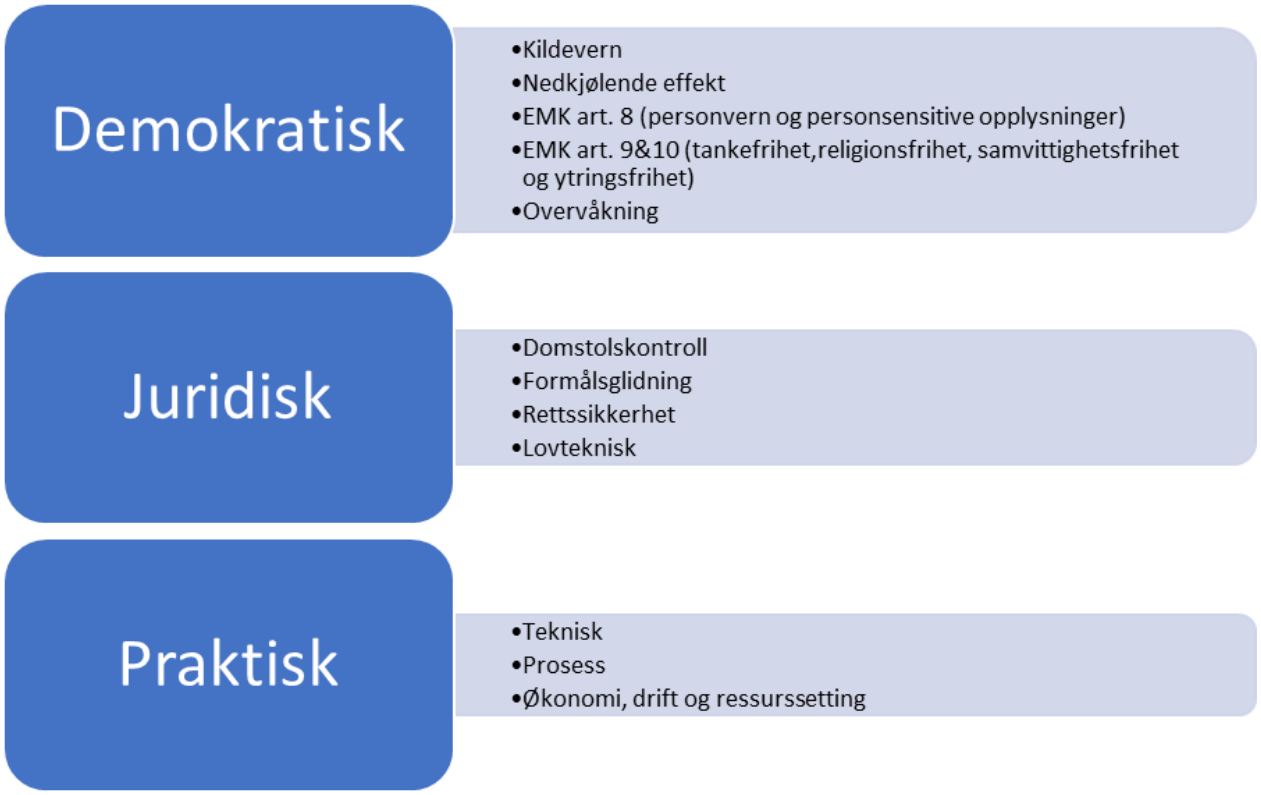
Vi har også gjort de samme valgene ovenfor høringssvar som er sendt inn av privatpersoner. De høringssvarene som ikke inneholder meningsinnhold som kan analyseres, er tatt ut. Eksempler på dette er at det kun er skrevet “nei” eller et tomt dokument uten merknad. Totalt gjelder dette 4 høringssvar fra privatpersoner.

38 høringssvar er dermed redusert til 25, og det er disse 25 som er gjenstand for vår analyse.

6. Analyse av høringssvar

6. 1 Analysemodell for høringssvar:

For å gjøre analysen mer oversiktlig har vi delt problemstillingene i høringssvarene inn i grupper, herunder demokratiske, juridiske og praktiske problemstillinger. Hver gruppe har underliggende problemstillinger som er kodet ut fra høringssvaret. Viser til modell under.



Under følger en mer detaljert beskrivelse av de forskjellige grupperingene.

Demokratisk:

Ved gjennomgang ser vi gjennomgang av høringssvarene at mye av meningsinnholdet tok opp temaer eller problemstillinger som er essensielle eller forutsettende for demokratiet, eller demokratiske rettigheter. Vi har også valgt å sortere menneskerettighetene under denne bolken, da vi mener de er nær beslektet og befinner seg i et annet domene enn meningsinnholdet vi har sortert under "juridisk". Vi har valgt å sortere "overvåkning" som en egen kode ettersom det stadig var uklart for oss hva som var argumentet eller den bakenforliggende årsaken til bruken av begrepet, da de i liten grad var begrunnet.

Juridisk:

Videre ser vi av høringssvarene så vi også at flere av høringssvarene hadde et meningsinnhold som omhandlet flere nyanser av det vi mener er juridiske implikasjoner eller begrunnelser. Vi ser at "domstolskontroll" og "rettssikkerhet" har overlappende meningsinnhold. Vi har allikevel valgt å beholde disse kategorien adskilt fordi begrepet brukes eksplisitt i flere av høringssvarene, og derav viktig å holde disse adskilt for å unngå å miste nyansene i analysen. Svak eller manglende domstolskontroll kan føre til dårlig rettssikkerhet, men det er også en indirekte konsekvens av svak domstolskontroll.

Praktisk:

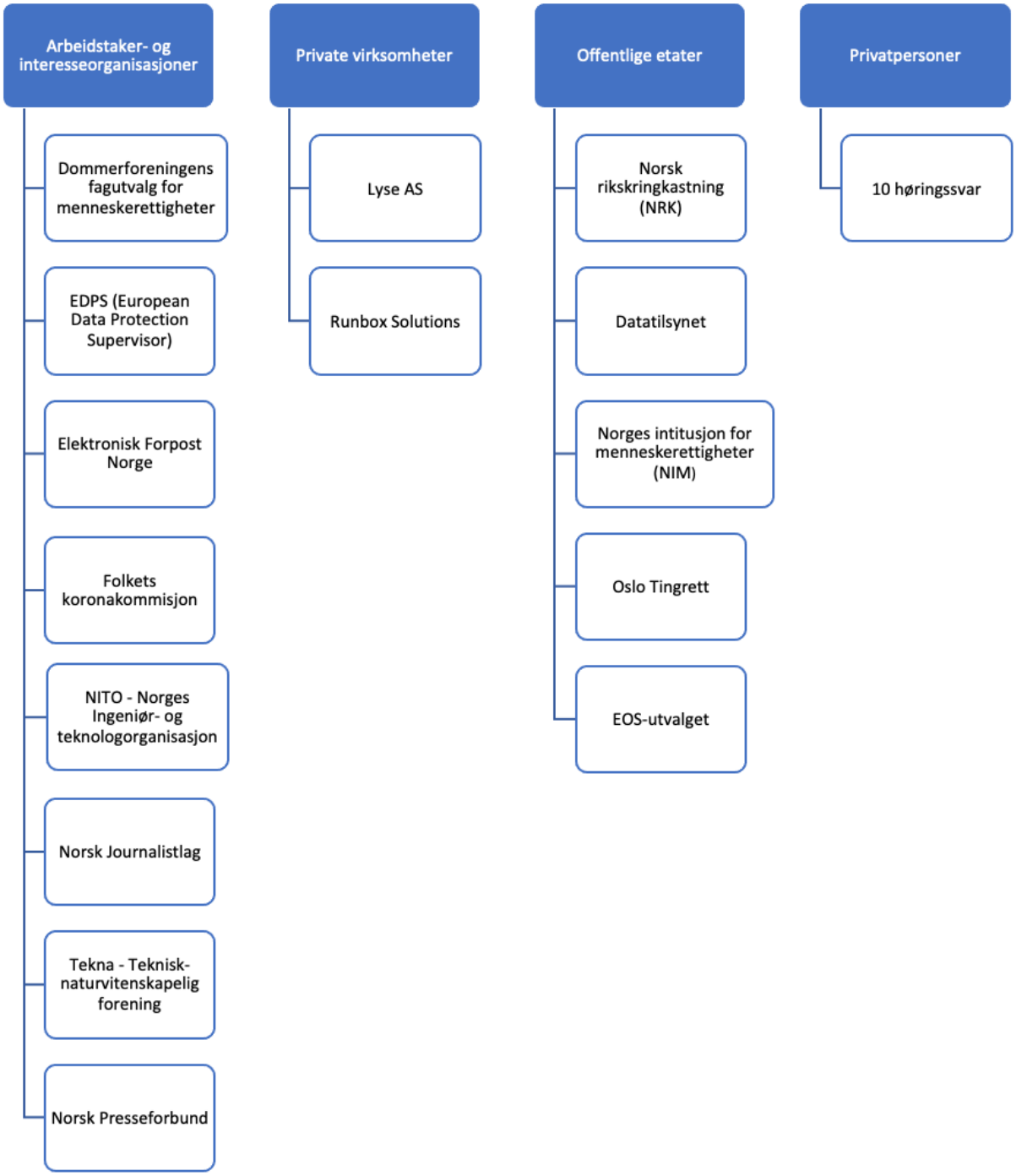
Ved gjennomgang så vi at det i flere av høringssvarene ble skrevet om momenter som gikk på den faktiske og praktiske gjennomføringen av tilrettelagt innhenting, tekniske spørsmål, dimensjonering, kunnskap, finansiering og prosess. Vi valgte å kalle denne delen av modellen for "Praktisk" ettersom meningsinnholdet handlet om det praktiske, som utførelse, gjennomføring, iverksetting og prosessuelle faktorer.

Begrunnelse for modell:

Som nevnt ovenfor gikk vi gjennom høringssvarene i fellesskap for å identifisere overordnede temaer som grunnlag for modellen. Vi gikk gjennom alle høringssvarene og identifiserte overordnede temaer som vi mener representerer meningsinnholdet på en god måte. Modellen er utarbeidet med bakgrunn i våre subjektive tolkninger og ville antakeligvis blitt inndelt og fått andre navn dersom andre skulle gjennomføre den samme øvelsen. Modellen ble revidert tre ganger før vi kom frem til den endelige versjonen. Dette fordi vi så at enkelte temaer var overlappende og forklarte det samme.

6.2 Kategorisering av høringssubjekter:

På samme måte som vi har tematisert meningsinnholdet har vi kategorisert høringssubjektene som har sendt høringssvar:



6.3 Demokratiske problemstillinger

Innenfor demokratiske problemstillinger ser vi av kodingen at det er flest individuelle høringssvar som tar opp kategorien overvåkning. Av totalt 25 høringssvar som vi har tatt med videre i analysen, har 12 av høringssvarene tatt opp overvåkning som en problemstilling. Dernest har 8 av høringssvarene tatt opp EMK § 8 og deretter 7 høringssvar som har tatt opp nedkjølende effekt. Innenfor de overordnede problemstillingene vi har identifisert, ser vi at problemstillinger som sorterer under det vi har tematisert som demokratiske, er mer fremtredende.

Arbeidstaker- og interesseorganisasjoner:

Basert på vår koding innenfor demokratiske problemstillinger ser vi at arbeidstaker- og interesseorganisasjoner reiser problemstillinger som går på nedkjølende effekt og overvåkning som de mest fremtredende.

Tekna skriver i sitt høringssvar:

> *"Tekna er opptatt av å synliggjøre risikoen for at nedkjølingseffekten inntrer idet systemet iverksettes. Vi mener det er en reell sannsynlighet for at innbyggerne begrenser sine ytringer i det digitale rom. Dette vil kunne, legge begrensninger på det offentlige ordskiftet og demokratiske prosesser, samt svekke befolkningens tillit til myndighetene. Vi er også bekymret for at e-tjenesteloven kan svekke forbrukernes tillit til norske virksomheter, siden det er norske selskaper som heretter kan pålegges å overvåke sine kunder".*

(Tekna høringssvar s. 4)

Foucault bruker fengselsformen Panoptikon som en metafor for å beskrive slik type overvåkning. I hans panoptiske beskrivelse av overvåkning vil ikke subjektene vite at de er utsatt for overvåkning, men begrenser seg selv på grunn av risikoen. Det er overførbart til det Tekna henviser til i sitt høringssvar, som beskriver en nedkjølende effekt ved at norske innbyggere

begrenser sine ytringer og kommunikasjon med bakgrunn i tilrettelagt innhenting. Dette fordi man ved å innføre tilrettelagt innhenting kan utsettes for overvåkning av Etterretningstjenesten på samme vis som Foucault beskriver sin teori. Et relevant argument mot Foucault er Macnish sitt etiske prinsipp om at overvåkning brukes til en verdig sak eller et verdig formål. Slike verdige formål beskriver han som straffbare eller skadelige konsekvenser. Det foreslåtte lovverket gir Etterretningstjenesten mulighet til å varsle om trusler mot Norge og norske interesser, og dermed i tråd med prinsipper utledet av Macnish.

Det er flere faremomenter ved å få en nedkjølende effekt i det norske samfunnet, som for eksempel lavere deltakelse i samfunnsdebatten og demokratisk deltakelse, men ettersom aktiviteten gjennomføres av en kompetent aktør med tilhørende lovhjemler som er utformet for å ta høyde for slike problemstillinger og utilsiktede konsekvenser kan det argumenteres for en slik effekt kan aksepteres. I henhold til Macnish sin teori kan en nedkjølende effekt kan vurderes å være en akseptabel konsekvens gitt den sikkerhetspolitiske situasjonen i verden. Spesielt gitt alternativet ved at man ikke klarer å identifisere trusler, som for eksempel påvirkningsaktivitet som mulig vil ha flere negative konsekvenser for demokratisk deltakelse og samfunnsdebatten i seg selv.

NITO skriver i sitt høringssvar:

> *"NITO har forståelse for at det er behov for handlingsrom og virkemidler for å ivareta Norges sikkerhet og beredskap. Samtidig er det viktig å ivareta rettssikkerheten og demokratiske verdier. Vanlige prinsipper for innsamling av elektroniske spor er at det må være skjellig grunn til mistanke før det samles inn data om mistenkte. Forslaget åpner for å registrere kommunikasjon mellom enkeltpersoner, lagre denne, for så å kunne drive etterretning og etterforskning mot egne borgere i etterkant. Det kan synes som om det dermed åpnes for masseovervåkning av borgere. Forslaget strider dermed mot ordinære demokratiske prinsipper for innsamling av elektroniske spor"*

(NITO høringssvar s. 1).

NITO beskriver en type overvåkning som rettes mot personer uten et definert mistankegrunnlag eller andre prinsipper. Marx knytter forskjellige typer overvåkning til kontekst. Der myndigheter utfører overvåkningen knytter Marx dette til tvang. For å kunne utføre slik tvangsmessig overvåkning, mener Marx at det stilles høyere krav til at slik overvåkning reguleres, som kan argumenteres for å oppfylles ved at man vedtar nye lovhjemler for Etterretningstjenesten. På en annen side beskriver Macnish diskriminering som et prinsipp innenfor jus in bello. Det må veksles mellom legitime og illegitime mål for overvåkning, som i dette tilfellet blir norske borgere som illegitime og utenlandske trusselaktører som legitime. Det er utledet fra tradisjonen om rettferdig krigføring som skiller mellom sivile og stridende, som henholdsvis illegitime og legitime mål, mener Macnish at det i en overvåkningskontekst kan skilles mellom skyldige og ikke skyldige for å definere legitime og illegitime mål. Her forstås det som det legitime målet er trusler mot Norge og norske interesser og illegitime som å overvåke norske borgere som ikke kan defineres som en trussel mot Norge og norske interesser. Det må foreligge et mistankegrunnlag for å kunne iverksette slik overvåkning. Det skal også ifølge Macnish gjøres en proporsjonalitetsvurdering i jus ad bellum (etiske regler for å kunne iverksette overvåkning), samt en proporsjonalitetsvurdering innenfor jus in bello (etiske regler for hvordan overvåkningen skal utføres). Stoddart kritiserer Macnish sin beskrivelse av diskriminering og mener det er vanskelig å skille mellom legitime og illegitime mål ved datainnsamling. Han mener også at det ikke er mulig å utføre en objektiv proporsjonalitetsvurdering innenfor en overvåkningskontekst. Stoddart mener at Macnish er for inspirert av etterforsking. I denne sammenhengen er det Etterretningstjenesten sin anledning til å bruke tilrettelagt overvåkning som diskuteres. Etterretningstjenesten har ikke hjemmel til å utføre etterforskning, men skal drive etterretningsaktivitet og utarbeide produkter som gir beslutningsstøtte.

NITO viser til at det åpnes for masseovervåkning av norske borgere. I høringssvaret deres brukes begreper som “skjellig grunn”, “mistankegrunnlag”, “elektroniske spor” og “etterforskning”. Vi mener NITO presenterer en uriktig slutning. Etterretningstjenestens innhenting skal ikke være basert på et mistankegrunnlag eller personbaserte terskler etter paralleller fra strafferetten. Det er kun politiet som har hjemmel til å etterforske etter strafferetten og benytte straffeprosessuelle midler i Norge. Videre mener vi at det legges opp til streng regulering ved at det i

etterretningstjenesteloven eksplisitt fremkommer at innsamling via tilrettelagt innhenting ikke skal tjene etterforskningsformål og kriminalitetsbekjempelse.

I forslag til ny lov er det regulert hvordan innhenting og bruk av innhentet materiale kan anvendes, samt er det anført forslag til presiseringer som går på kildeidentifiserende materiale. Det er lagt inn forslag i lovverket som skal ivareta en diskriminering og som skiller mellom legitime og illegitime mål, for eksempel innhenting som kan identifisere journalistiske kilder. Det er viktig å være bevisst at loven åpner for innsamling av store mengder data og det kan være muligheter for at data fra illegitime mål innsamles. Etter vår oppfatning kan en proporsjonalitetsvurdering av om tilrettelagt innhenting skal brukes og en proporsjonalitetsvurdering av hvordan det skal brukes, minske faren for at data fra illegitime mål innsamles.

Private virksomheter:

Basert på vår koding ser vi at private virksomheter er mest opptatt av problemstillingene som handler om EMK art. 8.

Runbox Solutions skriver i sitt høringssvar:

> *"Overvåkning kolliderer med personvernet. I henold til GDPR skal all innsamling av data som kan identifisere et datasubjekt skal være formålsbestemt. Runbox har inngått avale med sine kunder om at registrering av metadata har som formål å levere eposttjenester. Innholdet i meldinger til/fra kunder er kunde-eiendom som i prinsippet er oss uvedkommende – vi er kun en formidler som oppbevarer innholdsdata for videre forsendelse. Innsamling av metadata for etterretningsformål medfører åpenbart at denne avtalen brytes, og etjenestens eventuelle innsyn i meldingsdata (ved speiling) betyr i tillegg tilgang til potensielt sensitive personopplysninger i meldingene. Ivaretagelse av personvernet bør kreve domstolskontroll også for iverksettelse av speiling av kommunikasjonsstrømmer for testing og analyse, på samme måte som rettslig beslutning er nødvendig for speiling og søk for etteretningsformål."*

(Høringssvar Runbox Solutions s. 2)

Runbox Solutions skriver i sitt høringssvar at innholdsdata er kundens eiendom. Ved at selskaper blir pålagt å utføre speiling av kommunikasjonsstrømmer på vegne av Etterretningstjenesten ville det medføre at selskaper som Runbox Solutions bryter deres avtaler med kunder om konfidensialitet.

Etter Macnish sitt prinsipp om autoritet er det moralsk forsvarlig at andre organer, slik som private virksomheter, utfører overvåkning, men det stiller etter Macnish sin teori strenge krav til at overvåkningen er regulert av lov. Dette er også et krav i EMK art. 8. Fordi selskaper som Runbox Solutions ikke har anledning til å velge å ikke delta, er dette etter Gary Marx å anse som tvang, og derfor viktig at blir lovregulert. Dersom ansatte i eksempelvis Runbox Solutions blir pålagt noe de ikke ønsker kan man se for seg at den tekniske løsningen til Etterretningstjenesten blir nedprioritert fremfor deres egne kommersielle interesser. Stoddart på sin side mener at Macnish sine argumenter er for tett knyttet opp mot teorien om rettferdig krigføring og kan ikke knyttes til en overvåkningskontekst. Ifølge sårbarhetsprinsippet til Schartum må det alltid tas en grundig vurdering av om overvåkning skal utføres, da det er mulig at innhentet informasjon kan komme på avveie og misbrukes av uvedkommende.

Selv om Etterretningstjenesten utfører speiling og testing av kommunikasjonsstrømmer i henhold til lovverket, vil det være et brudd på EMK art. 8 dersom uvedkommende får tak i de innhentede dataene. Dette vil det være en risiko for all den tid tilbydere pålegges å gjøre om kryptert informasjon til ukryptert informasjon. På en annen side er Etterretningstjenesten sin informasjonsinnhenting skjult, og dette er en problemstilling det er rimelig å anta at det tas høyde for. Av de aktørene som lovlig utfører overvåkning på vegne av myndighetene i Norge, antas det at Etterretningstjenesten evner å gjennomføre slike tiltak med svært høy grad av operasjonssikkerhet.

Offentlig etat:

NRK skriver i sitt høringssvar:

> *"Informasjonsinnhentingen kan også rettes direkte mot nordmenn i utlandet. Dette åpner for at E-tjenesten, og andre myndigheter, kan få tilgang til kommunikasjon mellom kilder og journalister i norske mediehus."*

(NRK høringssvar s. 1)

Jamfør tidligere analyse av Tekna sitt høringssvar kan man også se dette fra et kildevernsperspektiv. Norske innbyggere kan begrense sine ytringer og kommunikasjon med journalister og mediehus, spesielt kommunikasjon med gravejournalister og annen avslørende journalistikk. Dette er relevant sett i lys av Foucaults teori om Panoptikon der befolkningen begrenser seg selv i frykt for at deres meningsinnhold kan bli overvåket. Dette kan i ytterste konsekvens få følger for medienes og pressens rolle som samfunnets "vaktbikkje" og deres arbeid i å avsløre maktmisbruk eller annet som allmennheten bør få kjennskap til. Muligheten for at Etterretningstjenesten kan få innsyn i slik informasjon og dermed en innskrenkning i kildevernet kan bidra til at terskelen for varslere eller andre med kritisk informasjon blir høyere.

Sett ut fra vårt perspektiv bør Etterretningstjenesten følge med på den digitale utviklingen og være til stede der truslene befinner seg for å kunne detektere og varsle om dem. Dette kan ha utilsiktede implikasjoner, hvor konsekvenser for kildevernet er en av dem. På en annen side må disse momentene sees opp mot sikkerheten man "kjøper" ved å ha muligheten til å avdekke, og i beste fall beskytte Norge mot trusler fra utlandet.

Oslo Tingrett skriver i sitt høringssvar:

> *"Tingretten peker også på at en nedkjølende effekt (chilling effect) også trolig vil være konsekvensen av målsøkende innhenting, jf § 5-1. I forhold til denne bestemmelsen må en nedkjølende effekt være en del av forholdsmessighetsvurderingen etter § 5-4."*

(Oslo Tingrett høringssvar s. 3.)

På samme vis som at det i rettferdig krigføring skal skilles mellom stridende og ikke stridende, skal det i et demokratisk samfunn, basert på rettssikkerhet og frihet, skilles mellom dem som overvåkning bør rette seg mot og ikke, ifølge Macnishs sitt prinsipp om diskriminering innen jus in bello. Det vil være legitimt å overvåke noen som utgjør en trussel mot Norge, men i tilfellet med tilrettelagt innhenting vil man også få informasjon om med en stor andel norske borgere som ikke utgjør en trussel. Altså vil en utilsiktet konsekvens være at flere illegitime mål blir utsatt for overvåkning som kan ha en nedkjølende effekt på samfunnet.

Vi mener verdenshistorien har vist flere tilfeller av styresett og ideologier som har medført gjennomgående overvåkning mot befolkninger fra myndighetenes side. Selv om dette bare er en hypotetisk tanke her i Norge, skal man være bevisst på historien og relevante paralleller. Fremtiden er ukjent, og hvordan det politiske klimaet i Norge kan forandre seg i fremtiden vites ikke. Det er dog viktig å påpeke at fullmakter som gis eller lover som blir vedtatt sjeldent fjernes eller oppheves, men slutter på tidspunkter å være relevante og heller utdateres.

Privatpersoner:

Basert på vår koding ser vi at privatpersoner er mest opptatt av problemstillingene som går på overvåkning og EMK art. 8 som de mest fremtredende.

Privatperson Nikolai Dragnes skriver følgende om overvåkning:

> *"DGF åpner derfor ikke bare for overvåkning av privatlivet til alle nordmen, men også for muligheten av manipulasjon og tankekontroll av hva alle nordmenn vil kunne komme til å foreta seg, gjennom kunstig intelligens og kvantedatamaskiner, det være seg av privatpersoner, økonomiske aktører eller så klart myndighetene og beslutningstakerne selv".*

(Høringssvar Nikolai Dragnes s. 3).

(DGF er en forkortelse for digitalt grenseforsvar).

Videre skriver privatperson Per Watne:

> *"Stortinget forgriper hele denne problemstillingen med dette forslaget som i beste fal bare undergrave folkets tillit til forvaltningen og Norge blir et overvåknings-samfunn for alle vet at de vil stå på lister som kan bli utpekt som lovbrudd ved en feil".*

(Høringssvar Per Watne s. 3)

Innen meningsinnhold som går på overvåkning ser vi at privatpersoner like fullt som arbeidstaker- og interesseorganisasjoner er opptatt av problemstillinger som sorterer under overvåkning, jf. tidligere drøftelse. Det er naturlig all den tid privatpersoner er opptatt å verne om sin private sfære, samtidig som arbeidstaker- og interesseorganisasjoner vil ha mange av de samme perspektivene ettersom de er opptatt av konsekvensene for sine medlemmer og interesseområder.

Privatperson Anders Lingjerde skriver om EMK art. 8:

> *"Her må dere høre på faginstanser og tekniske organisasjoner før dere godkjenner masseinnsamling av nordmenns personlige data. Skjønner godt at E-tjenesten og PST vil ha muligheten til å grave i folks privatliv, men dere trenger bare se til andre land som har prøvd lignende at det både er lite effektivt for legitim bruk og at det er nesten garantert å bli misbrukt"*

(Høringssvar Anders Lingjerde s. 1)

Det anføres at Etterretningstjenesten ønsker å bruke tilrettelagt innhenting til å grave i folks privatliv. Etter EMK artikkel 8 har privatpersoner rett til privatliv og vern om sin korrespondanse. Inngrep mot privatlivet kan kun utføres av hensyn til nasjonal sikkerhet m.m., som er en av hovedargumentene for bruk av tilrettelagt innhenting. Macnish beskriver korrekt intensjon som et etisk prinsipp. Det skal ikke ligge bakenforliggende motiver til grunn for bruk av overvåkning. Dersom Etterretningstjenesten skulle "gravd" i folks privatliv ville det vært en annen intensjon enn det som ligger til grunn i lovverket. Stoddart på sin side stiller spørsmål ved om det finnes noe som korrekt intensjon og at det ofte kan foreligge enkelte andre bakenforliggende motiver for å utføre overvåkning. Dette argumentet resonnerer godt med høringssvaret til Anders Lingjerde. Til tross for at innhentingen er lovregulert, beskriver Schartum i sitt sårbarhetsprinsipp at informasjonen som innhentes kan også tilfalle uvedkommende, og i verste fall misbrukes av fremmede stater.

Lingjerde mener at det bør sees til andre lands erfaringer med samme type overvåkning og at det er "nesten garantert" å bli misbrukt. Etter forrige høringsrunde har Forsvarsdepartementet lagt til grunn to dommer fra Den europeiske menneskerettighetsdomstolen, nettopp for å være i tråd med gjeldende rettspraksis, og implementerer dette i det nye forslaget som her omtales. Det fremstår som at intensjonen er å forbedre loven ved å legge til grunn erfaringer fra andre land og rettspraksis. Det taler imot argumentet til Lingjerde. Den tilrettelagte innhentingen er strengt lovregulert og formålsstyrt. Det fremgår blant annet i forarbeidene og loven at tilrettelagt

innhenting ikke skal brukes til kriminalitetsbekjempelse eller å forebygge kriminalitet. Det er likevel problematisert i flere høringssvar at tilrettelagt innhenting potensielt kan fange opp kommunikasjon som utføres av norske borgere i Norge. I et slikt tilfelle kan Etterretningstjenesten i prinsippet være i stand til å få innblikk i norske borgere sitt privatliv dersom de velger å omgå lovverket og analysere dataene om norske borgere som ikke utgjør en trussel. Det er vanskelig å se at Etterretningstjenesten skal kunne ha et utbytte av det, i tillegg til at misbruk vil kunne bli oppdaget, da tilrettelagt innhenting er underlagt kontroll av EOS-utvalget og bruk av metoden besluttes av en domstol. Når det kommer til korrekt intensjon er det mulig at intensjonen endrer seg over tid og man kan få en formålsglidning. Den nye etterretningstjenesteloven er omfattende og består av over 20 lovtekniske sider og har som formål å presist beskrive og å begrense Etterretningstjenestens mulighet til å bruke tilrettelagt innhenting utover det som eksplisitt beskrives. Det kan etter vår vurdering fremstå som at Lingjerde har en noe lav tillit til norske myndigheter, noe som kan være medvirkende for hans syn.

Oppsummering demokratiske problemstillinger:

Oppsummert for kategorien "demokratiske argumenter" ser vi at den største andelen av høringssvarene i hele høringsprosessen sorteres under denne hovedkategorien.

Den mest fremtredende problemstillingen blant privatpersoner er overvåkning, og høringssvarene fra denne gruppen har meningsinnhold som indikerer at flere av dem har lav tillit til norske myndigheter som utgangspunkt. På en annen side er det kun 14 privatpersoner som har valgt å sende inn høringssvar. Offentlige etater på sin side har kildevern som problemstillingen som den mest fremtredende. NRK tar opp dette, som en virksomhet som i stor grad har ansatte med journalistisk bakgrunn, som kan årsaksforklare hvorfor NRK i stor grad fokuserer på dette.
For private virksomheter er de mest fremtredende problemstillingene relatert til EMK art. 8. Det ligger kun to virksomheter til grunn i datamaterialet. Arbeidstaker- og interesseorganisasjoner har definert nedkjølende effekt og overvåkning som de to største problemstillingene.

På tvers ser vi at alle grupperinger, privatpersoner, private virksomheter, arbeidstaker- og interesseorganisasjoner og offentlige etater har en klar trend om at de problematiserer EMK art. 8.

Innenfor de demokratiske problemstillingene ser vi at høringssvarene treffer det teoretiske rammeverket gjennom Foucaults teori om panoptisk overvåkning, herunder problemstillingene som går på nedkjølende effekt og svekket kildevern. Andre problemstillinger treffer Macnish sine prinsipper om en verdig sak og formål, diskriminering, korrekt intensjon og autoritet.

6.4 Juridiske problemstillinger

Innenfor juridiske problemstillinger ser vi av kodingen at det er flest individuelle høringssvar som tar opp kategorien domstolskontroll. Av totalt 25 høringssvar som vi har tatt med videre har 9 av høringssvarene tatt opp domstolskontroll. 8 høringssvar tar opp lovtekniske problemstillinger, 6 høringssvar tar opp rettssikkerhet og 3 formålsglidning.

Arbeidstaker- og interesseorganisasjoner:

Basert på vår koding innenfor juridiske problemstillinger ser vi at arbeidstaker- og interesseorganisasjoner har lovtekniske problemstillinger som den mest fremtredende, etterfulgt av domstolskontroll.

De lovtekniske problemstillingene handler i hovedsak om at høringsinstansene mener at lovteksten som er foreslått er upresis og at den gir rom for tolkninger i et videre begrep, som i ytterste konsekvens kan gi Etterretningstjenesten et større handlingsrom enn det som var lovgivers intensjon eller andre utilsiktede konsekvenser.

Dommerforeningens menneskerettighetsutvalg skriver i sitt høringssvar:

> *"Vi nevner også at forslaget til § 7-2 tredje ledd synes å ha fått en uheldig lovteknisk utforming. Vi peker her på at forslaget til bestemmelse gir uttrykk for to forholdsmessighetsvurderinger, både i bokstav b og bokstav c, der sammenhengen mellom dem framstår som noe uklar."*

(Dommerforeningens menneskerettighetsutvalg s. 3)

Intensjon med overvåkning er viktig, og med uklar lovtekst kan man benytte overvåkningen utover det som var lovgivers intensjon. Macnish sitt prinsipp om korrekt intensjon gjør seg gjeldende i ovennevnte tilfelle. I dette tilfellet er det problematisert at man kan vurdere forholdsmessigheten på to ulike måter og sånn sett kan det gi inntrykk av en noe uklar intensjon. Stoddart mener at det ikke finnes noe som heter korrekt intensjon og at det alltid vil være bakenforliggende intensjoner som ligger til grunn.

Dersom det verserer uklarheter i hva lovgiver sin intensjon er, kan det føre til uheldige fortolkninger og et tilsynelatende større lovmessig rom enn det som har vært lovgivers opprinnelige intensjon. Det kan føre til uklare og inkonsistente forholdsmessighetsvurderinger som i verste fall kan bidra til narrativet om at utøvende ledd, som i dette tilfellet Etterretningstjenesten har andre, eller bakenforliggende motiver. Uklarheter i hvordan loven er utformet, kan gi et inntrykk av at Etterretningstjenesten får et større rom til å argumentere for forholdsmessighet i beslutning om å speile kommunikasjonsstrømmer. På en annen side ville rettspraksis etter hvert bidra til forståelse for hvordan forholdsmessigheten skulle fortolkes.

<u>Privat virksomhet:</u>

Basert på vår koding ser vi at private virksomheter er opptatt av domstolskontroll som den største problemstillingen.

Lyse AS skriver i sitt høringssvar:

> *"Lyse AS mener alle beslutninger om tilgang til innhentede data skal gjøres av domstolen. Videre er det avgjørende at ordlyden i reguleringen bidrar til at det ikke foreligger noen tvil om, eller rom for tolkning av, hvem som besitter den myndigheten. Det er et selvstendig poeng at denne reguleringen også vil bli lest og tolket av legfolk, ikke-statlige organisasjoner, journalister med flere, og det er viktig at reguleringen i seg selv er så tydelig at den bidrar til å opprettholde den nødvendige tilliten."*

(Lyse AS høringssvar s. 2)

Lyse AS problematiserer behovet for domstolskontroll for å opprettholde tillit. Marx beskriver noe av dette i sin teori der han deler overvåkning inn i utførelse og kontekst. De forskjellige kontekstene har forskjellige forventninger til hvordan overvåkning skal gjennomføres, for eksempel gjennom lovregulering, slik som Etterretningstjenesteloven. I dette tilfellet skal overvåkingen utføres av myndighetene, som Marx mener er en tvangsmessig kontekst.

Schartum på sin side argumenterer for at dersom man skal kunne bruke informasjon fra tilrettelagt innhenting må det en viss menneskelig gjennomgang til for å kunne gjennomføre den. Ved menneskelig gjennomgang og ikke maskinell, er faren for at lover og regler enten blir overtrådt eller ignorert til stede. Disse faremomentene kan reduseres ved domstolskontroll. Dette er i tråd med det Lyse AS argumenter for, ved at lovverket skal tolkes av lekfolk og ikke utøvende ledd før igangsettelse.

Schartum har utarbeidet en matrise for å si noe om alvorligheten av overvåkning. Dersom man ser kommunikasjonsstrømmene som Etterretningstjenesten vil gis tilgang til opp mot Schartums matrise vil det tilsvare alvorlighetsgrad 4, på en skala som går fra 1-8. Dette fordi mulig identifiserbar informasjon trolig vil måtte behandles av et menneske for å utarbeide etterretningsprodukter.

Domstolskontroll er et tema som har blitt problematisert i flere høringssvar og ble i denne prosessen innført som en endring av loven som ble innført i 2020. Det er tatt grep for å opprettholde tilliten som Lyse AS viser til gjennom å flytte beslutningsmyndighet fra Sjef Etterretningstjenesten til Oslo tingrett. Ifølge Schartum kan overvåkningens alvorlighetsgrad aksepteres ved lovregulering og domstolskontroll, som det her foreslås. På en annen side krever slik domstolskontroll god innsikt i Etterretningstjenesten sitt mandat og kunnskaper om den tekniske utførelsen, samt mulighetsrommet innenfor bruken av denne overvåkningsmetoden. Det kan reises spørsmål om ansatte i norske domstoler innehar kombinasjonen av teknisk innsikt, forståelse for rekkevidden og mulighetsrommet innhentingskapasiteten representerer i tillegg til den juridiske og lovmessige kompetansen.

Offentlige etater:

Basert på vår koding ser vi at offentlige virksomheter er mest opptatt av domstolskontroll som temaet med flest kodinger, dernest rettssikkerhet. For å skape en større bredde i analysen velger vi å analysere rettssikkerhet da vi tidligere har analysert domstolskontroll under privat virksomhet.

Datatilsynet skriver i sitt høringssvar:

> *"Slik Datatilsynet forstår forslaget, så vil ikke rettens beslutning innebære noe mer enn at det foretas en utvelgelse av allerede innhentede kommunikasjonsstrømmer til å danne grunnlag søk og innhenting etter § 7-8 og 7-9. Merk at i Big Brother Watch så skal den uavhengige forhåndskontrollen iverksettes før innhenting. I dette forslaget vil domstolskontrollen kunne foretas så sent som 18 måneder etter at opplysningene er innhentet."*

(Høringssvar Datatilsynet s. 7)

Høringssvaret kritiserer at det er svak domstolskontroll ettersom Etterretningstjenesten ikke må gå til retten med de innhentede kommunikasjonsstrømmene før 18 mnd. etter innhenting. Etter

Macnish sitt nødvendighetsprinsipp bør overvåkning kun gjennomføres dersom det som er absolutt nødvendig for å oppnå formålet og at mindre inngripende metoder først er forsøkt.

Med dagens ordning kan det fremstå som at det er lavere terskel for å iverksette speiling av kommunikasjonsstrømmer, fremfor å benytte seg av mindre inngripende metoder. Det er dog usikkert om det finnes mindre inngripende alternativer. I tilfellet er det mulig å speile en kommunikasjonsstrøm hvor legalitetskontrollen først gjøres i etterkant av domstolen. Ved at legalitetskontrollen gjøres så lang tid i etterkant av faktisk innhenting kan det stilles spørsmål om nødvendighetsvurderingen er utført i tilstrekkelig grad. Ved tidsriktig domstolskontroll kan utvalget gjøres i forkant, og unødvendig overvåkning kan unngås. På en annen side kan Etterretningstjenesten ha informasjon om trusler mot Norge der det ved opphold er fare for at sentral innhenting kan gå tapt. Dette er imidlertid en risiko lovgiver skal ta stilling til.

Det er viktig å stille kritiske spørsmål ved nødvendigheten av all form for overvåkning av privat korrespondanse m.m. og må hele tiden veies opp mot formålet med innhentingen og hva det skal brukes til. Det er uklart om Etterretningstjenesten har alternativer som kan brukes fremfor speiling av kommunikasjonsstrømmer til å avdekke de samme truslene, men Lysne-II utvalget avkrefter langt på vei at det finnes fullgode alternativer. Dette er sikkerhetsgradert informasjon, og ingen sikkerhets- eller etterretningstjeneste vil ønske å eksponere sine kapasiteter. Selv om kommunikasjonsstrømmene lagres i lengre tid med etterfølgende kontroll, vil det fortsatt være begrensninger på bruk av denne type data.

Privatpersoner:

Basert på vår koding ser vi at privatpersoner er opptatt av formålsglidning. Blant privatpersoner er det bare en person som har uttrykt seg om dette som en problemstilling innen den juridiske kategorien.

Privatperson Henning Norli Andersen skriver i sitt høringssvar:

> *"Dette blir fort en av mange små endringer som sakte åpner opp samfunnet for mer overvåkning, og skjer dette sakte nok merker man det kanskje ikke før det er "for seint"."*

(Høringssvar, Henning Norli Andersen s. 1)

Gary Marx skriver at terrorangrepet på World Trade Center i 2001, er en av de hendelsene som i størst grad har påvirket lovverket og utøvelsen av overvåkning i den vestlige verden i moderne tid.

Andersen argumenterer i sitt høringssvar for at små endringer over tid kan føre til en formålsglidning. Det er av Etterretningstjenesten uttrykt et behov for utvidede lovhjemler for å utføre tilrettelagt innhenting, men dersom trusselbildet endrer seg kan det problematiseres om hvorvidt metoden fortsatt vil brukes eller at eksisterende lovverk tilpasses eller utvides for å brukes til andre formål, eventuelt om bruken av tilrettelagt innhenting reduseres dersom verden skulle bli mer harmonisk og trusselbildet redusert.

Oppsummering juridiske problemstillinger:

Oppsummert for kategorien "juridiske problemstillinger" ser vi at offentlige etater og arbeidstaker- og interesseorganisasjoner er de som har avgitt flest høringssvar som vi har kodet til å være juridiske problemstillinger. Private virksomheter og privatpersoner har gitt henholdsvis 2 og 1 svar innen denne kategorien. Det er vanskelig å si noe om trender innenfor private virksomheter ettersom det er et lite antall høringssvar.

Lovtekniske problemstillinger er kodingen som er mest fremtredende innenfor hele kategorien av juridiske problemstillinger. Mulige forklaringer på dette er at det kan være flere med utdanning innen jus som vil se høringsnotatet fra et juridisk ståsted og svare basert på dette. Basert på egen erfaring fra arbeidslivet er vi kjent med at det ofte er de juridiske avdelingene i offentlige virksomheter som skriver og utarbeider høringssvar. Det samme vil gjøre seg gjeldende for

arbeidstaker- og interesseorganisasjoner som ofte har jurister som en del av sin stab, men også fordi interesser og rettigheter er nært forbundet med utarbeidelse av lovverk og juridiske spørsmål. Videre vil det være vanskelig for både enkeltpersoner og organisasjoner uten juridisk bakgrunn eller kompetanse å kommentere eller ha innsigelser av en lovteknisk karakter. Endelig handler denne prosessen om utformingen av en ny lov, og det er naturlig at lovtekniske problemstillinger vies oppmerksomhet.

Innenfor de juridiske problemstillingene ser vi at høringssvarene treffer det teoretiske rammeverket i form av Macnish sine prinsipper om nødvendighet og riktig intensjon. Videre gjennom Schartums poengmatrise og Marx teori om kontekst.

6.5 Praktiske problemstillinger

Innenfor praktiske problemstillinger ser vi av kodingen at det er flest individuelle høringssvar som tar opp kategorien økonomi, drift og ressurser. Av totalt 25 høringssvar er det 8 som tar opp denne problemstillingen. 7 høringssvar tar opp problemstillinger knyttet til prosess og 6 tar opp tekniske problemstillinger.

Arbeidstaker- interesseorganisasjoner:

Tekna skriver i sitt høringssvar:

> *"Tekna vil også påpeke at innsamling og lagring av store datamengder i seg selv innebærer en forhøyet sikkerhetsrisiko. Det vil introduseres nye sårbarheter hos e-komleverandørene som må tilrettelegge for ukryptert innhenting av informasjon, i datatrafikken fra e-komleverandørene til etterretningstjenesten, og i etterretningstjenestens datalagre. Flere aktører vil være interessert i denne informasjonen. Via hacking eller fysisk tilgang kan informasjon komme på avveie, bli misbrukt eller manipulert ved eksempelvis å skape en feilaktig situasjonsforståelse."*

(Tekna høringssvar s. 5)

Tekna bekymrer seg for at tilrettelagt innhenting vil medføre nye sårbarheter hos e-komleverandørene som pålegges å speile kommunikasjonsstrømmer på vegne av Etterretningstjenesten, som per i dag er kryptert. Bakgrunnen for kryptering er sikkerhetsmessige og personvernmessige årsaker, dette for å kunne beskytte informasjonens konfidensialitet. Dersom tilrettelagt innhenting innføres vil e-komleverandørene pålegges å levere fra seg kommunikasjonsstrømmene i et ukryptert format, som i seg selv med medføre en sårbarhet og sikkerhetsrisiko. Det er den forbindelse relevant å ta inn tidligere drøftelse om Schartum sitt sårbarhetsprinsipp, som sier noe om varsomheten som bør utvises da det er risiko for at informasjonen kan tilfalle uvedkommende. På en annen side må man kunne anta at Etterretningstjenesten vil utforme den tekniske løsningen på en slik måte som gjør at den vil tilfredsstille kravene i Sikkerhetsloven, all den tid Etterretningstjenesten er underlagt Sikkerhetsloven. Når det kommer til risikoen de private virksomhetene vil løpe som mulige mål for fremmed etterretning sine etterretningsoperasjoner kan det tenkes for at denne vil bli høyst reell ved innføring av tilrettelagt innhenting. Tilrettelagt innhenting vil utgjøre en ny kapasitet for Etterretningstjenesten, og etterretningsorganisasjonene sine kapasiteter er høyaktuelle mål i en etterretningskontekst.

I en tid med krig i Europa er vi godt kjent med at cyberangrep og hacking er hyppig brukte virkemidler. Norge ansees som en fiendtlig stat av russiske myndigheter, blant annet på bakgrunn av vår støtte til Ukraina (TV2, 2022). Som følge av at Norge tilhører det kollektive Vesten og NATO, samt at Norge er et av Russlands naboland, må man anta at personopplysninger om nordmenn, og spesielt myndighetspersoner er interessant å innhente i etterretningsøyemed. Tekna sin problematisering illustrerer noe av dette. På en annen side må det tas høyde for at denne risikoen er akseptabel veiet opp mot risikoen man løper ved ikke å innføre muligheter for speiling av kommunikasjonsstrømmer.

Offentlige etater:

Datatilsynet skriver i sitt høringssvar:

> *"Datatilsynet mener det er svært uheldig at deler av et regelverk som er på høring gjøres gjeldende før høringsfristen har gått ut og faginstansene har blitt hørt. Høringen retter seg direkte mot lovens § 7-3 og spørsmålet om bestemmelsen er i tråd med menneskerettighetene, noe som ikke er drøftet før ikrafttredelsen av ovennevnte bestemmelse. Dette svekker tilliten til høringsprosessen."*

(Datatilsynet høringssvar s. 10)

Macnish beskriver proporsjonalitet i jus ad bellum som et vurderingskriterium for om overvåkning kan innføres. Datatilsynet problematiserer at et regelverk gjøres gjeldende før det har vært gjennom en demokratisk prosess, herunder at høringsinstansene og andre relevante aktører har fått mulighet til å komme med innspill eller innsigelser i forkant av iverksetting. Det kan argumenteres for at det er uproporsjonalt å iverksette et lovverk før alle innspill er drøftet og vurdert. Stoddart på sin side mener at det mangler klare definisjoner på hva proporsjonalitet består av hvordan det skal vurderes, spesielt i en overvåkningskontekst.

Videre problematiserer Datatilsynet at de menneskerettslige perspektivene ikke er drøftet før iverksettelse. Slike vurderinger ville sagt noe om proporsjonaliteten ved tilrettelagt innhenting, og hadde slike innspill blitt lagt til grunn, er det muligheter for at lovverket ville vært utformet annerledes. Det er menneskerettighetsrelaterte argumenter fra kjennelsene i EMD som er lagt til grunn for endringene som har vært med i denne høringsprosessen. Vurderingene fra disse kjennelsene er dermed ikke tatt inn i vurderingen av om aktiviteten i seg selv er forholdsmessig før man begynner testing. Det finnes ingen åpenbare grunner til at disse vurderingene ikke burde være gjeldende for begge typer innhenting, både test-innhenting og faktisk innhenting. Et annet prinsipp som omtales av Macnish er prinsippet om intensjon. Dersom intensjonen med overvåkningen er at det skal skje i overensstemmelse med europeiske lover, spesielt menneskerettighetene, er det bemerkelsesverdig at loven i sin helhet (med unntak av

etterretningstjenesteloven § 7-3) iverksettes før alle høringsprosessene er ferdig og loven er vedtatt. Dette kan gi grobunn for tanker om at det har vært en intensjon om å innføre lovverket uten å ta høyde for menneskerettslige perspektiver.

Privat virksomhet:

Runbox Solutions skriver i sitt høringssvar:

> *"Når e-tjenesten installerer utstyr for speiling, vil dette iht. § 7-4 taushetsbelegges. Vi kan da ikke møte kundeklager, oppsigelser av abonnementer og svekket renommé med rapportering om årsak til driftsforstyrrelser. Statusrapportering og årsaksforklaringer virker normalt avbøtende, noe vi må avstå fra ved tilrettelagt innhenting.*
> *I tillegg vil tilrettelegging belaste organisasjonen (ref. § 7-2) som blir tvunget til å nedprioritere egne vedlikeholds- og utviklingsprosjekter – i tillegg til å håndtere økt mengde kundeklager. Tilrettelagt innhenting fremstår som et særdeles invaderende tiltak med potensielt store negative konsekvenser for tjenesteleverandører."*

(Runbox Solutions høringssvar s. 1-2).

Macnish sitt prinsipp om at overvåkning må gjennomføres av riktig autoritet er relevant i denne sammenhengen. I tilfellet med tilrettelagt overvåkning vil staten ved Etterretningstjenesten pålegge private virksomheter å installere og drifte speilingsutstyr, og på den måten ta del i overvåkningen av befolkningen. Macnish argumenterer for at andre enn staten kan drive overvåkning eller bistå til dette, men i slike tilfeller er det viktig at det er lovregulert. Macnish sitt argument vil i så måte gjøre seg gjeldende. På en annen side mener Stoddart at Macnish i for stor grad lar seg inspirere av rettferdig krigføring, og mener at autoritetsprinsippet ikke lar seg overføre til en overvåkningskontekst.

Det er mulig vi snart står i en situasjon hvor kommersielle aktører vil bli bedt om å speile trafikk på vegne av Etterretningstjenesten. Den praktiske gjennomføringen vil ikke kunne bekjentgjøres kunder eller andre interessenter grunnet lovregulert taushetsplikt. Macnish sitt prinsipp om at

overvåkning må erklæres, blir her relevant. Den kommersielle aktøren vil ikke kunne etterleve dette prinsippet i form av å opplyse sine kunder om overvåkningen de risikerer å utsettes for dersom de benytter deres tjenester, noe som kan bidra til mistillit.

Stoddart på sin side argumenterer for at intensjonsforklaringen, som er viktig i erklæringen av krig ikke gjør seg gjeldende når det kommer til overvåkning. Dette fordi at man ikke kan forvente at befolkningen vil samtykke, da overvåkningen vil gjøres i skjul, et uhåndterbart antall mennesker vil utsettes for det, og det vil være vanskelig å kunne sortere dersom det fantes en reell mulighet for å samtykke. På denne måten kan man si at Stoddarts argumentasjon er relevant for denne dimensjonen av tilrettelagt innhenting.

Innenfor Jus ad Bellum beskriver Macnish proporsjonalitetsvurderingen som et vurderingskriterium. Det vil si at tiltaket som brukes må stå i proporsjon til det det skal beskytte mot. Tilrettelagt innhenting problematiseres som et inngripende virkemiddel som vil medføre store merkostnader for involverte virksomheter i form av drift og tjenestebrudd som følge av speiling av informasjon fra deres kommunikasjonsstrømmer. Dette som ledd i den tilrettelagte innhentingen. Stoddart mener at det ikke finnes en klar definisjon på hvordan man kan utføre en proporsjonalitetsvurdering og hvordan den skal brukes.

Runbox Solutions er en kommersiell aktør som er avhengig av å selge sine tjenester og opprettholde et godt forhold til sine kunder. Det er naturlig at Runbox Solutions og tilsvarende selskaper vil ha motforestillinger til å bli pålagt endringer som vil kunne påvirke tillitsforholdet til kundene og ha driftsmessige konsekvenser. Den pålagte speilingsaktiviteten er en stor inngripen mot private selskapers sine kunder som er uvitende om at de blir overvåket av Etterretningstjenesten. Videre kan det også argumenteres for at de private virksomhetene også blir utsatt for en inngripen de ikke kan motsette seg. Samtidig kan det argumenteres for at slike tiltak er proporsjonale sett opp mot farene som er forbundet ved ikke å gi Etterretningstjenesten anledning til å utføre tilrettelagt innhentning, dette med referanse til trusselbildet.

Til forskjell fra Etterretningstjenesten er private selskaper drevet av kommersielle interesser. Det kan også argumenteres for at det utgjør en sikkerhetsrisiko å etablere statlig overvåkningsutstyr

hos kommersielle aktører som ikke er underlagt Sikkerhetsloven. Det kan tenkes at ansatte kan ta snarveier eller ikke har den samme evnen til å etterleve regelverk, samtidig som det kan være vanskelig å kontrollere om dette blir gjort. På en annen side kan dette handle om sikkerhetskultur, motivasjon og andre faktorer som ligger utenfor denne oppgaven å beskrive ytterligere.

Privatpersoner:

Odd Oskarsen skriver i sitt høringssvar:

> *"Nå foregår det en massiv testing av etterretningsvertøyet, og det før loven eventuelt er vedtatt. Her utviser statsråden og departementet en heller tvilsom holdning til demokratiet. Denne høringen fremstår dermed som en reell skinnprosess."*

(Odd Oskarsens høringssvar s. 1)

Innenfor temaet praktiske problemstillinger har vi kun kodet tre underkategorier. Det er fire høringsgrupper og derfor gjentas problemstillingen "prosess" igjen. Vi ønsker å vise til at denne problemstillingen også opptar privatpersoner. Det er den samme argumentasjonen som Datatilsynet la til grunn som vi har drøftet over. Vi viser derfor til ovennevnte drøftelse.

Oppsummering praktiske problemstillinger:

Arbeidstaker- og interesseorganisasjoner er mest opptatt av problemstillinger som går på økonomi, drift og ressurssetting. Ettersom deres oppgave er å fremme interessene til deres arbeidstakere og organisasjoner, er det naturlig at disse vil ha motforestillinger mot å pålegge dem ekstra oppgaver og ansvar som kan medføre risiko, videre fordi det vil påvirke både bedriftens og de ansattes ressurser. Det samme gjør seg gjeldende overfor private virksomheter, selv om det bare er to private virksomheter som har sendt inn høringssvar.

På tvers av alle kodinger er problemstillinger som går på økonomi, drift og ressurssetting den problemstillingen som opptar alle kategoriene av høringsinstanser på tvers. Det nest mest problematiske området er prosess.

Innenfor de praktiske problemstillingene ser vi at høringssvarene treffer det teoretiske rammeverket i form av Macnish sine prinsipper om autoritet, riktig intensjon, erklæring av overvåkning og proporsjonalitet. Videre treffer det Stoddarts kritikk mot Macnish sitt prinsipp om at overvåkning må erklæres.

7. Konklusjon

I denne oppgaven har vi ønsket å besvare problemstillingen "Hva oppfattes som de største problemstillingene ved tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon i Etterretningstjenesteloven?". Vi har strukturert oppgaven på en slik måte at vi har forsøkt å gi leserne et innblikk i de mer generelle trekkene, for så å gå mer spesifikt inn på detaljer. Ettersom vi ønsket å finne ut hva som oppleves som de største problemstillingene ved tilrettelagt innhenting har vi valgt å bruke overvåkningsteori i analysen. Vår hovedteori omhandler etiske prinsipper for implementering av overvåkning. Vi har også valgt teori som argumenterer mot vår hovedteori, da vi ønsket en drøfting som skulle fremheve forskjellige perspektiv, uten å låse oss fast i én teoretikers synspunkter.

Gjennom en kvalitativ analyse har vi fokusert på å identifisere problemstillinger, der vi har gått i dybden på enkelte av dem. Etter å ha analysert vårt uttrekk fra høringssvarene mener vi at vi har identifisert en rekke problemstillinger ved innføring av tilrettelagt innhenting. Selv om problemstillingene ikke kan sies å kunne generaliseres til den øvrige populasjonen, så mener vi likevel at gir en god dybdeinnsikt i de enkelte problemstillingene, sett i lys av overvåkningsteori. Vi valgte å tematisere de forskjellige problemstillingene, samt å dele opp høringssvarene i høringskategorier. På den måten har vi ønsket å gi leseren et innblikk i trender innenfor de forskjellige kategoriene, men også trender hos de forskjellige høringssubjektene.

Ved å se på antall kodinger innenfor de forskjellige kategoriene av høringssubjekter definert i modellen har vi funnet følgende:

Arbeidstaker- og interesseorganisasjoner i høy grad er opptatt av lovtekniske problemstillinger, samt problemstillinger som går på økonomi, drift og ressurssetting. Denne gruppen har kodinger innenfor alle undertemaene, noe som vil si at høringssvarene fra denne gruppen treffer bredden i problemstillingene som ble definert i modellen.

5 av høringssubjektene innenfor denne gruppen er arbeidstakerforening, som består av folk med både journalistisk og juridisk bakgrunn. Det er naturlig at jurister vil være opptatt av juridiske problemstillinger, på lik linje som at journalister vil være opptatt av hvordan kildevernet problematiseres rent juridisk da det er avgjørende for deres virksomhet. De to

interesseorganisasjonene er organisasjoner som engasjerer seg i personvern og juridiske spørsmål knyttet til digitale og elektroniske problemstillinger, og det vurderes som naturlig at disse vil ha innspill til en høringsprosess som denne.

Videre ser vi at offentlige etater er mest opptatt av lovtekniske problemstillinger som den største andelen og domstolskontroll som den nest største. 1 av 5 høringssubjekter i denne kategorien er offentlige etater som antas å ha sterk juridisk kompetanse, og som et av organisasjonens fremste formål er å tolke og vurdere lovverk, samt drive kontrollvirksomhet i forhold til overholdelse av regelverk. Disse instansene vil naturlig kunne identifisere problematiske sider ved hvordan lovtekst er utformet og ha evne til å forskuttere og identifisere potensielle implikasjoner ved uklar lovformulering. Det ene høringssubjektet innen kategorien offentlige instanser som ikke er å anse som en juridisk organisasjon i er høringssvaret signert av lederen for organisasjonens juridiske avdeling.

Private virksomheter har økonomi, drift og ressurssetting som en hovedproblemstilling, og denne er problematisert like mye som domstolskontroll. Det skal påpekes at det bare er to høringssubjekter innenfor denne kategorien som har skrevet høringssvar, noe som sannsynligvis påvirker mangelen på bredde. Det er naturlig at private virksomheter som vil pålegges å installere speilingsutstyr i sin virksomhet vil problematisere dette, da det oppleves som at det vil ha konsekvenser for deres kommersielle virksomhet og drift.

Privatpersoner har overvåkning som sin største problemstilling i tillegg til EMK art. 8. Det er naturlig at ingen privatpersoner ønsker å bli overvåket og at de ønsker at retten til privatliv skal opprettholdes slik det er i dag. Dog er det meningsinnhold i høringssvarene og formuleringer som indikerer at flere av dem som har sendt inn høringssvar har lav tillit til norske myndigheter som utgangspunkt.

Overordnet ser vi at problemstillingene som trekkes frem i høringssvarene i stort treffer det teoretiske rammeverket, og dermed Macnish sine etiske prinsipper. Det samme gjør seg gjeldende når det kommer til Stoddarts motargumenter til Macnish sine prinsipper, da disse gjerne er to sider av samme sak. Foucaults teori om panoptisk overvåkning gjør seg relevant for flere problemstillinger som trekkes frem, spesielt når det kommer til kildevern og nedkjølende

effekt. Schartums sårbarhetsteori og poengmatrise, samt Marx teori om overvåkningens kontekst er relevant for flere av høringssvarene, men andre deler av rammeverket vurderes som mer relevant. De mest relevante er etter vår analyse og vurdering Macnish, Stoddart og Foucault.

På tvers av alle kategoriene er det flest høringssvar som har kodinger som viser at de er opptatt av problemstillingen overvåkning og domstolskontroll, uavhengig av type høringssubjekt. Det kan gjennom kodingen antas at blant alle problemområder tilknyttet tilrettelagt innhenting er overvåkning av befolkningen, samt svak eller mangelfull domstolskontroll det som oppleves som det mest problematiske.

I en tid med endringer i trusselbildet og stadig nye digitale utfordringer har sikkerhet- og etterretningsorganisasjonene behov for nye verktøy og innhentingsmetoder. Vi mener at vår studie har overføringsverdi til en annen lignende og dagsaktuell problemstilling. Endringene i Politiregisterloven gir PST adgang til behandling av åpent tilgjengelig informasjon til etterretningsformål, som i praksis gir dem mulighet til å lagre store mengder informasjon fra Internett til etterretningsformål. Vi mener at vår studie om tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon har overføringsverdi til PSTs nye adgang da vi mener at både fremgangsmåten og teoriene vi har lagt til grunn i vår oppgave er relevante. Dette da PSTs adgang kan problematiseres på samme måte ved at de samme personvernmessige og etiske dilemmaene gjør seg gjeldende. Vi mener det er rimelig å anta at sikkerhets- og etterretningsorganisasjonene i takt med digital utvikling vil få nye behov for innhentingskapasiteter og lovendringer i fremtiden, og at fremgangsmåten vist i denne studien kan være relevant for å identifisere og forstå utfordringene.

8. Litteraturliste

Accenture iDefense. (2014). BlackEnergy & Quedagh: *The convergence of crimeware and ATP attacks*. Hentet fra https://blog-assets.f-secure.com/wp-content/uploads/2019/10/15163408/BlackEnergy_Quedagh.pdf

Andrew, C., Aldrich, R. J. & Wark, W. K. (2009). *Secret Intelligence - A reader.* Routledge

Asdal, K. og Reinertsen, H. (2020). *Hvordan gjøre dokumentanalyse - en praksisorientert metode.* Cappelen Damm

Born, H. & Wetzling, T. (2007). *Intelligence accountability: challenges for parliaments and intelligence services.* I Handbook of Intelligence studies, Johnson, L., K. (red). New York: Routledge

Braun, V. & Clarke, V. (2006). *Using thematic analysis in psychology*. Qualitative Research in Psychology, 3:2, 77-101, DOI: 10.1191/1478088706qp063oa

Bryman, A., Clark, T., Foster, L., & Sloan, L. (2021). *Social Research Methods* (5th ed.). London: Oxford University Press

Corbin, J. & Strauss, A. (2008). *Basics of Qualitative Research.* Med. Graw-Hill. Boston

Datareportal. (2021, 21. april). *6 in 10 people around the world now use the Internet.* Hentet fra https://datareportal.com/reports/6-in-10-people-around-the-world-now-use-the-internet

Datareportal. (2023, 26. januar). *Global Overview report 2023.* Hentet fra https://datareportal.com/reports/digital-2023-global-overview-report

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

Datatilsynet (2019, 6. februar) *Høringsuttalelse fra Datatilsynet - Forslag til ny lov om etterretningstjenesten.* Hentet fra

https://www.datatilsynet.no/contentassets/9d3198322e844b9d804e89753d737cf0/horingsuttalelse--datatilsynet---ny-lov-om-etterretningstjenesten.pdf

Datatilsynet. (2018). *Datatilsynets strategi - 1. januar 2018- 31. desember 2020*. Hentet fra https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/om-datatilsynet/planer-strategier/datatilsynet_strategi.pdf

Den nasjonale forskningsetiske komité for samfunnsvitenskap og humaniora. (2016, april). *Forskningsetiske retningslinjer for naturvitenskap og teknologi* (2. utg.) Hentet fra https://www.forskningsetikk.no/ressurser/publikasjoner/retningslinjer-nent/

Det kongelige fornyings-, administrasjons- og kirkedepartement. (2013). *Digital agenda for Norge. IKT for vekst og verdiskapning.* (Meld. St. 23(2012-2013). Hentet fra https://www.regjeringen.no/contentassets/4339bb2154bd4b829f1d147bb2b26da8/no/pdfs/stm201220130023000dddpdfs.pdf

Det Norske Akademis Ordbok. (u.å.). *Overvåke*. Hentet fra https://naob.no/ordbok/overv%C3%A5ke

EOS-utvalget. (2012). *Årsmelding 2012-2013*. Hentet fra https://eos-utvalget.no/wp-content/uploads/2019/05/a%CC%8Am2012.pdf

EOS-utvalget. (2016, 17. juni). *Pressemelding 17. juni 2016: EOS-utvalget ber Stortinget vurdere endringer i lovgrunnlaget for etterretningstjenesten*. Hentet fra https://eos-utvalget.no/wp-content/uploads/2019/05/pressemelding_s_rskilt_melding_e_tjenestens_rettsgrunnlag.pdf

Etterretningstjenesteloven. (2020, 19. juni). *Lov om Etterretningstjenesten* (LOV-2020-06-19-77). Hentet fra https://lovdata.no/lov/2020-06-19-77

Etterretningstjenesten. (2022, 14 juni). *Hva gjør etterretningstjenesten?* Hentet fra https://www.etterretningstjenesten.no/om-oss/hva-gjor-etterretningstjenesten

Etterretningstjenesten. (2022. 27. januar). *Fokus 2022.* Hentet fra https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/rapporter/Fokus-2022-til-web.pdf

Etterretningstjenesten. (2023. 27. januar). *Fokus 2023.* Hentet fra https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus-norsk/Fokus2023%20-%20NO%20-%20Weboppslag%20v3.pdf/_/attachment/inline/c1a9a458-aa1d-4bf6-a558-9cec57acde8f:9b2050d897a2b2db1bddc8e505db7b666e608b98/Fokus2023%20-%20NO%20-%20Weboppslag%20v3.pdf

Forente Nasjoner. (1948). *Konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter*. Roma, 4. november 1948.

Forsvaret. (2021, 1. mars). *Forsvarets etterretningsdoktrine 2021*. Forsvarssjefen. Hentet fra https://www.etterretningstjenesten.no/publikasjoner/etterretningsdoktrinen/Etterretningsdoktrine_2021_Web_LoRes_02.pdf/_/attachment/inline/633b7840-43de-42af-bb89-243d81076208:edd1367bd55a434b4489162637336d7d632d42a0/Etterretningsdoktrine_2021%20-%20Web_LoRes%2002%20(PROD).pdf

Forsvarets forskningsinstitutt. (2021, 9. juni). *Hvordan gjøre samfunnet mer robust mot uønsket påvirkning i sosiale medier*. Hentet fra https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/2898/21-01237.pdf

Forsvarsdepartementet. (2015-2016). *Kampkraft og bærekraft-Langtidsplan for forsvarssektoren.* (Prop. 151S 2015-2016). Hentet fra https://www.regjeringen.no/contentassets/a712fb233b2542af8df07e2628b3386d/no/pdfs/prp201520160151000dddpdfs.pdf

Forsvarsdepartementet. (2019-2020). *Lov om etterretningstjenesten (Etterretningstjenesteloven)*. (Prop. 80L 2019-2020). Hentet fra

https://www.regjeringen.no/contentassets/b7bada5f31bc482092318df675a2019d/no/pdfs/prp201920200080000dddpdfs.pdf

Forsvarsdepartementet. (2022, 27. juni). *Forslag til lov om endringer i etterretningstjenesteloven.* Hentet fra https://www.regjeringen.no/no/dokumenter/horing-forslag-til-endringer-i-etterretningstjenesteloven/id2920954/?expand=horingsnotater

Foucault, M. (1979). *Discipline and punish : the birth of the prison.* New York: Vintage Books

Gadamer, H-G. (1960). *Truth and Method.* (overs. 2006 Weinscheimer, J. & Marshall, D. G.) London, Continum. Hentet fra https://edisciplinas.usp.br/mod/resource/view.php?id=3681667

Halvorsen, K. (2008). *Å forske på samfunnet. En innføring i samfunnsvitenskapelig metode.* Oslo: Cappelen Akademisk Forlag.

Haugsbø, E. og Harkestad, I. (2022, 18. oktober). *Masseovervåkning uten sidestykke.* NRK Kronikk. Hentet fra https://www.nrk.no/ytring/masseovervakning-uten-sidestykke-1.16133987

Intelligence and Security Committee of Parliament. (2020, 21. juli). *Russia.* Hentet fra https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf

Kvale, S. & Brinkmann, S. (2009). *Det kvalitative forskningsintervju.* Gyldendal akademisk

Larssen, A. K. & Dyndal, G. L. (2020). *Strategisk ledelse i krise og krig - Det norske systemet.* Universitetsforlaget.

Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

Lysne, O. / Forsvarsdepartementet. (2016, 26. august). *Digitalt grenseforsvar (DGF): Lysne II-utvalget*. Hentet fra https://www.regjeringen.no/contentassets/ca1f705dbebd48cb9a61889d4cfee6bf/digitalt-grenseforsvar-lysne-ii-utvalget.pdf

MacAfee .(2011, 10. februar). *Global Energy Cyberattacks:"Night Dragon"*. Hentet fra https://www.mcafee.com/blogs/wp-content/uploads/2011/02/McAfee_NightDragon_wp_draft_to_customersv1-1.pdf

Macnish, K. (2014). *Just surveillance? Towards a normative theory of surveillance.* Surveillance & Society, 12(1), 142-153.

Marx, G. T. (2015). *Surveillance studies*. International encyclopedia of the social & behavioral sciences, 23(2), 733-741.

Nasjonal sikkerhetsmyndighet. (2022, 3. oktober). *Cyberangrep har blitt hverdagskost.* Hentet fra https://nsm.no/aktuelt/digitalt-risikobilde-2022-cyberangrep-har-blitt-hverdagskost

New York State Department of Financial Services .(2021, april). *Report on the SolarWinds Cyber Espionage Attack and Institutions Response.* Hentet fra https://www.dfs.ny.gov/system/files/documents/2021/04/solarwinds_report_2021.pdf

NOU 2015:13. (2015). *Digital sårbarhet - sikkert samfunn. Beskytte enkeltmennesker i et digitalt samfunn*. Oslo: Departementenes sikkerhet- og serviceorganisasjon

NOU 2022: 11. (2022). *Ditt personvern- vårt felles ansvar.* Oslo: Departementenes sikkerhet- og serviceorganisasjon

Omand, Sir. D. (2020, 30. april). *Uten sikkerhet er ikke friheten og rettssikkerheten fullstendig. Dagens Næringsliv.* Hentet fra https://www.dn.no/innlegg/etterretningstjenesten/digitalt-grenseforsvar-dgf/personvern/innlegg-uten-sikkerhet-er-ikke-friheten-og-rettssikkerheten-fullstendig/2-1-798509

Oppen, M., Mørk, B.E., Haus, E. (2020). *Kvantitative og kvalitative metoder i merkantile fag* (Utg.1). Oslo: Cappelen Damm Akademisk

PST. (2020, 8. desember). *Datainnbrudd mot Stortinget er ferdig etterforsket.* Hentet fra https://www.pst.no/alle-artikler/pressemeldinger/datainnbruddet-mot-stortinget-er-ferdig-etterforsket/

PST (2022) *Nasjonal trusselvurdering 2022*. Hentet fra https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2022/

PST. (2023). *Nasjonal trusselvurdering 2023*. Hentet fra https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2023/

PwC. (2016). *The Industrial Internet of Things*. Hentet fra https://www.pwc.no/no/publikasjoner/Digitalisering/the-industrial-internet-of-things.pdf

Regjeringen. (2021, 19. juli). *Datainnbruddet i Stortingets e-postsystem*. Hentet fra https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/ud/pressemeldinger/2021/pm_datainnbrudd/id2866410/

Regjeringen. (2022, 27. juni). *Forslag til endringer i etterretningstjenesteloven på høring.* Hentet fra https://www.regjeringen.no/no/aktuelt/forslag-til-endringer-i-etterretningstjenesteloven-pa-horing/id2920988/

Regjeringen. (2022, 27.juni). *Høring – Forslag til endringer i etterretningstjenesteloven.* Hentet fra https://www.regjeringen.no/no/dokumenter/horing-forslag-til-endringer-i-etterretningstjenesteloven/id2920954/?expand=horingsnotater

Regjeringen. (2022, 28.juni). *Kva er ei høyring?* Hentet fra https://www.regjeringen.no/no/dokument/hoyringar/kva-er-ei-hoyring/id2459635/

Rønnfeldt, C. (2005). *Konsept for læring og utvikling ved Krigsskolen*. Oslo: Krigsskolen.

Schartum, D. W. (Red.). (2010). *Overvåkning i en rettsstat.* Bergen: Fagbokforlaget.

Sejersted, F. (2005). *Intelligence and Accountability in a State without Enemies: The Case of Norway*. I H. Born, L K. Johnson & I. Leigh (Red.), Who's Watching the Spies? Establishing Intelligence Service Accountability (s. 119-141). Potomac Books.

Silverman, D. (2010). *Doing Qualitative Research.* 3. Utg. Sage. London

Språkrådet. (2018, 10. januar). *Høring.* Hentet fra https://www.sprakradet.no/Vi-og-vart/hva-skjer/Aktuelt-ord/horing/

Statistisk sentralbyrå. (2022). *11124: Hyppighet på internett- og PC-bruk siste 12 måneder (prosent), etter kjønn, alder, statistikkvariabel og år*. Hentet fra https://www.ssb.no/statbank/table/11124/tableViewLayout1/

Statistisk sentralbyrå. (2022:). *06998: Aktiviteter utført på Internett de siste 3 måneder (prosent), etter statistikkvariabel, kjønn, alder og år.* Hentet fra https://www.ssb.no/statbank/table/06998/tableViewLayout1/

Stenslie, S., Haugom, L. & Vaage, B. H. (2019). *Etterretningsanalyse i den digitale tid - En innføring.* Fagbokforlaget.

Stoddart, E. (2014). *Challenging 'just surveillance theory': a response to Kevin Macnish's 'just surveillance? Towards a normative theory of surveillance'*. Surveillance & Society, 12(1), 158-163.

Store norske leksikon. (2022, 25. januar). *Direktiv.* Hentet fra http://snl.no/direktiv

Stortinget. (u.å). *Lov om Etterretningstjenesten* (etterretningstjenesteloven). Hentet fra https://www.stortinget.no/no/Saker-og-publikasjoner/Saker/Sak/?p=79451

Svendsen, H. L. (19. oktober 2022). *Edward Snowden med Norge-kritikk:- Uforståelig for meg.* Nettavisen Økonomi. Hentet fra https://www.nettavisen.no/okonomi/edward-snowden-med-norge-kritikk-uforstaelig-for-meg/s/5-95-713460

Thagaard, T. (2013). *Systematikk og innlevelse – en innføring i kvalitativ metode.* Fagbokforlaget

The White House- President Barack Obama. (2014, 17. januar). *U.S. Presidential Policy Directive on Signals Intelligence Activities.* Hentet fra https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

Tilsynet for universell utforming. (2022, 2. november). *Er du innafor eller utafor?* Hentet fra https://www.uutilsynet.no/uubloggen/er-du-innafor-eller-utafor/1449

Tjernshaugen, A., Berg, O. & Gisle, J. (2022, 21. april). *Høring* i Store norske leksikon på snl.no. Hentet fra http://snl.no/h%C3%B8ring

TV2. (2022, 7. mars). *Norge på russisk liste over uvennlige land.* Hentet fra https://www.tv2.no/nyheter/utenriks/norge-pa-russisk-liste-over-uvennlige-land/14628058/

U.S Office of the Director of National Intelligence. (2017, 6. januar). *Background to "Assessing Russian Activities and Intentions in Recent US Elections:" The Analytic Process and Cyber Incident Attribution.* Hentet fra https://www.dni.gov/files/documents/ICA_2017_01.pdf

US Department of Justice. (2018, 13. juli). *Indictment of 12 russian intelligence officers for hacking the Democratic National Committee and Clinton Campaign.* Hentet fra https://www.justice.gov/file/1080281/download

Vabo, S., Klausen, J.E. Askim, J. (2020). *Offentlig politikk.* Universitetsforlaget

World Economic Forum. (2022). *Networked Readiness Index Norway 2022* https://networkreadinessindex.org/country/norway/

9. Høringssvar

Høringssvarene er hentet fra regjeringens nettsider:

https://www.regjeringen.no/no/dokumenter/horing-forslag-til-endringer-i-etterretningstjenesteloven/id2920954/?expand=horingssvar

Anders Lingjerde
Anita Eriksson
Anne-Helene Andersen
Borgarting lagmannsrett
Datatilsynet
Dommerforeningens fagutvalg for menneskerettigheter
Domstoladministrasjonen (uten merknader)
EDPS
Elektronisk Forpost Norge
EOS-utvalget
Folkets koronakommisjon
Henning Norli Andersen
Høringssvar JD
Høringssvar PST
Høringssvar Telenor
International Business Machines AS (IBM)
Lyse AS
Magnus T Kristiansen
Nikolai Dragnes
NITO - Norges Ingeniør- og Teknologorganisasjon
Norges Høyesterett
Norges institusjon for menneskerettigheter (NIM)
Norsk Journalistlag
Norsk Presseforbund

Norsk rikskringkasting AS

Norsk senter for informasjonssikring (NorSIS) (uten merknader)

Oslo tingrett

Per Watne

Person som ikke har oppgitt navn (101044)

Person som ikke har oppgitt navn (124283)

Person som ikke har oppgitt navn (132765)

Person som ikke har oppgitt navn (323795)

Person som ikke har oppgitt navn (661740)

Runbox Solutions AS

Tekna - Teknisk-naturvitenskapelig forening

Teleplan Globe AS (uten merknader)

Therese Nylander

Torfinn Rygh (uten merknader)