



Datalagringsdirektivet: Frihet, sikkerhet og personvern
En kvalitativ studie av stortingsdebatten og syv politiske partiprogram

Masteroppgave
Risikostyring og sikkerhetsledelse
Universitetet i Stavanger

Høst 2017
Simen Bakke

MASTERGRADSSTUDIUM I
RISIKOSTYRING OG SIKKERHETSLEDELSE

MASTEROPPGAVE

SEMESTER:

Høst 2017

FORFATTER:

Simen Bakke

VEILEDER:

Professor Ole Andreas Hegland Engen

TITTEL PÅ MASTEROPPGAVE:

Datalagringsdirektivet: Frihet, sikkerhet og personvern – En kvalitativ studie av stortingsdebatten og syv politiske partiprogram

EMNEORD/STIKKORD:

Verdier, verdivurderinger, overvåkning, kriminalitetsbekjempelse, terror, alvorlig kriminalitet, frihet, sikkerhet, personvern, personopplysningsvern, datalagring, stordata, datalagringsdirektivet, stortingsbehandling, stortingsdebatt, partiprogram, politikk

SIDETALL:

87 (99 med forsider, innholdsfortegnelse og litteraturliste)

Oslo, 13.09.2017

«Many of our most serious conflicts are conflicts within ourselves. Those who suppose their judgements are always consistent are unreflective or dogmatic».

John Rawls

Forord

Masteroppgaven er skrevet som avslutning på masterstudiet i Risikostyring og sikkerhetsledelse ved Universitetet i Stavanger.

Studiene har vært en kunnskapsreise, hvor jeg har fått anledning til å kombinere flere ulike fagtilnærminger. Fra filosofiske og samfunnsvitenskapelige til mer tekniske-, juridiske- og økonomiske tilnærminger. Perspektivene som fagretningene bidrar med har økt min bevissthet om at menneskeheten representerer et mangfold av ulike måter å forstå verden på, og slik tror jeg det også bør være i velfungerende demokratiske samfunn.

Takk til professor Ole Andreas Hegland Engen for konstruktiv veiledning igjennom hele skriveperioden.

Takk til Therese, Simen, Eline og Siri for tilbakemeldinger og språkvask.

Takk til deg som leser denne avhandlingen og til deg som bidrar til konstruktiv offentlig debatt.

Sammendrag

Denne studien undersøker hvordan de politiske partiene på Stortinget vurderte virkningene av EUs datalagringsdirektiv, og hvordan partiprogrammene kan forklare deres standpunkter. Den første delen av undersøkelsen er gjennomført ved kvantitativ innholdsanalyse av referatet fra stortingsdebatten den 4. april 2011. Gjennom innholdsanalysen er det kartlagt og analysert hvordan de politiske partiene mente at direktivet ville påvirke verdiene frihet, sikkerhet og personvern i det norske samfunnet. Den andre delen av undersøkelsen er gjennomført ved kvalitativ innholdsanalyse av syv partiprogrammer fra 2009. Deretter er funnene fremkom ved innholdsanalyse av stortingsdebatten, vurdert opp imot de forpliktelser som er beskrevet i partienes respektive partiprogram for stortingsperioden 2009 – 2013.

Ved undersøkelse av partienes standpunkter under stortingsdebatten, ser partiene i hovedsak ut til å dele seg i tre grupperinger med ulike syn på direktivets virkninger. AP og Høyre uttrykte at direktivet ville styrket sikkerhet og personvern. FrP, SV og Venstre uttrykte at direktivet ville svekket frihet og personvern. KrF og SP uttrykte at friheten ville blitt svekket og uttrykker i mindre grad hvordan personvernet ville blitt påvirket.

Partiprogrammene ser i varierende grad ut til å kunne forklare de ovenfor nevnte funnene. For APs del, kan partiprogrammet i liten grad forklare partiets standpunkt under stortingsdebatten. Partiprogrammene til Høyre, FrP, KrF og SP kan i noen grad forklare deres standpunkter. Derimot kan partiprogrammene til SV og Venstre i stor grad forklare hvorfor de mente at direktivet ville bidra til å svekke både frihet og personvern i det norske samfunnet. Partiprogrammene til SV og Venstre skilte seg fra de resterende stortingspartiene, ved at de allerede i 2009 hadde tatt eksplisitt avstand fra innføringen av EUs datalagringsdirektiv.

Innholdsfortegnelse

1	Innledning	1
1.1	Problemstilling.....	2
1.2	Definisjoner og begrepsavklaring.....	3
1.3	Avgrensning.....	4
1.4	Begrunnelse for valg av tema	5
1.5	Kontekst.....	6
1.6	Litteratursøk, kildekritikk og tidligere forskning	8
1.7	Oppbygning	10
2	Teori.....	12
2.1	Fremveksten av sikkerhet, frihet og personvern.....	12
2.1.1	Statsdannelse som sikkerhet.....	12
2.1.2	Individets rett på frihet	13
2.1.3	Privatlivet anerkjennes	15
2.2	Verdiene i overvåkningskonteksten.....	16
2.2.1	Terrortrusselen og forebyggende sikkerhet.....	16
2.2.2	Frihet fra overvåkning.....	20
2.2.3	Personopplysningsvern i informasjonssamfunnet	22
3	Begrepene i undersøkelsen.....	25
3.1	Sikkerhet.....	25
3.2	Frihet.....	26
3.3	Overvåkning	27
3.4	Personvern	27
4	Metode	29
4.1	Innholdsanalyse	29
4.2	Datautvalg og datakilder.....	30
4.3	Induktiv og deduktiv metode.....	30
4.4	Reliabilitet og validitet	31
4.5	Analyseenheter, kodeenheter og kontekstenheter	32
4.6	Innholdsanalyse av stortingsdebatten	33
4.6.1	Metodiske problemstillinger	36
4.7	Innholdsanalyse av partiprogrammene	37
4.7.1	Metodiske problemstillinger	39
4.8	Fremstilling av data	39
5	Empiriske funn fra innholdsanalysene.....	40

5.1	Kvantitativ innholdsanalyse av stortingsdebatten	40
5.2	Kvalitativ innholdsanalyse av partiprogrammene	43
6	Diskusjon	45
6.1	Partiprogrammet kan i liten grad forklare partiets standpunkt	45
6.1.1	Arbeiderpartiet (AP).....	45
6.2	Partiprogrammet kan i noen grad forklare partiets standpunkt	51
6.2.1	Høyre (H)	51
6.2.2	Fremskrittspartiet (FrP)	58
6.2.3	Kristelig Folkeparti (KrF)	62
6.2.4	Senterpartiet (SP)	66
6.3	Partiprogrammet kan i stor grad forklare partiets standpunkt	71
6.3.1	Venstre (V).....	71
6.3.2	Sosialistisk Venstreparti (SV)	76
7	Konklusjon.....	81
7.1	Partienes verdivurderinger.....	81
7.2	Partiprogram som forklaringsmodell.....	83
7.3	Begrepsbruk.....	85
7.4	Veien videre.....	86
8	Litteraturliste.....	88
8.1	Offentlige dokumenter.....	90
8.2	Andre kilder.....	91
8.3	Partiprogram	92

1 Innledning

Justisdepartementet la den 10. desember 2010 frem forslag i Prop. 49L (2010) om hvordan Norge kunne implementere den Europeiske Unions (EU) direktiv 2006/24/EF, også kjent som datalagringsdirektivet, i norsk rett. EU begrunnet behovet for direktivet med at unionens medlemsland med fordel burde harmonisere sine regelverk overfor tilbydere av offentlig elektronisk kommunikasjonstjeneste eller offentlig elektronisk kommunikasjonsnett, når det gjaldt lagring av data. Hensikten med direktivet var ifølge EU at data skulle være tilgjengelig for oppdagelse, etterforskning og straffeforfølgning av alvorlig kriminalitet (European Union, 2006). Justisdepartementet la den samme begrunnelsen som EU til grunn for innføring av datalagringsdirektivet, og i Prop. 49L (2010, s. 7) la departementet frem forslag til endringer i lov om elektronisk kommunikasjon, straffeprosessloven, politiloven, tvisteloven og verdipapirhandelloven.

Forslaget om innføring av EUs datalagringsdirektiv i norsk rett fikk stor oppmerksomhet i norske medier og i offentligheten forøvrig. Hele 130 skriftlige innspill ble sendt inn under høringsrunden, og justisdepartementet erkjenner at lovforslagene skapte betydelig debatt på tvers av tradisjonelle politiske skillelinjer (Prop. 49L, 2010, s. 8). Flere store og små offentlige etater, forskningsinstitusjoner, interesseorganisasjoner, politiske partier og privatpersoner sendte inn høringsuttalelser til lovforslaget. Enkelte av høringsinstansene uttrykte direkte støtte til lovforslaget, mens andre uttrykte eksplisitt at de var imot innføringen. Høringsuttalelsene som ble levert kan i stor grad sies å ha inntatt to ulike tilnærminger. Den første tilnærmingen, som i særdeleshet politiet i stor grad gav uttrykk for, var at datalagringsdirektivet var et nødvendig virkemiddel som ville bidra til at norske borgeres *sikkerhet* ble styrket igjennom bedre forutsetninger til å forebygge og etterforske alvorlig kriminalitet. Den andre tilnærmingen var om direktivet i hovedsak var et lovforslag som ville bidra til å svekke norske borgeres *frihet*. I hovedsak ved kontinuerlig overvåking av borgernes telekommunikasjon, og derfor også i strid imot den europeiske menneskerettighetskonvensjonen (EMK). I tillegg var *personvern* et sentralt tema som ble omtalt av både de som var for, og de som var imot innføringen av datalagringsdirektivet. Justisdepartementet viser også i lovforslaget til at de er langt på vei enige i påstanden om at det er betydelige personvernutfordringer knyttet til lagring av store mengder kommunikasjonsdata for hele befolkningen (Prop. 49L, 2010, s. 8).

Under stortingsbehandling av lovforslaget den 4. april 2011, heretter kalt stortingsdebatten, fremstod det som at politikerne på Stortinget hadde delt syn på hvorvidt direktivet var å anse som et positivt eller et negativt tiltak. Debatten kan omtales som en verdidebatt, der de abstrakte verdiene frihet, sikkerhet og personvern ble satt opp imot hverandre, ved vurderingen av et nytt sikkerhetstiltak. De to største partiene på Stortinget stilte seg positive til innføringen av datalagringsdirektivet, og voterte *for* lovforslaget. Dette var Arbeiderpartiet (AP) og Høyre (H). De resterende fem partiene representert på Stortinget, Fremskrittspartiet (FrP), Kristelig Folkeparti (KrF), Senterpartiet (SP), Sosialistisk Venstreparti (SV) og Venstre (V), stilte seg negative til innføringen, og voterte *imot* lovforslaget. Også under stortingsdebatten ser diskusjonen ut til å ha foregått på tvers av tradisjonelle politiske skillelinjer som de norske partiene representerer. Sosialistiske partier med fokus på fellesskapet inntok tilsvarende argumentasjon og standpunkt under stortingsdebatten som liberale partier med fokus på individet, og vice versa. De tre regjeringspartiene under stortingsdebatten i 2011, AP, SP og SV, var heller ikke samstemte om lovforslaget. Ettersom EUs datalagringsdirektiv førte til offentlig debatt, et tegn på at saken vekket interesse hos den norske befolkningen, fremtvinger deg seg noen interessante politiske spørsmål. Hadde partiene i noen grad tatt standpunkt til saken om EUs datalagringsdirektiv i sine respektive partiprogrammer fra 2009, og dermed også i forkant av stortingsdebatten i 2011? Hadde partiene forpliktet seg ovenfor sine velgere, og overholdt de sine forpliktelser ved behandlingen av lovforslaget?

Med dette som utgangspunkt vil det i denne oppgaven undersøkes nærmere hvordan de politiske partiene representert på Stortinget i 2011 gav oppslutning om de tre nevnte verdiene. Både under stortingsdebatten om innføring av datalagringsdirektivet, og i deres partiprogrammer for stortingsperioden. Problemstillingen som er førende for undersøkelsen er todelt, og lyder som følger:

1.1 Problemstilling

- i. Hvordan uttrykte de politiske partiene på Stortinget at datalagringsdirektivet ville påvirket verdiene frihet, sikkerhet og personvern under stortingsdebatten i 2011?
- ii. Hvordan kan partiprogrammene fra 2009 bidra til å forklare stortingspartienes standpunkt under debatten?

1.2 Definisjoner og begrepsavklaring

Begrepene sikkerhet, frihet og personvern omtales i denne oppgaven som *verdier*. En sentral årsak til at disse begrepene kan omtales som verdier, er at de i lengre tid har vært viktig for samfunnsutviklingen, noe som vil redegjøres for nærmere i oppgavens teoridel. De tre nevnte verdiene kan også omtales som abstrakte¹ begreper som trenger nærmere definisjon, avgrensning og presisering for å benyttes i denne undersøkelsen. Definisjonene nedenfor er valgt ut fordi egner seg til å bidra til å besvare problemstillingen, de er relevante for konteksten til undersøkelsen og de er forankret i faglitteratur som vil beskrives nærmere i teorikapittelet.

Verdi defineres som «kvaliteten ved noe, det som er godt ved noe» (Store Norske Leksikon, 2017a). Videre presiseres det at «en tings verdi sies gjerne å bestemme dens viktighet med hensyn til hvordan vi bør gjøre våre vurderinger og beslutninger» og videre at «verdi kan i utgangspunktet tillegges alle ting (personer, objekter, handlinger, tilstander)». I kapittel 2.1 vil det redegjøres nærmere for hvordan de tre nevnte verdiene har vokst frem, og hvorfor de fortsatt er sentrale i dagens samfunn.

Sikkerhet tar i denne undersøkelsen utgangspunkt i begrepet *kriminalitetsbekjempelse* og defineres som «den virksomhet som drives for å hindre at samfunnet og borgerne utsettes for kriminelle handlinger» (NOU 2009:15, s. 68).

Frihet defineres som «fravær av tvang» (Berlin, 1969, s. 128 – 130).

Personvern tar i denne undersøkelsen utgangspunkt i begrepet *personopplysningsvern* og defineres som «normer for behandling av personopplysninger med sikte på å verne om personlig integritet, autonomi og privatlivets fred» (Schartum & Bygrave, 2016, s. 20) og «regler og standarder for behandling av personopplysninger som har ivaretagelse av personvern som hovedmål» (NOU 2009:1, s. 32). De to definisjonene er nokså sammenfallende, og det vises til kapittel 3 hvor en mer inngående redegjørelse for valgte begreper finner sted.

¹ Abstrakt viser til noe tenkt eller ikke-håndgripelig, noe som ikke er sansbart og derfor også immaterielt. Motsetningen til abstrakt er konkrete gjenstander som er sansbare og materielle (Store Norske Leksikon, 2017g).

Overvåkning defineres som «systematisk og rutinemessig innsamling og behandling av personopplysninger med det formål å utøve innflytelse, administrasjon, styring og kontroll» (David Lyon, 2001, s. 2).

Ettersom de utvalgte definisjonene er avgjørende for gjennomføring av undersøkelsen, vil begrepene gjøres rede for og aktualiseres ytterligere i kapittel 3.

1.3 Avgrensning

Stortingsdebatten om datalagringsdirektivet fra 4. april 2011 inneholder mye informasjon innenfor ulike temaer. Det samme gjør de syv stortingspartienes partiprogrammer for stortingsperioden 2009 – 2013. Det er av hensyn til undersøkelsen, kun utsagn relatert til de tre verdiene frihet, sikkerhet og personvern i tråd med definisjonene ovenfor, som vil undersøkes. Det undersøkes ikke inngående hva datalagringsdirektivet er, eller hvorvidt datalagringsdirektivet faktisk ville medført endringer i det norske samfunnet. Undersøkelsen har til hensikt å analysere hvordan stortingspolitikerne uttrykker at direktivet ville påvirket verdiene, og hvordan politikernes standpunkter samsvarer med deres partiprogrammer for perioden.

Datalagringsdirektivet handler i hovedsak om statens mulighet til å benytte overvåkning og datalagring for å forhindre terror og alvorlig kriminalitet² (Prop. 49L, 2010, s. 8). Derfor vil ikke andre former for privat eller kommersiell overvåkning omtales nærmere. Alternative metoder for kriminalitetsbekjempelse, slik som kriminalitetsforebyggende arbeid rettet mot barn og unge, eller styrking av tradisjonelt politiarbeid³ vil få mindre oppmerksomhet. Temaene vil likevel nevnes der hvor det fremstår som relevant i undersøkelsesmaterialet. Hvilken effekt

² Begrepet *alvorlig kriminalitet* benyttes ikke i straffelovgivningen. Likevel benyttes begrepene ofte i det offentlige ordskiftet for kriminalitet med høy strafferamme. Paul Larsson (2011) forklarer at begreper som alvorlig kriminalitet og alvorlig organisert kriminalitet er uklare. De benyttes til ulike formål (også politiske) med stor effekt, nettopp fordi begrepene i seg selv er så uklare. Datalagringsdirektivet ville imidlertid medført endringer i straffeprosessloven, noe som igjen bidrar til å tydeliggjøre grensen for hva som er å anse betrakte alvorlig kriminalitet. Med endringene i straffeprosessloven § 210 b) og c), kunne trafikkdata bli utlevert til politiet ved mistanke om straffbare handlinger med strafferamme på fire år eller mer i fengsel (Graver, 2015, s. 37). Det er derfor naturlig å tolke begrepet alvorlig kriminalitet i denne sammenheng som ulovlige handlinger hvilket medfører en strafferamme på over fire år. Folkemord, terrorhandlinger, kroppsskade, drap, voldtekt, grovt tyveri, grovt bedrageri og ran, er eksempler på ulike handlinger som etter straffeloven har over 4 års strafferamme.

³ Med *tradisjonelt politiarbeid* vises det til de inngrep som politiet vanligvis benytter for å forebygge eller etterforske ulovlige handlinger. I politiloven finner vi politiets tilgang til bruk av «tradisjonelle» maktmidler som å anholde og bortvisning for å forebygge hendelser, og i straffeprosessloven finner vi politiets hjemler for bruk av tvangsmidler som å ransake, beslaglegge og pågripelse. Eksempler på «utradisjonelle» politimetoder er ifølge Nordenhaug og Engene (2008, s. 40 – 41) spaning, postkontroll, telefon- og romavlytting, og bruk av informanter.

datalagringsdirektivet ville hatt på Forsvaret- eller andre etaters etterretningsvirksomhet, vil ikke omtales. Det er politiets mulighet til å avdekke, forebygge og etterforske terrorisme og annen alvorlig kriminalitet som er førende tematikk for undersøkelsen.

Etter terrorangrepet mot USA 11. september 2001 hvor over 3000 mennesker døde, ser overvåkningen for å avverge terror og annen alvorlig kriminalitet ut til å ha blitt sterkt intensivert (Dragu, 2011, s. 4, Richards, 2013, 1935-37, Hammerlin, 2008, s. 14-45). Teorien i denne oppgaven tar derfor utgangspunkt i litteratur som forklarer hvordan behovet for sikkerhetstiltak oppstår som følge av terror, og hvordan overvåkningen påvirker borgernes friheter og personvern. Mindre alvorlige former for kriminalitet vil få lite oppmerksomhet, ettersom datalagringsdirektivet i stor grad ble foreslått som et virkemiddel mot terror og annen alvorlig kriminalitet (Prop. 49L, 2010, s. 8).

I etterkant av stortingsdebatten om innføringen av datalagringsdirektivet i 2011, har det forekommet terrorangrep i Norge. Den 22. juli 2011 ble regjeringskvartalet bombet og ungdommer ved AUFs sommerleir på Utøya, ble skutt og drept. Totalt mistet 77 mennesker livet. I flere europeiske storbyer, som Paris og Brussel, ble det begått terrorangrep i 2015 (NOU, 2016:19, s. 61) og senest i 2017 ble det begått terrorangrep i Stockholm og London (Aftenposten, 2017a og Aftenposten, 2017b). Det har altså oppstått flere terror-relaterte hendelser både i og utenfor Norge i etterkant av stortingsdebatten. Hendelsene kan ha påvirket stortingspartienes synspunkter. Likevel er den empiriske undersøkelsen avgrenset til å gjelde stortingsdebatten fra 2011 og partiprogrammene fra 2009. Årsaken er at undersøkelsen er en analyse av sammenhengen mellom partienes forpliktelser i partiprogrammene, og hva de samme partiene faktisk uttrykte under stortingsdebatten.

1.4 Begrunnelse for valg av tema

Bakgrunnen for undersøkelse av den valgte problemstillingen, er fordi vi lever i en tid med stor usikkerhet om fremtidig samfunnsutvikling. For å møte usikkerheten, blir kunnskap betraktet som en viktig kilde til å svare på store og kompliserte samfunnsspørsmål. Til tross for at kunnskap er viktig, kan det også argumenteres for at *verdier* og *verdivurderinger* i stor grad også er styrende for politiske beslutninger i kompliserte saker. En sentral årsak til at verdier er styrende, er nettopp fordi vi som samfunn ikke alltid innehar tilstrekkelig kunnskap til å kunne forutsi de fremtidige konsekvensene av våre handlingsalternativer. Eller at det hefter stor

usikkerhet ved politiske beslutninger i kompliserte saker. I tillegg er det ofte slik at vi som mennesker innehar ulik oppfatning av hvorvidt konsekvensene er å betrakte som positive eller negative, selv ved én og samme beslutning (Renn, 2008, s. 1 og 2).

Stortingsdebatten om innføring av datalagringsdirektivet i 2011 kan ha fremstått som en slik verdidebatt. En debatt der de fremtidige konsekvensene ved innføring av et sikkerhetstiltak (datalagringsdirektivet), var usikre. På grunn av denne usikkerheten, kan det hevdes at stortingspolitikere også under denne debatten la deres verdivurderinger til grunn ved beslutningen om å stemme for eller imot innføringen av direktivet. Etersom de totale samfunnsmessige virkningene av datalagringsdirektivet heller ikke lot seg beregne nøyaktig, ble det i stor grad opp til de politiske partiene å gjøre seg opp en mening om direktivet og dets fremtidige virkninger. Etersom stortingspolitikere velges inn på vegne av, og for å representere deler av den norske befolkningen, er det interessant å undersøke de sikkerhetspolitiske aspektene som denne undersøkelsens problemstilling tar opp, nærmere.

1.5 Kontekst

Justisdepartementet la som nevnt i Prop. 49L (2010) frem et lovforslag om hvordan EUs Datalagringsdirektiv (EUs direktiv 2006/24/EF) kunne gjennomføres i norsk rett. Lovforslaget ble behandlet i Stortinget, og vedtatt. Den norske loven som ble utformet på bakgrunn av direktivet, fikk navnet «lagringsloven». Lagringsloven gav pålegg til tilbydere av elektronisk kommunikasjon om å lagre data tilknyttet fasttelefon, mobiltelefon, internettaksess, e-post og bredbåndstelefon. Senere ble det klart at EU-domstolen konkluderte med at direktivet var ugyldig, ettersom det brøt med retten til privatliv og retten til personvern. Ifølge jusprofessor Hans Petter Graver (2015, s. 4) som skrev en utredning om lovforslaget, var direktivet mer inngripende enn hva EU-domstolen betraktet som nødvendig for å ivareta allmenne interesser.

Ifølge Hans Petter Graver (2015, s. 37) inneholdt lovvedtaket to hovedelementer. Det første var en plikt for ekomtilbydere til å lagre abonnements-, trafikk-, og lokaliseringsdata i seks måneder. Det andre var en rett til utlevering av disse dataene på bestemte vilkår. Datalagringsdirektivet ville derfor medført endringer i flere lovverk. Blant annet ekomloven, som regulerer teletilbyderes virksomhet, og straffeprosessloven, som regulerer blant annet politiets tilgang til bruk av tvangsmidler. To av de vesentligste endringene som gjelder

lagringsplikten og retten til utlevering, vil det her redegjøres for. Slik at det er klart hva datalagringsdirektivet faktisk ville medført, dersom det ble innført og iverksatt.

Lagringsplikten (Ekomloven § 2-7a):

Tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste skal lagre trafikkdata, lokaliseringsdata og data nødvendig for å identifisere abonnenten eller brukeren i 6 måneder til bruk for etterforskning, oppklaring og straffeforfølgning av alvorlige straffbare forhold. Plikten etter første punktum gjelder data som genereres eller behandles i tilbyders elektroniske kommunikasjonsnett ved bruk av fasttelefon, mobiltelefon, internettelefon, internettaksess og e-post.

Utlevering av basestasjonsdata (Straffeprosessloven § 210c):

Retten kan ved kjennelse pålegge utlevering for et begrenset tidsrom av opplysninger om hvilke telefoner eller annet kommunikasjonsutstyr som innenfor et nærmere bestemt geografisk område har vært satt i forbindelse med bestemte telefoner eller kommunikasjonsutstyr og som tilbyder har plikt til å lagre etter lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon § 2-7 a. Pålegg kan gis når det foreligger skjellig grunn til mistanke om en eller flere straffbare handlinger som etter loven kan medføre straff av fengsel i 5 år eller mer.

Utlevering av trafikkdata (Straffeprosessloven § 210b):

Retten kan ved kjennelse pålegge utlevering for et bestemt tidsrom av trafikkdata, og lokaliseringsdata som ikke omfattes av § 210 c, og som tilbyder har plikt til å lagre etter lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon § 2-7 a. Pålegg kan gis når det foreligger skjellig grunn til mistanke om en eller flere straffbare handlinger som etter loven kan medføre straff av fengsel i 4 år eller mer.

Ifølge Graver (2013, s. 45) var det ikke foreslått i de nye straffeprosessbestemmelsene at de skulle kunne benyttes i forebyggende øyemed. Likevel påpeker Graver at det også kunne være aktuelt med utlevering av data etter politiloven § 17 d til Politiets sikkerhetstjeneste (PST), som kan benytte bestemte tvangsmidler i sin forebyggende virksomhet. Videre mener Graver at adgangen er begrenset til enkelte forbrytelser, blant annet terrorhandlinger, ulovlig

etterretningsvirksomhet og en del grove frihets- og legemskrenkelser. Bruk av tvangsmidler i forebyggende øyemed krever likevel kjennelse fra retten, og forutsetter at «det er grunn til å tro at inngrepet vil gi opplysninger av vesentlig betydning for å kunne forebygge handlingen». Tvangsmidler til bruk for forebyggende virksomhet hvor *grunn til å tro* er tilstrekkelig for inngrep, er et lavere beviskrav sammenliknet med det tradisjonelle *skjellig grunn til mistanke* som normalt sett er beviskravet ved bruk av tvangsmidler til politiets etterforskning.

Tilgangen til data var ifølge Graver (2015, s. 43 – 44) primært forbeholdt politi og påtalemyndighet. Likevel ville også Finanstilsynet ha adgang til de lagrede dataene igjennom verdipapirhandelloven. Ingen andre myndigheter skulle ha tilgang til dataene, slik lovvedtaket var utformet. Videre var lagringsplikten begrenset til seks måneder. Lagringsplikten skulle avløses av en sletteplikt, som trådte i kraft etter seks måneder. Data som ble utlevert til politiet, skulle behandles i samsvar med politiregisterloven. Dersom tjenestemenn i politiet skulle ha tilgang til opplysningene, kunne opplysningene gis igjennom direkte søk, eller gjøres tilgjengelig på annen måte etter tjenestens behov.

1.6 Litteratursøk, kildekritikk og tidligere forskning

Deler av det teoretiske materialet i denne oppgaven er hentet fra internasjonal forskning, og i særdeleshet forskning på amerikanske og europeiske forhold. Forskning på overvåkning er et større fagfelt i USA og Storbritannia sammenliknet med i Norge. Studiene går ofte under betegnelsen «surveillance studies». Studier om sikkerhet, ofte betegnet som «security studies» er også et stort fagfelt både i USA og Storbritannia. Det har vært gjennomført søk i google scholar og ulike bibliotek- og artikkeldatabaser på søkeord som «terror», «terrorism», «surveillance», «security», «privacy», «liberty», «freedom», «proactive policing», «sikkerhet», «frihet», «overvåkning», «personvern», «big data», «stordata» etc. i ulike kombinasjoner for å komme frem til relevante artikler. I tillegg har referanselister fra forskningsartikler og masteroppgaver, ledet frem til egnet litteratur for bruk i denne undersøkelsen.

Ved den teoretiske gjennomgangen i denne oppgaven påpekes det flere steder at forskningen er gjennomført på forhold utenfor Norge. Likevel er det forsøkt å finne frem til forskning på feltet hva gjelder norske forhold. Blant annet har Joakim Hammerlin (2009) og Iselin Nordenhaug & Jon Oscar Engene (2008) skrevet inngående om forholdet mellom forebygging av terror, personvern og overvåkning, og hvordan fenomenene har utviklet seg i Norge i etterkant av

terrorangrepene mot USA, 11. september 2001. Også på feltet personvern, og i særdeleshet hvordan informasjonsteknologi og registrering av personopplysninger påvirker personvernet, finnes det norsk litteratur. Blant annet fra Schartum & Bygrave (2016) og Jon Bing (2010). De deler av oppgaven hvor internasjonal forskning har preget undersøkelsen, er det undersøkt om det også finnes paralleller til norsk forskning. Hensikten har vært å styrke teoriens gyldighet til bruk på norske forhold, som er denne undersøkelsens hovedanliggende.

Når det gjelder temaet overvåkning, har det vært enklere å lete frem vitenskapelige artikler som påpeker at overvåkning har negative fremfor positive konsekvenser. Det ser ut til å herske liten tvil om at overvåkning som fenomen bidrar til å svekke borgernes friheter. Spesielt dersom overvåkningen rettes mot hele befolkningen eller bestemte befolkningsgrupper, og ikke kun de som mistenkes for å ha begått kriminelle handlinger (Richards 2013, Solove 2008, Lyon 2014, Lewis 2005 og Citron & Gray 2013). Under litteratursøkene har det ikke fremkommet vitenskapelige artikler som viser positive effekter av overvåkning, som eksempelvis avdekking og avverging av terrorisme. Det finnes imidlertid flere artikler som påpeker at myndighetene selv hevder at overvåkningen har eller kan ha positive effekter, uten at dette er dokumentert ved hjelp av vitenskapelige fremgangsmåter (Richards 2013, Lyon 2014 og Dragu 2011).

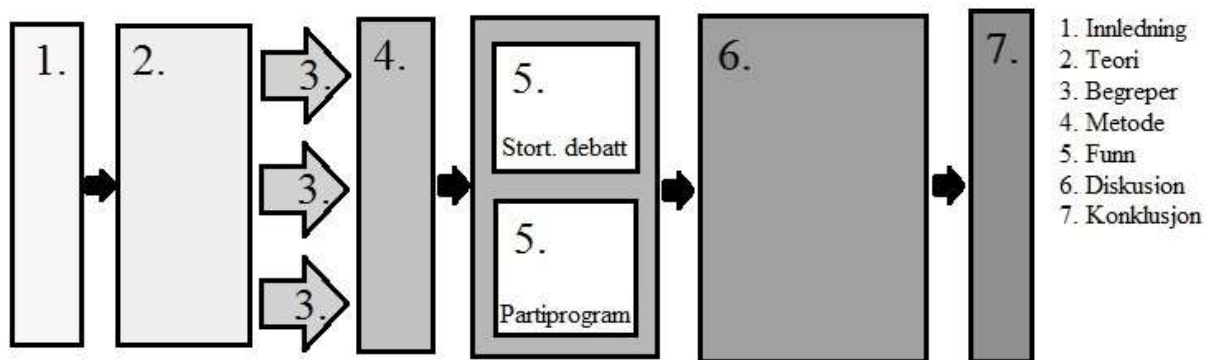
Det er skrevet flere masteravhandlinger i Norge om datalagringsdirektivet, og i særdeleshet flere juridiske avhandlinger som drøfter rettslige problemstillinger ved lovforslaget. Av relevante samfunnsvitenskapelige masteravhandlinger om direktivet finner vi blant annet Nicolaysen (2011) som gjennomførte en diskursanalyse av høringsuttalelsene til lovforslaget. Studien til Nicolaysen konkluderte med at høringsuttalelsene representerte en rekke ulike diskurser, hvor økonomi-, overvåkning-, og etterforskningsdiskurser var de mest sentrale. Refviks (2011) masteravhandling er også relevant da studien bidrar til å forklare hvorfor debatten rundt lovforslaget har vært så konfliktfylt. Refvik konkluderer blant annet med at direktivet har et komplekst innhold, konflikten mellom aktørene er i stor grad moralsk-etisk, og både rettsstaten og personvernbegrepet kommer under diskusjon. En analyse av mediedekningen i forkant av stortingsdebatten er gjennomført av Jamtvedt (2011). Studien konkluderer blant annet med at direktivet i hovedsak ble fremstilt negativt i norsk offentlighet.

Denne masteravhandlingen vil bidra til å belyse et fagområde med samfunnsmessig nytteverdi, som tidligere ikke er undersøkt vitenskapelig. Studien som inngående undersøker

stortingsdebatten ved behandling av lovforslaget, og videre vurderer politikernes standpunkter under debatten opp mot forpliktelser i deres partiprogrammer, er frem til nå, et ubelyst tema.

1.7 Oppbygning

Figur 1 er utarbeidet for å synliggjøre undersøkelsens struktur. Figuren er en visualisering av oppbygningen som vil beskrives nærmere i dette kapittelet.



Figur 1: Undersøkelsens struktur. Hvert av undersøkelsens kapitler (1-7) er representert i modellen ovenfor.

Nå som innledning med problemstilling, definisjoner, avgrensning og kontekst er beskrevet, vil oppgaven løses ved å redegjøre for sentrale teoretiske perspektiver i kapittel 2. Teorien har til hensikt å bidra til besvarelse av oppgavens problemstilling. Sikkerhet, frihet og personvern omtales som abstrakte verdier og begreper, som ville blitt påvirket dersom datalagringsdirektivet ble innført. Ved hjelp av tekstene til Thomas Hobbes (*Leviathan*, 1651), John Stuart Mill (*On Liberty*, 1859), Isaiah Berlin (*Two Concepts of Liberty*, 1958) og Warren & Brandeis (*The Right to Privacy*, 1890) vil det redegjøres for hvordan de tre nevnte verdiene historisk sett har vokst frem som viktige samfunnsverdier.

Terror og alvorlig kriminalitet er områder som utfordrer statens evne til å beskytte egne borgere. Det vil derfor redegjøres for hvordan statlige myndigheter responderer på terror. Et sentralt sikkerhetstiltak for å avverge terror og alvorlig kriminalitet, er overvåkning. Overvåkning ville i større grad blitt muliggjort for staten og politiet gjennom datalagringsdirektivet. Overvåkning som konsept trenger derfor ytterligere redegjørelse slik at både positive og negative konsekvenser ved virkemiddelet kan belyses nærmere. I særdeleshet vil det belyses hvordan overvåkning påvirker balansen mellom oppgavens tre verdier, frihet, sikkerhet og personvern.

I kapittel 3 vil begrepene frihet, sikkerhet, personvern og overvåkning gjøres ytterligere rede for. Begrepene som er definert innledningsvis i kapittel 1.2, er så sentrale for datainnsamling

og tolkning av det empiriske materialet – at det er nødvendig med nærmere presisering av begrepene. Deretter vil det metodiske rammeverket som de empiriske dataene innsamles og analyseres igjennom, gjennomgås i kapittel 4. Kvalitativ metode ved bruk av innholdsanalyse har vært et egnet utgangspunkt. Både kvantitativ- og kvalitativ innholdsanalyse er benyttet. Datainnsamlingen er todelt. Den første delen av innholdsanalysen tar for seg stortingsdebatten om datalagringsdirektivet fra 2011. Her vil antallet utsagn som kan knyttes til verdiene frihet, sikkerhet og personvern – fra hvert av stortingspartiene, kartlegges. Deretter vil den kvalitative innholdsanalysen av stortingspartienes partiprogrammer for perioden 2009 – 2013, gjennomføres. På bakgrunn av innholdsanalysene, vil det være mulig å si noe om hvordan de ulike partiene uttrykker at datalagringsdirektivet ville påvirket de tre verdiene, og om partienes standpunkter under stortingsdebatten er i tråd med forpliktelser i eget partiprogram.

En kort oppsummering av funnene fra innholdsanalysen av stortingsdebatten og partiprogrammene vil presenteres i kapittel 5. I kapittel 6 vil funnene fra hvert enkelt parti diskuteres i lys av oppgavens problemstilling. Diskusjonen vil ta for seg ett og ett parti, og sammenlikne hva partiet uttrykte under stortingsdebatten i 2011, med hva partiet hadde forpliktet seg til i partiprogrammet fra 2009.

Avslutningsvis vil kapittel 7 besvare oppgavens problemstilling. Etersom problemstillingen er todelt, hvor del én er som følger: «Hvordan uttrykte de politiske partiene på Stortinget at datalagringsdirektivet ville påvirket verdiene frihet, sikkerhet og personvern under stortingsdebatten i 2011?». Og del to: «Hvordan kan partiprogrammene fra 2009 bidra til å forklare stortingspartienes standpunkt under debatten?», vil også konklusjonen deles i to underkapitler. Kapittel 7.1 vil besvare den første delen av problemstillingen, mens kapittel 7.2 vil besvare den andre delen. Avslutningsvis vil jeg knytte noen viktige merknader til begrepsbruk, fagkunnskap om temaet og veien videre innen fagfeltet overvåking i Norge.

Nå som innledning, problemstilling, avgrensning, kontekst og oppbygning er redegjort for, vil de teoretiske innfallsvinklene som bidrar til å belyse problemstillingen, undersøkes nærmere.

2 Teori

Kapittel 2 vil innledningsvis gi en historisk redegjørelse for fremveksten av begrepene frihet, sikkerhet og personvern. Oppgavens problemstilling har til hensikt å besvare hvordan stortingspolitikkerne uttrykte seg med hensyn til de tre nevnte verdiene under stortingsdebatten om datalagringsdirektivet. Etablering av en grunnleggende forståelse for hva de tre verdiene *er*, og hvordan de *påvirkes* av overvåkning – er nødvendig for å besvare oppgavens problemstilling. Det vil også redegjøres for hvordan terror og alvorlig kriminalitet ofte fører til økt politisk fokus på sikkerhet, og hvordan overvåkning utfordrer borgernes rett på frihet og personvern.

2.1 Fremveksten av sikkerhet, frihet og personvern

I kapittel 2.1 vil det redegjøres for sentrale teoretiske bidrag som forklarer den historiske fremveksten av samfunnsverdiene sikkerhet, frihet og personvern.

2.1.1 Statsdannelse som sikkerhet

Thomas Hobbes skrev i 1651 boken *Leviathan* (2012, s. 174), som også i dag sees på som et grunnleggende verk innenfor statsvitenskap og politisk filosofi. Hobbes redegjorde for hvordan det han omtalte som naturtilstanden, også kjent som «alles kamp mot alle», utfordret individenes sikkerhet i forfatterens levetid. Naturtilstanden førte til at ulike grupper, byer, klaner og familier kom i konflikt med hverandre og førte kamp seg imellom for makt, naturressurser og territorium. Grupperingene var mange, og ingen felles maktoverhode forente dem.

Som en løsning på utfordringene som naturtilstanden medførte, mente Hobbes at borgerne i bystaten skulle frasi seg sin rett til å bestemme over seg selv, og overlate makten til en felles hersker.

Det finnes bare en måte å gå frem på for å opprette en felles makt som kan forsvare menneskene mot angrep fra ytre fiender [...] Og det er gjennom å overføre all den makt og styrke de har til ett menneske eller en forsamling av mennesker til å representere deres person (Hobbes, 2012, s. 177).

Herskeren skulle ha som primæroppgave å sørge for borgernes sikkerhet, da sikkerhet ikke var noe borgerne kunne ta for gitt på Hobbes' levetid. Gjennom en samfunnskontrakt gav borgerne

avkall på store deler av sin frihet, til fordel for sikkerhet som herskeren skulle garantere. Hobbes hevdet at herskeren hadde rett til å gjøre alt det han fant nødvendig for å bevare fred og forsvar, og at herskeren kunne dømme hvilke meninger og læresetninger som enten strider mot, eller bidrar til fred. Ettersom menneskers handlinger springer ut av deres meninger, mente Hobbes at herskeren også måtte kunne styre individenes meninger – og bestemme hvilke emner som skulle tillates når det gjaldt å tale til folkemasser (Hobbes, 2012, s. 183). *Leviathan* kan i større grad betraktes som et verk der Hobbes redegjør for mer autoritære styreformer sammenliknet med dagens moderne demokratiske stater. Likevel kan sikkerhetsperspektivet som forfatteren bidro med, sies å være nyttig for forståelsen av staten som borgernes sikkerhetsgarantist.

2.1.2 Individets rett på frihet

John Stuart Mill blir sett på som en sentral frihetstenker innen politisk filosofi. I hans litterære bidrag *On Liberty* fra 1859, beskriver Mill viktigheten av at individene sikres tilstrekkelig grad av individuell frihet. Med frihet mente Mill først og fremst «beskyttelse mot de herskendes maktsyke». Mill forklarte at hensikten med hans verk *On Liberty* var å behandle spørsmål som «hvilke grenser kan man trekke for den makt samfunnet rettmessig kan utøve over individet? Hvor må grensen for denne makten settes?» Ifølge Mill var dette særdeles viktige spørsmål, som dessverre sjeldent ble diskutert prinsipielt (Mill, 2010, s. 9).

Mill (2010, s. 21) begrunnet behovet for borgernes frihet som en forutsetning for individenes mulighet for selvrealisering, sannhetssøken, og til å være herre i egne liv. Menneskeheten har mer å tjene på at folk får leve slik de selv vil, enn å tvinge hverandre til å leve slik andre mener de bør leve. I særdeleshet gjør behovet for individenes frihet seg gjeldende i tilfeller hvor flertallet av folket, eller deler av folket, undertrykker et mindretall – eller der hvor staten urettmessig undertrykker individet (Mill, 2010, s. 12). For komme frem til sannhet, som ifølge Mill er en av de viktigste oppgavene til menneskeheten – er borgerne avhengige av å kunne utøve fri og uhindret meningsutveksling. Frihet til å føre åpne og ærlige diskusjoner uten frykt for reaksjoner fra andre borgere eller staten, er ifølge Mill en av de viktigste forutsetningene for selvrealisering, og derfor også samfunnsutviklingen.

Å oppdage noe som på det dypeste angår verden og som den tidligere var uvitende om, å bevise at man har tatt feil på et avgjørende punkt verdslig eller åndelig sett, er vel blant de største tjenester man kan gjøre sine medmennesker (Mill, 2010, s. 37).

Historien er ifølge Mill (2010, s. 31 – 33), full av eksempler på mennesker som har vært forut for sin tid og båret frem nye sannheter, men likevel har måtte fryktet for sine liv dersom de uttalte sine meninger i offentlighet. I slike situasjoner mente Mill det var helt sentralt at staten nettopp beskytter individet mot overgrep fra andre, men også mot overgrep begått av staten selv. Mill var kritisk til det han kalte flertallets tyranni, der alle individer presses til likhet og konformitet – og ikke lengre benytter den frie tanke til sannhetssøking og selvrealisering. Til tross for at Mill var en forkjemper for individuelle friheter, aksepterte han likevel innskrenkinger i tilfeller hvor ytringer og handlinger kunne være til skade for andre individer. I tilfeller hvor enkeltindivider brøt loven og påførte andre individer skade, mente Mill i likhet med Hobbes, at handlingene måtte straffes (Mill, 2010, s. 89 – 90). Likevel problematiserte han staten og politiets mulighet til å forhindre hendelser, da han i teksten stiller det retoriske spørsmålet: «hvor store innhugg i borgernes frihet kan vi gjøre for å forebygge forbrytelser og ulykker?» Funksjonen «å forebygge» rommer langt større muligheter for misbruk av borgernes frihetsrettigheter enn det å kunne ilegge straff. Nettopp det faktum at vi er frie individer, gjør det dermed også lettere å begå forbrytelser (2010, s. 113 – 114).

Isaiah Berlin skapte i artikkelen *Two Concepts of Liberty* (1969, s. 128 – 130) et skille mellom positive friheter og negative friheter. Berlin beskriver negative friheter som «området hvor mennesker er eller har muligheten til å være det de ønsker, uten inngrep fra andre». Negative friheter kan med andre ord forstås som naturgitte rettigheter som alle mennesker er medfødt, i form av å være mennesker. Til tross for at frihet er et abstrakt begrep som ikke kan måles kvantitativt, så kan omfanget av frihet forstås slik at jo større rommet for utfoldelse uten inngrep fra andre er, desto større er også området for individets frihet. Positiv frihet handler ifølge Berlin om individets rett til å realisere seg selv som medlem av et samfunn eller et sosialt fellesskap. Retten til å realisere seg selv skal likevel være begrenset innenfor rammene av hva samfunnet tillater. Underforstått ligger det derfor et paternalistisk⁴ budskap, der staten ikke kan overlate til individet selv å bedømme hva som er gode eller dårlige valg, og moralske spørsmål om hva som er rett eller galt (Lavik og Fjørtoft, 2008, s. 154). Berlin hevdet at en slik positiv frihetsforståelse nettopp kan benyttes til å forsvare totalitære statsformer hvor myndighetene kan legitimere sitt eget diktatur i at det finnes objektiv, moralsk og politisk sannhet som folk flest ikke har innsikt i. Fordi det er til borgernes eget beste, så kan myndighetene diktere

⁴ Paternalisme omhandler forholdet mellom de styrende og de styrte, som innebærer at de styrende nærmest tar faderlig omsorg og kontroll over den styrte. Den underdanige styrte betraktes som uselvstendig og dermed i dårligere stand enn de styrende til å ta beslutninger som angår eget liv (Store Norske Leksikon, 2017e).

borgerne – nettopp for at sistnevnte ikke selv vet best. På denne måten blir borgerne, ironisk nok, tvunget til frihet (Lavik og Fjørtoft, 2008, s. 171 – 174).

Når det gjelder negative friheter, skriver Berlin at til tross for at rommet for frihet må være stort nok til at vi som individer kan oppfylle våre individuelle mål, må også våre friheter begrenses av statens lover. Dersom ikke menneskenes friheter begrenses, vil man kunne risikere å havne tilbake i en naturtilstand der alle mennesker begrenser hverandres frihet og man tilslutt havner i sosialt kaos. Fordi man av hensyn til rettferdighet, krever at alle individer skal ha tilgang på et minimum av frihet, må også alle individenes frihet begrenses. Om så ved bruk av makt (Berlin, 1969, s. 128 – 130).

2.1.3 Privatlivet anerkjennes

I artikkelen *The Right to Privacy* (1890, s. 193) skrevet av Samuel D. Warren og Louis D. Brandeis, forklarer de to amerikanske Harvardjuristene bakgrunnen for fremveksten av fenomenet personvern. De forklarer at eiendomsrett og beskyttelse av individet er prinsipper som har stått sterkt siden lovene i vestlige samfunn ble fastsatt, men at det fra tid til annen er nødvendig å definere det eksakte og avgrensede området for slik beskyttelse. Politiske, sosiale og økonomiske endringer skaper krav om nye rettigheter som samfunnet må imøtekomme igjennom lovgivningen.

Warren og Brandeis (1890, s. 195 – 196) skriver at «retten til liv» var sentral i beskyttelsen av individet, hvor det engelske ordet liberty (frihet) ble forstått som «frihet fra tvang». Senere ble også individets spirituelle natur anerkjent, hvilket også innebar følelser og intellekt. Gradvis har spekteret av rettigheter ifølge Warren og Brandeis, utvidet seg. Det som tidligere ble forstått som «retten til liv» utviklet seg videre til «retten til å nyte liv» og «retten til å være alene». Intensiteten og kompleksiteten som er fremtredende med sivilisasjonens fremskritt, har gjort det nødvendig for individene også å kunne trekke seg tilbake. Kulturens innflytelse har gjort oss mer sensitive til publisitet, og derfor blir også retten til personvern desto mer essensiell for individet. Ifølge Warren og Brandeis er retten til personvern sentral nettopp fordi uønsket eksponering og inngrep i privatlivet er mer skadelig for individets mentale helse og kan skape lidelser mer alvorlig enn hva som kan påføres av fysisk skade.

Ifølge Warren og Brandeis (1890, s. 198) skal det være individets rett å bestemme i hvilken utstrekning ens tanker, oppfatninger og følelser skal kommuniseres til andre. Foruten å vitne i rettssystemet, kan individet aldri bli tvunget til å uttrykke tankene, oppfatningene eller følelsene sine. Denne retten til personvern eksisterer uavhengig av hvilken metode for kommunikasjon som benyttes. Enten det er ord, tegn, gjenstander eller musikk. Retten skal ifølge Warren og Brandeis beskyttes uavhengig av verdien og budskapet i kommunikasjonen.

Sikkerhet, frihet og personvern slik Hobbes, Mill, Berlin og Warren & Brandeis beskriver fenomenene – er å betrakte som viktige samfunnsverdier. Til tross for at verdiene kan omtales som abstrakte, har de utvilsomt kvaliteter som gir verdiene høy status. At verdiene er forankret i lovverk, blant annet den norske Grunnloven – bidrar til å opprettholde verdienes viktige posisjon i det norske samfunnet. Det vil nå gjøres rede for mer dagsaktuell teori innen feltet.

2.2 Verdiene i overvåkningskonteksten

I kapittel 2.2 vil det redegjøres for hvordan terror og alvorlig kriminalitet har ført til økt fokus på sikkerhet og ytterligere bruk av overvåkning. Hvordan borgernes friheter og personvern utfordres av økt overvåkning, er sentralt for besvarelse av oppgavens problemstilling.

2.2.1 Terrortrusselen og forebyggende sikkerhet

Terrorangrepet 11. september 2001 mot World Trade Center i USA var ifølge Tiberiu Dragu (2011, s. 4), et paradigmeskifte i den politiske sikkerhetsutviklingen. Oppmerksomheten endret seg drastisk fra å ha fokus på straff i etterkant av terrorangrep, til å forsøke å forebygge og forhindre fremtidige angrep. Utviklingen er ifølge Dragu, ikke spesielt overraskende tatt i betraktning skadepotensialet til terrorangrep dersom de utføres ved hjelp av biologiske, kjemiske eller nukleære virkemidler. Nancy Lewis (2005, s. 109 - 111) forklarer at det i USA, blant eksperter og militære analytikere, har festet seg en antakelse om at «det er ikke et spørsmål om hvis det neste terrorangrepet vil finne sted, men når».

Joakim Hammerlin (2009, s. 17 – 43) forklarer at frykten for terrorangrep i etterkant av 11. september førte til lagring av flere personopplysninger i USA, Europa og i Norge. Lagringen begrunnes i at politiet og etterretningstjenestene skal ha mulighet til å forebygge terror. Personopplysninger, herunder også biometriske data om individet, er ifølge myndighetene sentralt for å identifisere individer med «risikoprofiler» og dermed også potensielle terrorister.

Sikkerhetsarbeidet er i stor grad desentralisert, privatisert og innebærer involvering av en rekke ulike aktører. Personopplysninger blir derfor i større grad distribuert mellom ulike aktører. Private-, offentlige- og internasjonale aktører og stater, tar alle del i sikkerhetsarbeidet. Nordenhaug & Engene (2008, s. 147) viser til at Norge i etterkant av 11. september 2001 innførte straffebud mot terrorisme, og at handlingene i USA var direkte medvirkende til innføringen. Terrorangrepene mot USA førte til en internasjonal innsats mot bekjempelse av terrorisme, hvor stater uten særlig erfaring med terrorisme, som Norge, i større grad begynte å nærme seg tilsvarende politikk som stater med lengre erfaring med nasjonal eller internasjonal terrorisme. Utviklingen i Norge har også medført større bruk av *preaktiv*⁵ strafferett, hvor hensikten er at politiet skal kunne gripe inn før en hendelse har funnet sted. Bruk av utradisjonelle etterforskningsmetoder som ransaking av personer uten skjellig grunn til mistanke, spaning, postkontroll, telefon- og romavlytting og bruk av informanter benyttes i større grad mot potensielle terrorister (Nordenhaug & Engene, 2008, s. 40 – 41).

Myndighetene er avhengig av etterretningsinformasjon i forkant av en mulig hendelse, for å kunne avdekke og forhindre fremtidige terrorangrep. Neil Richards (2013, s. 1935 – 1937) viser til at demokratisk valgte myndigheter i vesten har inngått mer omfattende forpliktelser til å overvåke sin egen befolkning, og har investert stort i overvåkningsteknologi i etterkant av 11. september 2001. Ofte har kontra-terrorisme, cybersikkerhet og beskyttelse av barn fra overgrep vært begrunnelser for økt overvåkning fra myndighetenes side. Ettersom overvåkningsteknologien blir mer tilgjengelig, billigere og mer brukervennlig – vil sikkerhetsmiljøet ta i bruk mer overvåkningsteknologi (Lewis, 2005, s. 109 - 111). Paul Larsson viser til at det for norsk politi, har vært vanlig å se til utlandet for å være «føre var» og for å utvikle nye politimetoder. Larsson, som har forsket på politiets bruk av de utradisjonelle politimetodene til bruk i narkotikabekjempelse, forklarer at reguleringen og kontrollen likevel er vesentlig strengere i Europa og Norden, sammenliknet med i USA (Larsson, 2014, s 45).

Masseovervåkning med lav presisjon

Utviklingen innenfor det forebyggende sikkerhetsarbeidet generelt og ved bruk av tvangsmidler som overvåkning spesielt, kan beskrives som utfordrende og full av dilemmaer. Flere

⁵ Strafferetten er vanligvis *re-aktiv* i den forstand at handlinger kan straffes etter at de er begått. Med *pre-aktive* straffebud kan også forberedelse til bestemte handlinger straffes (Reinan, 2016, s. 3). Et eksempel på et *pre-aktivt* straffebud finner vi i straffeloven § 147a), der planlegging og forberedelse til terrorhandlinger kan straffes med inntil 12 år i fengsel.

personsensitive opplysninger om vanlige borgere samles inn. Opplysningene distribueres mellom en rekke ulike aktører. Risikoprofiler på det som antas å representere mistenkelige individer ser ut til å ha liten grad av treffsikkerhet, og tvangsmidler benyttes i større grad preaktivt for å avdekke potensielle terrorister før en eventuell hendelse finner sted. Resultatet av en slik utvikling vil kunne være at tvangsmidler i større grad også benyttes mot uskyldige individer, i den gode hensikt for å avverge fremtidige terrorangrep. Peter Bergen m.fl. (2014, s. 2 – 3) bekreftet en slik tendens da de gjennomførte en studie med dybdeanalyser av 225 rettsaker om rekruttering til terrororganisasjoner i etterkant av 11. september 2001. Trafikkdata fra den amerikanske etterretningstjenesten National Security Agency's (NSA) overvåkning av mobiltelefoner mot egne borgere, hadde bidratt til opplysning av 1,8 % av sakene. Med generell overvåkning også rettet mot utenlandske borgere var tallet 4,4 %. Det viste seg derimot at målrettede overvåkningstiltak ved bruk av arrestordre hadde bidratt i hele 48 % av sakene. I flere av sakene hadde myndighetene forsøkt å overdrive effekten av overvåkningsprogrammene, som også medførte generell overvåkning av uskyldige borgere.

Studien til Bergen m.fl. (2014, 2 – 3) konkluderer med at amerikanske etterretningsmyndigheter ikke trenger større informasjonstilgang, men at de i større grad må forstå og dele den allerede tilgjengelige informasjonen som de besitter. Informasjon som er tilegnet igjennom tradisjonelt politiarbeid og lovlige etterretningsmetoder blir ikke i tilstrekkelig grad brukt og delt med relevante samarbeidsaktører. Når det gjelder norske forhold, konkluderte også 22. juli kommisjonen med at PST må ta mer initiativ og vise større vilje til samarbeid og informasjonsdeling med andre etater, herunder også det ordinære politiet og Forsvarets Etterretningstjeneste (NOU 2012:14, s. 459).

Rasjonalet som benyttes for å legitimere mer sikkerhet og økt overvåkning, er ifølge Dragu (2011, s. 4) at kostnadene ved å feile når det gjelder forebygging av terrorangrep er uakseptabelt høy, og at forebyggingen krever mer inngripende virkemidler (Dragu, 2011, s. 4). Også Claudia Aradau og Rens van Munster (2012, s. 2) argumenterer for at moderne politikk har økende fokus på ukjente, men likevel mulige fremtidige katastrofale hendelser. Klimaendringer, ekstremvær, teknologisk sammenbrudd og «det neste terrorangrepet» er fremst når det gjelder vår kollektive oppfattelse av fremtidige katastrofer. Politikere blir ifølge Aradau og van Munster (2012, s. 2) i dag bedt om å svare på, og beslutte etter det paradoksale spørsmålet «tenk det utenkelige». I denne konteksten har viktigheten av å ta sine forhåndsregler, fokus på unngåelse, beredskap og å skape robusthet, blitt til privilegerte retningslinjer for å håndtere

fremtidige uventede hendelser. Bergen m.fl. (2014, s. 1) viser til at kun to uker etter at Edward Snowden avslørte NSAs illegale overvåkning av amerikanske borgere, gikk President Obama ut og forsvarte overvåkningsprogrammene. Ifølge Obama visste amerikanske myndigheter om minst 50 trusler som hadde blitt avverget på bakgrunn av informasjonen. Aradau & van Munster (2012, s. 8) forklarer at myndighetene i katastrofenes tidsalder har omfavnet «handlekraft» som den eneste riktige respons for å møte en usikker fremtid. Ukjente, fremtidige hendelser blir på denne måten gjort håndterbare. Forberedelser til det neste terrorangrepet skaper oppmerksomhet mot skillet mellom «normalt» og «unormalt». Det normale, uniforme, kjente og statiske blir synonymt på trygghet. Det unormale, enten det gjelder folk, gjenstander, kjøretøy, lukt, informasjon eller bilder – kan potensielt være signaler på det neste terrorangrepet.

Overvåkning for eller imot sikkerhet?

Til tross for det økte fokuset på å avdekke og å forhindre terror i etterkant av terrorangrepet mot USA den 11. september 2001, utgjør antallet europeiske ofre for terror i underkant av én prosent av det totale antall drepte i verden. Likevel er tendensen slik at det vurderes et større behov for avsperring av offentlige rom og overvåkning av befolkningen i den hensikt å forebygge forekomsten av alvorlige terrorangrep. En sentral utfordring og et paradoks i dette henseendet, er at myndighetenes erklærte hovedmål er å beskytte sine innbyggere. Likevel risikerer man at sikkerhetstiltakene kan få den motsatte effekten der borgerne opplever frykt, mistenksomhet, eksklusjon og utrygghet (Engen m.fl. 2016, s. 73 – 74). Debatten om statlig overvåkning viser seg også å være gjeldende her i Norge. I etterkant av terrorangrepet 22. juli 2011 har et normalt sikkerhetsargument blitt at overvåkingen i samfunnet må være så altomfattende at det vil gå på bekostning av andre samfunnsverdier, dersom man ønsker å forhindre soloterrorisme (Engen m.fl. 2016, s. 30 – 31). Dette til tross for at også norsk etterretningstjeneste har hatt sine utfordringer når det gjelder illegal overvåkning av norske borgere under den kalde krigen (Engen m.fl. 2016, s. 29). Paul Larsson (2014, s. 52) viser til at det i Norge har utviklet seg en situasjon hvor grensene mellom politiets forebyggende og etterforskende arbeid er utydelig. Utradisjonelle etterforskningsmetoder (skjulte og hemmelige) benyttes også til forebygging og «ren» etterretning ifølge Larsson, som blant annet har undersøkt narkotika- og organisert kriminalitet. Ettersom terror-relatert aktivitet er ansett som å være mer alvorlig enn narkotikaforbrytelser, er det sannsynlig at utviklingen som Larsson beskriver, også gjelder ved andre alvorlige kriminalitetsområder.

2.2.2 Frihet fra overvåkning

I artikkelen *The Dangers of Surveillance* fra 2013 (s. 1934) skriver jusprofessor Neil M. Richards at den digitale teknologien som har revolusjonert våre daglige liv, også har skapt presis og sanntidsoppdatert sporbarhet av våre liv. I en tid preget av terror, har myndighetene også vist en formidabel vilje til å samle disse dataene og bruke dem til ukjente formål. Ifølge Lewis (2005, s. 101) har overvåkningen flyttet seg langt utover kun de som er funnet skyldige i å begå kriminell aktivitet. Ettersom den disiplinære kontrollen har viklet seg inn i våre daglige rutiner stiller vi ikke lengre spørsmål ved den. Kontrollen utvider seg gradvis slik at flere og flere av oss plasseres inn i generaliserende overvåkningsregimer.

I kjernen av hvorfor intellektuell frihet er essensielt, finnes det ifølge Richards en normativ og en empirisk begrunnelse. Den normative viser til den angloamerikanske tradisjonen av borgerrettigheter, hvor vi finner en forpliktelse til uhindret tanke og tro. Frie borgere skal ha muligheten til å gjøre opp sine egne meninger om store og små ideer, politiske og trivielle. Ideer som omhandler sannhet, verdier og kulturer bør genereres fra bunnen av samfunnet og opp, ikke motsatt (Richards, 2013, s. 1946). Videre skriver Richards (2013, s. 1935) at et av de mest sentrale poengene er at våre samfunn mangler forståelse om hvorfor og når myndighetenes overvåkning er skadelig. For det første mener Richards at overvåkning er skadelig fordi det kan nedkjøle individenes vilje til utøvelse av fundamentale borgerrettigheter. Overvåkning kan være spesielt farlig fordi det kan føre til at mennesker ikke lengre ønsker å eksperimentere med nye, kontroversielle eller avvikende ideer. For det andre påvirker overvåkning maktbalansen mellom de som overvåker og de overvåkede. Som vi ser av argumentasjonen til Richards når det gjelder overvåkning – har den flere likhetstrekk med John Stuart Mills argumenter for å ivareta individenes grunnleggende friheter. Til tross for at samfunnet har utviklet seg i stor utstrekning på de 150 årene fra Mills til Richards levetid, kan de negative konsekvensene med hensyn til individenes frihet i stor grad sies å være de samme.

Richards viser til høyesterettsdommer Holmes som begrunnet verdien av uhindret søk for sannhet på denne måten:

When men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas – that the best test of truth is the power of the

thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out (Richards, 2013, s. 1947).

Den empiriske begrunnelsen til Richards er at overvåkning degenererer oss til det normale og kjedelige. Når vi blir overvåket, blir vi også avskrekket til å engasjere oss i tanker og handlinger som andre kan oppfatte som avvikende. Overvåkingen roter dermed til våre samfunns fundamentale forpliktelser til intellektuelt mangfold og individualitet. Frykten for å bli overvåket fører dermed til at mennesker handler og tenker annerledes enn hva vi ville gjort uten overvåkingen (Richards, 2013, s. 1948). Jeremy Benthams fengselside *The Panopticon*, har flere likhetstrekk med den empiriske begrunnelsen til Richards. I Benthams fengsel kan individet være under kontinuerlig overvåkning av fangevokteren, hvor designet fører til at den fengslede aldri vet når fangevokteren observerer vedkommende. Usikkerheten fører til at den fengslede antar at han blir overvåket til enhver tid, og justerer sin atferd deretter. På denne måten internaliseres en væremåte hos den fengslede som er selvdisciplinerende og føyelig. Slike mikro-teknikker av disiplinær makt fører til konformitet hos individene, slik at de over tid blir lydige og underdanige (Lewis, 2005, s. 101).

Frihet, overvåkning og stordata

I de senere årene har fremveksten av *stordata*⁶ ført til at både private industrier og myndigheter kan lage og analysere massive datasett. Stordata tilnærmingen gjør det mulig å skape nye slutninger som tidligere ikke har vært tilgjengelig, gjennom å koble rådata fra ulike databaser sammen i nettverk, hvor rådataene analyseres automatisk. Et sentralt element i stordata tilnærmingen er ifølge Citron & Gray (2013, s. 272) at metadata (data om data) identifiserer blant annet IP-adresse, identiteter til kontakter, steds plassering ved samtaler og meldinger, samt varighet på samtaler. Dette er data som EUs datalagringsdirektiv hadde til hensikt å pålegge tele- og internettilyderne å lagre (Graver, 2015, s. 37).

David Lyon (2014, s. 9) påpeker at stordata som konsept er særdeles viktig for informasjonsinnhenting, etterretning og overvåkning. Teknologien blir ansett som en løsning på sikkerhetsutfordringene, noe som igjen fører til et større behov for oversikt og kontroll. Ifølge Lyon må det eksistere samarbeid med private organisasjoner for at de teknologiske

⁶ Stordata er en fellesbetegnelse på datamengder som kan inneholde mye informasjon. Datamengdene er ofte store, mangartede og ustrukturerte, slik at man må benytte avanserte analysemetoder for å sette informasjonen i sammenheng, for at dataene skal gi mening (Store Norske Leksikon, 2017f).

løsningene skal kunne benyttes til myndighetenes overvåkning. På denne måten deltar flere ulike aktører i arbeidet, noe som gjør overvåkningen vanskeligere å avdekke. Ifølge Richards (2013, s. 1939 – 1940) reiser utviklingen prinsipielle og etiske utfordringer om *hvem* som skal ha tilgang på trafikkdata som EUs datalagringsdirektiv vil pålegge internettleverandørene å lagre.

Utfordringen er ikke lenger hvilken informasjon som samles, men *omfanget* av informasjon som ubetenksomt og kontinuerlig er under konstant innsamling. Ifølge Citron og Gray (2013, s. 270 – 271) er det ingen tvil om at dette er karakteristikk på en overvåkningsstat. I motsetning til dagens overvåkningsteknologi, hvor personvernutfordringene betegnes av *hvor ofte* et individ overvåkes, så vil de nye utviklede teknologiene kunne undergrave både individers mulighet for selvutvikling og dermed også deres demokratiske kultur. Fagfeltet som også betegnes *kvantitativt personvern*, begynner å få vesentlig anerkjennelse, blant annet som følge av truslene mot personvernet som representeres av store datainnsamlingsentre. I etterkant av at den tidligere NSA ansatte varsleren, Edvard Snowden, avslørte at amerikanske myndigheter urettmessig samlet inn stordata om amerikanske innbyggere, forsøkte myndighetene å underslå viktigheten av datainnsamlingen. Amerikanske myndigheters argumenter var blant annet at det kun var metadata, og at opplysningene derfor ikke var personsensitive (Lyon, 2014, s. 3).

Nancy Lewis (2005, s. 109 - 111) viser til at det kun er et spørsmål om tid før det globale sikkerhetsmiljøet deler DNA registre, grensekontrollsystemer og kriminalitetsregistre. Menneskekroppen og individet er på denne måten under press, og det utvikles i dag systemer som i større grad samler og bruker blant annet biometrisk informasjon. Tatt den hurtige teknologiske utviklingen i betraktning, kan det raskt skje før de politiske miljøene har planlagt for det. Noe overvåkning er ifølge Citron & Gray (2013, s. 272) helt essensielt, men at det går en grense for hva som kan aksepteres og innføringen av teknologier med total informasjonsbevissthet. Et sentralt spørsmål er hvordan samfunnet skal beskyttes mot den gradvise aksepten og institusjonaliseringen av slike omfattende informasjonsinnsamlingssystemer.

2.2.3 Personopplysningsvern i informasjonssamfunnet

Alessandro Acquisti (2004, s. 1) skriver at en av de største utfordringene når det gjelder personvern, er at konseptet har ulik betydning for forskjellige folk. Inkludert de akademiske

miljøene som studerer personvern. Det kan dermed reises spørsmål om det å «beskytte personvernet» dermed blir et vagt konsept. Interessegrupper har også ulike syn på mengden av personlig informasjon som skal være tilgjengelig, når ulike interesser settes opp mot hverandre. Ifølge Schartum og Bygrave har en videre begrepsforståelse festet seg, ettersom personvernsbegrepet har blitt allemannseie. Personvern i den allmenne debatten har nærmest blitt synonymt med beskyttelse av personlig integritet. Begrepet personvern benyttes i Norge for å beskrive de to ulike fenomenene privatlivets fred og kontroll med behandling av personlige opplysninger (Schartum og Bygrave, 2016, s 19). Historisk sett bygger begrepet ifølge Jon Bing på to ulike rettspolitiske fundamenter, som begge er relatert til informasjonsteknologi. Det første vokste frem som følge av massemedienes eksponering av privatlivet, slik Warren & Brandeis forklarte allerede i 1890. Det andre vokste frem som følge av databehandling, hvor formidling av personopplysninger kunne utføres med større effektivitet og utbredelse enn tidligere. Allerede i 1967 skrev Alan Westin at databehandling og økt registrering av personopplysninger medførte et press mot personvernet. Westins tilnærming er særdeles aktuell i dagens samfunn, hvor det nettopp er data- innsamling og behandling av personopplysninger som er en av de store utfordringene (Bing, 2010, s. 29).

Personopplysningsvern og databehandling

Fra og med 1970 årene var det spesielt datamaskinbehandling av personopplysninger i registre som fikk stor oppmerksomhet. Mulighetene til å samkjøre, gjenfinne, utveksle og manipulere personopplysninger var så mange og kraftige. Utviklingen har også ført til at det ikke bare er tekst, men også bilder, lyd og video med mer som lagres. I tillegg er det i dag større grad av automatisk registrering av personopplysninger ved hjelp av sensorer fremfor menneskelige vurderinger og tolkninger. GPS-sporing av personer og gjenstander, lokalisering av personer via GSM-nettet, kameraovervåkning og hastighetsmålinger er eksempler på teknologi som gjør at vi kan se deler av vår fysiske verden som et spørsmål om elektronisk behandling av persondata (Schartum & Bygrave, 2016, s. 28). Personvern i det moderne samfunn handler i større grad om en erkjennelse av at personopplysninger kan danne grunnlag for beslutninger med konsekvenser for enkeltpersoner, og dermed også for utøvelsen av makt. Av denne grunn er det behov for kontroll med innsamling, behandling og bruk av personopplysningene (Bing, 2010, s. 28).

Personvernkommisjonen (NOU 2009:1, s. 31) viser til at «personvernet har å gjøre med det moderne informasjonssamfunnets teknologi, og at det først og fremst er reaksjonen på

automatisk behandling og sammenstilling av store mengder personopplysninger som betegnes av dette ordet». Videre skriver kommisjonen at det kun er en side av personvernet i vid forstand som spesielt Datatilsynet har noe med å gjøre. Den som knytter seg til «registrering av personopplysninger i registre, og bruken av slike registre». Schartum og Bygrave (2016, s. 20) har differensiert personvernbegrepet og benytter personopplysningsvern som de mener er en mer dekkende betegnelse for beskrivelse av personvern i informasjonssamfunnet. Med personopplysningsvern mener Schartum og Bygrave «normer for behandling av personopplysninger, med sikte på å verne om personlig integritet, autonomi og privatlivets fred». Denne tilnærmingen stemmer overens med Bings definisjon av det moderne personvernet, som omhandler kontroll med behandling av personlige opplysninger.

Nå som teorien er redegjort for, vil begrepene som undersøkes (frihet, sikkerhet og personvern) samt begrepet som omhandler oppgavens kontekst (overvåkning) – knyttes opp mot sentrale deler av teorien redegjort for i kapittel 2.

3 Begrepene i undersøkelsen

Dette kapittelet vil plassere de historiske tekstene til Thomas Hobbes, John Stuart Mill og Warren & Brandeis i en mer nåtidsaktuell kontekst for denne undersøkelsen. Kapittelet vil være en brobygger mellom den historiske utviklingen hvor begrepene sikkerhet, frihet og personvern først vokste frem, og begrepenes aktualitet i dagens overvåkningssamfunn. Begrepene er sentrale for den videre datainnsamlingen som vil beskrives nærmere i kapittel 4.

3.1 Sikkerhet

Sikkerhet i denne oppgaven tar utgangspunkt i Thomas Hobbes argumentasjon for at staten (herskeren) skulle være en sikkerhets garantist igjennom samfunnskontrakten med egne borgere. Til tross for at Hobbes allerede i 1651 skrev om opprettelse av stater i hensikt å beskytte egne borgere først og fremst mot «ytre trusler og fiender», er perspektivene fremdeles relevante i dag. Den statlige organiseringen og forvaltningen av sikkerhet, har naturligvis endret seg i stor grad siden Hobbes' levetid. Likevel er statens oppgave om å sørge for borgernes sikkerhet, fortsatt en av de mest sentrale også for dagens stater. Begrepet *sikkerhet* kan defineres vidt, eksempelvis som i NOU 2016:13 (s. 34) hvor begrepet defineres som «beskyttelse mot trusler og farer som kan forårsake uønskede hendelser». En slik definisjon er vurdert som et mindre hensiktsmessig til bruk for datainnsamlingen i denne undersøkelsen. Årsaken er at definisjonen i NOU 2016:13 er svært vid, og ville ikke bidratt med tilstrekkelig avgrensning for besvarelse av oppgavens problemstilling.

En sentral aktør i å sørge for borgernes sikkerhet i Norge, er politiet. Politiet har i Norge lovfestet plikt etter politiloven til å sørge for borgernes sikkerhet. I politiloven § 1 står det at «staten skal sørge for den polititjeneste som samfunnet har behov for». Videre står det i politiloven § 2 at politiet skal «forebygge kriminalitet og andre krenkelser av den offentlige orden og sikkerhet» og «avdekke og stanse kriminell virksomhet og forfølge straffbare forhold i samsvar med regler gitt i eller i medhold av lov.» Politiet er med andre ord en vesentlig aktør i utøvelse av statens plikt i å sørge for borgernes sikkerhet. Forebygge, avdekke, stanse og forfølge (etterforske) straffbare forhold, er ulike betegnelser på polisiær aktivitet som kan omtales under fellesbetegnelse kriminalitetsbekjempelse. *Kriminalitetsbekjempelse* er i NOU 2009:15 (s. 68) definert som «den virksomhet som drives for å hindre at samfunnet og borgerne utsettes for kriminelle handlinger». Datalagringsdirektivet handler ifølge Justisdepartementet (Prop. 49L, 2010, s. 8) i sin kjerne om å sørge for at staten ved politiet har tilgjengelige

virkemidler for å sørge for borgernes sikkerhet gjennom tilstrekkelig god kriminalitetsbekjempelse. Når begrepet *sikkerhet* benyttes i denne undersøkelsen, er det *kriminalitetsbekjempelse* som definert ovenfor – som omtales, med mindre annet nevnes eksplisitt.

3.2 Frihet

Frihetsbegrepet tar i denne oppgaven utgangspunkt i John Stuart Mills og Isaiah Berlins argumentasjon. Mill (2010, s. 89 – 90) som var særdeles kritisk til undertrykkelse av enkeltindividet, mente at det kun var akseptabelt å innskrenke et individs frihet dersom vedkommende kunne mistenkes for å ha skadet andre individer. Mill (2010, s. 113 – 114) mente også at staten måtte være restriktiv med bruk av tvang for å forebygge og forhindre fremtidige kriminelle handlinger. Isaiah Berlin (1969, s. 128 – 130) skilte videre mellom positive og negative friheter, hvor det negative frihetsbegrepet var å forstå som «fravær av tvang». Berlins forståelse av negativ frihet har flere likheter med argumentasjonen til John Stuart Mill, og handler i sin kjerne om at individet har krav på å få utfolde sitt legeme, sine tanker, meninger og ytringer uten at staten skal gripe inn i individets privatliv. *Frihet* forstått som «fravær av tvang» slik Berlin definerte begrepet, er ikke avgrenset til kun å handle om fravær av statlig tvang. Eksempelvis kan det også være slik at et individ begår tvang ovenfor et annet individ. I mange tilfeller vil en slik tvangsutøvelse være å anse som kriminalitet, da det kun er staten som i bestemte tilfeller med legitimitet har mulighet til å benytte seg av tvang igjennom statens voldsmonopol (Weber, 1997, s. 3 – 4). Individer som ikke har begått eller kan mistenkes for lovbrudd, skal i utgangspunktet ikke få sine friheter ytterligere innskrenket. Staten skal som utgangspunkt dermed ikke benytte tvangsmakt ovenfor individet. I demokratiske rettsstater omtales prinsippet som uskyldspresumpsjonen, og er forankret i den europeiske menneskerettighetskonvensjonen (EMK) artikkel 6 og den norske Grunnloven § 96 (Store Norske Leksikon, 2017d).

Frihet definert som «fravær av tvang» kan oppfattes som en vid definisjon. Likevel vil det i hovedsak være *statlig tvang* ved bruk av *overvåkning* som er gjenstand for undersøkelsen, ettersom dette også utgjør undersøkelsens kontekst. Datalagringsdirektivet kan derfor betraktes som en motsetning til frihet (det å være fri) fordi direktivet ville pålagt innsamling og lagring av trafikk- og lokasjonsdata om alle norske borgere (Graver, 2015, s. 37). Fravær av tvang er

dermed vurdert som en egnet definisjon på begrepet frihet, med de avgrensninger som står beskrevet. Nyanser ved bruk av frihetsbegrepet vil fremkomme i diskusjonen (kapittel 6).

3.3 Overvåkning

David Lyon (2001, s. 2) definerer *overvåkning* som «systematisk og rutinemessig innsamling og behandling av personopplysninger med det formål å utøve innflytelse, administrasjon, styring og kontroll». Innflytelse, administrasjon, styring og kontroll ovenfor individer, kan betraktes som en motsetning til det at individene er frie. Overvåkning kan derfor etter Lyons definisjon, betraktes som et virkemiddel for å utøve tvang. I tillegg står det sentralt i definisjonen at det er personopplysninger som innsamles og behandles på en systematisk og rutinemessig måte. Med andre ord samles det inn personopplysninger, for på et senere tidspunkt å kunne utøve en form for tvang. Definisjonen viser dermed til en sentral sammenheng mellom innsamling av personopplysninger og bruk av tvangsmidler, noe som bekreftes av Bing (2010, s. 28). Overvåkning kan med andre ord forstås som et tvangsmiddel som griper direkte inn i balansen mellom verdiene frihet og sikkerhet. Når det gjelder overvåkning, så vil virkemiddelet kunne skape nedkjølende effekter på viktige demokratiske friheter som ytringsfrihet og meningsfrihet (Richards, 2013, s. 1935). I særdeleshet kan dette være tilfellet for «generell» (ikke målrettet) overvåkning av alle borgere, slik datalagringsdirektivet ville tilrettelagt for.

Begrepet *overvåkning* er ikke direkte gjenstand for datainnsamling i denne undersøkelsen. Likevel er definisjonen sentral for etablering av oppgavens kontekst og videre diskusjon om hvordan de tre undersøkte verdiene ville blitt påvirket ved innføringen av datalagringsdirektivet.

3.4 Personvern

Personvern, slik Warren & Brandeis argumenterer, har til hensikt å beskytte borgerne fra uønsket eksponering og inngrep i borgernes privatliv. Den historiske utviklingen har ifølge Schartum og Bygrave (2016, s. 19) ført til at personvern som begrep har blitt forstått på ulike måter. Ifølge Personvernkommissjonen (NOU 2009:1, s. 33) kan *personvern* ved begrepets bredeste definisjon, forstås som «å beskytte individets integritet mot overgrep». Definisjonen sammenfaller med det som ofte omtales som *personlig integritet*. Personlig integritet kan imidlertid sies å være nært beslektet med både sikkerhet- og frihetsbegrepet som benyttes i denne undersøkelsen. Eksempelvis dersom staten ikke sørger for individets sikkerhet, slik at

det blir begått kriminalitet mot et individ – kan det argumenteres for at individets integritet har blitt krenket. Det samme vil være tilfellet dersom staten urettmessig benytter tvang (eksempelvis overvåkning), mot et individ som er uskyldig.

Som nevnt omhandler datalagringsdirektivet i hovedsak innsamling og lagring av elektroniske opplysninger som kan knyttes til enkeltindivider. Begrepet *personopplysningsvern* vil derfor være mer hensiktsmessig å benytte til datainnsamlingen i denne undersøkelsen. Personopplysningsvern betraktes av Schartum & Bygrave og Personvernkommisjonen (NOU, 2009:1, s. 32) som et mer aktuelt begrep som følge av IKT teknologiens fremvekst og elektronisk lagring av personopplysninger. Begrepet personopplysningsvern defineres i NOU 2009:1 (s. 32) som «regler og standarder for behandling av personopplysninger som har ivaretagelse av personvern som hovedmål». Schartum og Bygrave (2016, s. 20) definerer begrepet som «normer for behandling av personopplysninger med sikte på å verne om personlig integritet, autonomi og privatlivets fred.» De to definisjonene ovenfor er nokså sammenfallende. Schartum og Bygraves definisjon er tolket noe videre enn personvernkommisjonens, da *normer* kan omtales som mer uformelle praksiser enn hva som er tilfellet for mer formaliserte *regler og standarder*. Eksempelvis kan det vise seg at normer (og praksiser) for behandling av personopplysninger kan være dårlige, til tross for at det finnes etablerte regler og standarder. I slike tilfeller kan det være aktuelt å hevde at personopplysningsvernet ikke er tilstrekkelig godt ivaretatt, fordi reglene ikke etterleves. Når begrepet *personvern* benyttes i denne undersøkelsen, er det definisjonene av *personopplysningsvern* ovenfor som omtales – med mindre annet er eksplisitt nevnt.

For å besvare oppgavens problemstilling, er det nødvendig å gjennomføre datainnsamling og analyse av tekstmaterialet fra stortingsdebatten den 4. april 2011 og de syv partiprogrammene fra 2009. Innholdsanalyse er vurdert som en egnet fremgangsmåte for å kartlegge og analysere i hvilket omfang og hvordan de politiske partiene omtaler verdiene frihet, sikkerhet og personvern i både partiprogram og under stortingsdebatten.

4 Metode

Det empiriske datagrunnlaget til bruk i denne undersøkelsen er samlet inn ved bruk av kvalitativ metode. Innholdsanalysen representerer en systematisk fremgangsmåte som egner seg til å kartlegge kvalitative data, både med og uten kvantitativ tilnærming. På denne måten kan innholdsanalysen bidra til å kartlegge omfang og utbredelse, samtidig som metoden ivaretar dybde og kvalitet. Både induktiv og deduktiv fremgangsmåte er benyttet for innsamling og tolkning av undersøkelsens datamateriale.

Datainnsamlingen har vært gjennomført i to deler, hvor den første har omhandlet kvantitativ innholdsanalyse av referatet fra stortingsdebatten. Den andre delen omhandler kvalitativ innholdsanalyse av stortingspartienes partiprogrammer. Del én om stortingsdebatten er mest omfattende og vil beskrives mest inngående, da den kvantitative innholdsanalysen ifølge Øyvind Bratberg (2014, s. 85) stiller noe større krav til beskrivelse av fremgangsmåte, sammenliknet med den kvalitative innholdsanalysen.

Metodekapittelet vil også beskrive hvordan undersøkelsene er gjennomført, prosedyrer for tolkning av datamaterialet og øvrige problemstillinger rundt dataenes pålitelighet (reliabilitet) og gyldighet (validitet).

4.1 Innholdsanalyse

Innholdsanalyse defineres av Klaus Krippendorf (2004, s. 14) som «analysis of the manifest and latent content of a body of communicated material through classification, tabulation, and evaluation of its key symbols and themes in order to ascertain its meaning and probable effect.»

Innholdsanalyse er en forskningsteknikk for å fremstille pålitelige og gyldige slutninger fra tekst eller annet meningsfullt materiale som forstås i den *kontekst* som materialet befinner seg i (Krippendorf, 2004, s. 18). Ifølge Øyvind Bratberg (2014, s. 84) viser innholdsanalyse til enhver analyse som systematisk sammenfatter tekstinhold. Innholdsanalysen favner ifølge Bratberg både om kvalitative og kvantitative teknikker. Metoden kan betraktes som et egnet utgangspunkt for denne undersøkelsen, ettersom referatet fra stortingsdebatten og partiprogrammene er meningsbærende tekst. Den kvantitative tilnærmingen vil benyttes for undersøkelse av stortingsdebatten og vil bidra til å identifisere trender og mønstre i teksten. Den kvalitative innholdsanalysen vil egne seg til å analysere både partiprogrammene i lys av de

etablerte definisjonene frihet, sikkerhet og personvern, og for å utdype funnene fra den kvantitative innholdsanalysen av stortingsdebatten.

4.2 Datautvalg og datakilder

Ifølge Thagaard (2014, s. 58) er en viktig avveining i undersøkelsen å vurdere behovet for å utvikle nye data fra felten, eller benytte allerede foreliggende data. I denne undersøkelsen vil allerede foreliggende data benyttes. Partiprogrammene til de syv politiske partiene for stortingsperioden 2009 – 2013 og referatet fra stortingsdebatten den 4. april 2011, vil benyttes som kildemateriale. Fordelen med å benytte allerede eksisterende data, er at de er etablert uavhengig av forskerens medvirkning. Tekstene gir dermed uttrykk for hvordan det enkelte politiske parti, eller den enkelte stortingsrepresentant, presenterer seg selv og sine budskap i den kontekst som vedkommende befinner seg i.

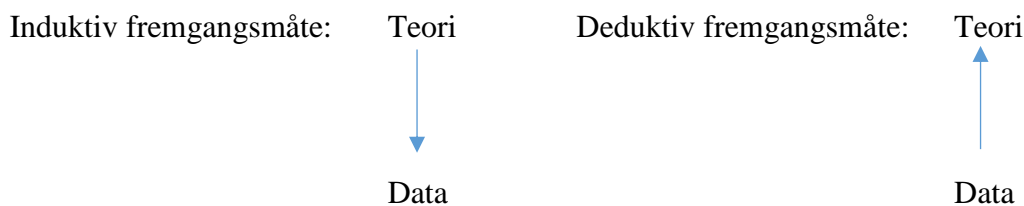
En sentral problemstilling med bruk av allerede foreliggende data, er at dataene er laget for et annet formål enn den undersøkelsen som nå utføres. Dataene kan derfor kreve større grad av tolkning. De empiriske datakildene som er benyttet i denne undersøkelsen er ved gjennomlesning vurdert til å være egnet for å besvare oppgavens problemstilling. Det er vurdert som mindre hensiktsmessig å innhente ytterligere data, ettersom oppgaven er avgrenset til å undersøke hvordan stortingspolitikere uttrykker seg under stortingsdebatten og hvordan partiprogrammene kan bidra til å forklare disse funnene.

4.3 Induktiv og deduktiv metode

Denne undersøkelsen er gjennomført ved bruk av både deduktiv og induktiv metode. Innledningsvis ble deduktiv metode benyttet til å etablere definisjoner for de tre kategoriene frihet, sikkerhet og personvern. Problemstillingen som skal besvare hvordan de politiske partiene på stortinget mente at datalagringsdirektivet ville påvirket verdiene frihet, sikkerhet og personvern – forutsetter at de tre begrepene defineres. Definisjoner av de nevnte begrepene er fastsatt i kapittel 1.2, og en nærmere redegjørelse for valg av begreper er beskrevet i kapittel 3. Kapittel 3 har til hensikt å synliggjøre hvorfor de utvalgte begrepene er spesielt aktuelle og relevante for konteksten til denne undersøkelsen.

En deduktiv tilnærming er benyttet etter at dataene fra det empiriske materialet ble innsamlet og analysert. Etter at datainnsamlingen var gjennomført og undersøkelsen utviklet seg, var det

behov for å finne ytterligere faglitteratur som kunne bidra til å forklare funnene. Den deduktive fremgangsmåten har på denne måten bidratt til å styrke undersøkelsens gyldighet, ved at relevant teori oppsøkes på bakgrunn av dataene som har fremkommet. Thagaard (2014, s. 31) fremhever at kvalitative metoder kjennetegnes av et fleksibelt forskningsopplegg. Datainnsamling og analyse bør derfor foregå parallelt slik at forskeren kan tilpasse den videre datainnsamlingen til tidligere analyser av materialet. En slik tilnærming er også benyttet ved utarbeidelse av denne undersøkelsen.



Figur 2: Fremstilling av induktiv og deduktiv fremgangsmåte

4.4 Reliabilitet og validitet

To sentrale krav ved bruk av innholdsanalyse er ifølge Krippendorf (2004, s. 19) *reliabilitet* (pålitelighet) og *validitet* (gyldighet). Innholdsanalysen må være pålitelig, den skal helst kunne reproduseres av andre, og slutningene må være gyldige. For at et forskningsresultat skal kunne reproduseres, må det være tydelig styrt av regler som eksplisitt er uttalt og benyttet på samme måte ved alle enheter i analysen. På denne måten skal andre individer ideelt sett kunne gjenta samme undersøkelse, og komme frem til en tilsvarende konklusjon ved bruk av samme datamateriale og undersøkelsesmetodikk. De neste kapitlene (4.1.4, 4.1.5 og 4.1.6) redegjør for fremgangsmåten i undersøkelsen, slik at den metodiske tilnærmingen er tilgjengelig for leseren.

Når det gjelder validitet, så handler dette om hvor stor grad av gyldighet undersøkelsen innehar, og dermed hvor stor grad av sannhet som undersøkelsen kan sies å representere (Krippendorf, 2004, s. 212). For at undersøkelsen skal være gyldig, må den også kunne møte eksterne kriterier, som blant annet kan finnes i annen forskning. Krippendorf (2004, s. 19) påpeker likevel utfordringene med å ivareta både pålitelighet og gyldighet ved bruk av innholdsanalyse. Pålitelighet garanterer nemlig ikke gyldighet, og i søken etter høy pålitelighet kan gyldighet ha en tendens til å svekkes. Dilemmaet når analytikerens må velge mellom interessante, men ikke-reproduserbare intellektuelle tolkninger og overforenklede, men reproduserbare analyser – tydeliggjør dette skillet. Innholdsanalysen bør derfor ta sikte på å etablere pålitelige prosedyrer med forsiktighet, samtidig som den forsøker å ivareta intellektuelle tolkninger (Krippendorf,

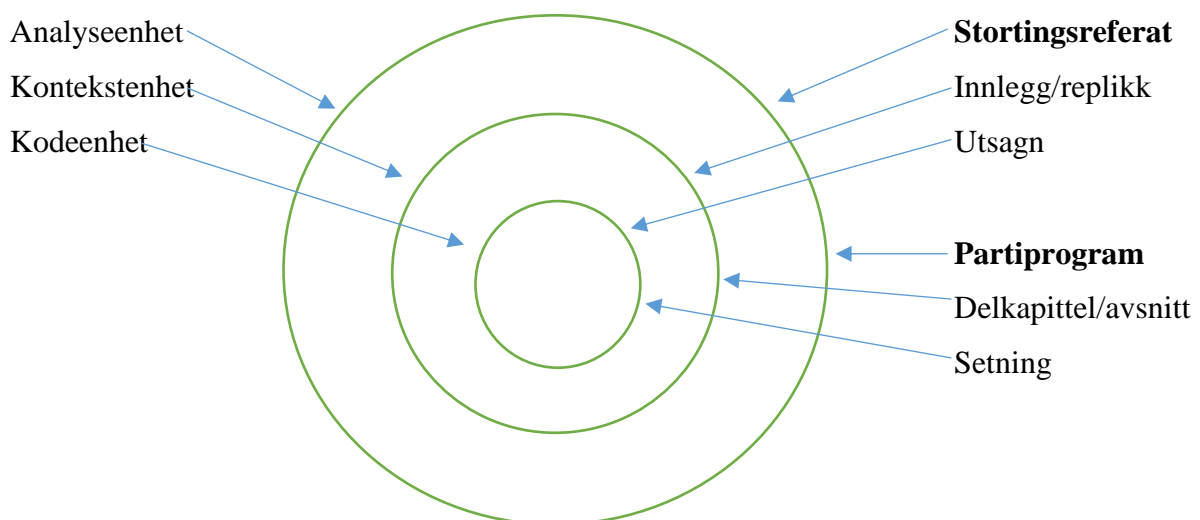
2004, s. 214). I denne undersøkelsen har det vært viktig for oppgavens repliserbarhet å etablere gjennomtenkte og relevante definisjoner på frihet, sikkerhet og personvern. Beskrivelse av fremgangsmåten for gjennomføring av den kvantitative innholdsanalysen av stortingsdebatten i kapittel 4.1.5 er også sentralt for undersøkelsens repliserbarhet.

Det har underveis ved datainnsamling i innholdsanalysen fremkommet informasjon som kunne ha vært relevant for oppgaven – men som ikke tilfredstilte de etablerte definisjonene. Eksempelvis har dette vært tilfellet når begrepet personvern enkelte ganger har blitt benyttet av representantene under stortingsdebatten. Et eksempel på begrepsunøyaktigheten kan leses av sitatet nedenfor. Eivind Sivertsen (AP), uttaler at for han er personvern det samme som sikkerhet, i tråd med denne oppgavens definisjoner. For at begrepsunøyaktigheter som dette ikke skal påvirke undersøkelsens gyldighet, vil problematikken synliggjøres og diskuteres nærmere under oppgavens diskusjonsdel.

For meg handler ikke personvern bare om beskyttelse mot overvåking og at opplysningene kan komme på avveie. Personvern handler for meg også om at innbyggerne beskyttes mot grov kriminalitet (Stortinget, 2011, s. 3241).

4.5 Analyseenheter, kodeenheter og kontekstenheter

Krippendorff deler det empiriske datamaterialet innholdsanalysen inn i tre ulike nivåer. *Analyseenheter*, *kodeenheter* og *kontekstenheter*. Figuren nedenfor viser hvordan de tre enhetene henger sammen generelt (til venstre), og i denne undersøkelsen spesielt (til høyre).



Figur 3: Analyseenheter, kontekstenheter og kodeenheter i denne undersøkelsen

Analyseenheter er den overordnede enheten som er selektivt utvalg for å inngå i analysen. Eksempelvis kan en bestemt sak, i en bestemt avis, for en bestemt periode, være et utvalg som tilfredsstillende kriteriene til analyseenheten (Krippendorf, 2004, s. 98). I denne undersøkelsen vil analyseenheten være stortingsreferatet eller hvert enkelt av partiprogrammene. Det er innholdet i stortingsreferatet og partiprogrammene som vil analyseres nærmere, slik at analyseenheten er avgrenset til kun å gjelde de nevnte dokumentene.

Kodeenheter er enheter som vanligvis skiller seg fra hverandre basert på hvilken kategori enheten plasseres inn i. Kodeenheten befinner seg inne i analyseenheten (stortingsreferat/partiprogram) – men overskrider aldri analyseenhetens grenser. Det spesifikke innholdet som karakteriserer en bestemt setning, tekst eller utsagn, bidrar til å plassere kodeenheten i en bestemt kategori (Krippendorf, 2004, s. 99). I denne undersøkelsen vil derfor ethvert *utsagn* under stortingsdebatten eller *setning* i partiprogrammet, være å anse som kodeenheter. Kodeenheten må videre tilfredsstillende en av definisjonene (frihet, sikkerhet eller personvern) som er relevante for datainnsamlingen.

Kontekstenheter er grenser for hvilken informasjon som skal vurderes til å tilfredsstillende kodeenhetene. Eksempelvis kan en bestemt setning som i utgangspunktet ikke tilfredsstillende de fastsatte kriteriene, likevel oppfattes som en kodeenhet. Fordi konteksten som den bestemte setningen befinner seg i, også vil påvirke hvordan setningen skal forstås. Setningen kan dermed tolkes inn blant en av kodeenhetene (Krippendorf, 2004, s. 101). I denne undersøkelsen vil kontekstenhetene under stortingsdebatten være å anse som et hvert innlegg eller replikk som representantene fremsetter. I partiprogrammene vil det være delkapitlene og avsnittene som utgjør kontekstenhetene. Den enkelte kodeenhet (utsagn/setning) må altså betraktes i lys av kontekstenheten (innlegg/replikk eller delkapittel/avsnitt) når det vurderes hvorvidt utsagnet tolkes til å være innenfor eller utenfor de etablerte definisjonene. Det vil nå redegjøres for hvordan analyse av stortingsdebatt og partiprogram er gjennomført.

4.6 Innholdsanalyse av stortingsdebatten

Innholdsanalysen kan som kvantitativ teknikk måle forekomsten av bestemte elementer i teksten gjennom å tallfeste elementene og deretter gjennomføre statistisk analyse. På denne måten kan ulike mønstre i teksten påvises. En underliggende ambisjon ved bruk av kvantitativ

innholdsanalyse er ifølge Bratberg (2014, s. 84) å trekke slutninger til forhold også utenfor det teksten omtaler direkte. Ettersom kvantitativ innholdsanalyse i hovedsak er en metode innenfor den kvalitative sjangeren, legger fremgangsmåten vekt på forskerens egne fortolkninger. Likevel kan det hevdes at den kvantitative fremgangsmåten stiller noe større krav til reliabilitet og validitet sammenliknet med andre kvalitative metoder innenfor sjangeren av tekst- og dokumentanalyse (Bratberg, 2014, s. 85). Fordi kvalitative og kvantitative tilnærminger i hovedsak gir ulike typer data, kan det ifølge Thagaard (2014, s. 18) være fordelene ved å kombinere begge typer av metoder innenfor samme forskningsprosjekt.

I denne undersøkelsen er det etablert tre hovedkategorier (frihet, sikkerhet og personvern) i tråd med oppgavens problemstilling. Ettersom problemstillingen har til hensikt å måle hvordan stortingspolitikerne mener at de tre nevnte verdiene påvirkes, må det også etableres underkategorier som synliggjør stortingspolitikernes normative⁷ standpunkt. Under hver av de tre hovedkategoriene frihet, sikkerhet og personvern er underkategoriene *svekket*, *styrket* og *nøytral*, etablert. De tre normative underkategoriene vil dermed bidra til å synliggjøre stortingspolitikernes *vurderinger* av hvordan de tre undersøkte verdiene ville blitt påvirket.

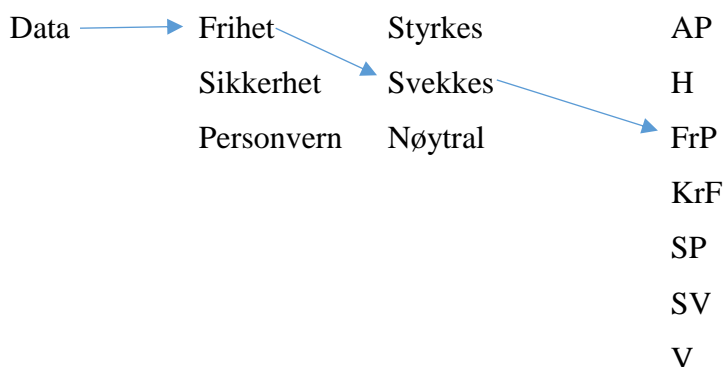
Datamaterialet vil tolkes inn under ni forhåndsdefinerte kategorier per politiske parti, som er betraktet som et egnet utgangspunkt for å besvare oppgavens problemstilling. Totalt gir dette 63 mulige kategorier for datainnsamlingen. Til tross for at de 63 kategoriene kan oppfattes som mange, har det vært slik at partiene har uttrykt seg relativt konsistent. Dermed har ikke antallet kategorier representert noen vesentlig utfordringer. Mange kategorier kan i dette tilfellet betraktes som en styrke ved undersøkelsen, fordi den er gjennomført med et en «åpen» og «bred» tilnærming. I tillegg kan flere kategorier bidra til å gi en mer nyansert og nøyaktig besvarelse av oppgavens problemstilling.

Eksempel på et utsagn fra FrP som er tolket i kategorien frihet svekkes, finner vi nedenfor:

Norge trenger ikke EUs datalagringsdirektiv. Norge trenger ikke mer overvåkning av sine borgere. Norge trenger styrking av personvernet. Norge trenger mer effektiv innsats mot terror og organisert kriminalitet. Det kan og bør gjøres uten datalagringsdirektivet (Stortinget, 2011, s. 3223).

⁷ Begrepet *normativ* beskriver utsagn som innebærer en subjektiv vurdering og derfor er av en rettleidende art. Motsetningen til *normativ* er *deskriptiv* som beskriver de faktiske forhold. (Store Norske Leksikon, 2017c).

Utsagnet ovenfor har dermed blitt kategorisert på følgende måte:



Samtlige innlegg har vært analysert og kategorisert basert på fremgangsmåten som er beskrevet.

Datainnsamlingen ble gjennomført ved å analysere de 105 innleggene og 114 replikkene (219 kontekstenheter) som ble fremsatt under stortingsdebatten. Totalt ble det samlet inn 281 kodingsenheter, hvorav 184 kodingsenheter fra de 105 innleggene og 197 kodingsenheter fra de 114 replikkene. Kodingsenhetene utgjør en eller flere setninger i teksten, og er kategorisert ved hjelp av analyseprogrammet Nvivo Pro 11⁸.

Tabell 1 viser resultatet etter at utsagnene som har fremkommet i stortingsdebatten ble analysert og kategorisert basert på variablene *parti* (7 stk), *verdi* (3 stk) og *standpunkt* (3 stk). I tillegg er antallet *utsagn* og antallet *innlegg/replikker* fra hvert parti, synliggjort til høyre i tabellen.

Tabell 1: Datainnsamling fra stortingsdebatten

Verdi	Frihet			Personvern			Sikkerhet			Utsagn	Innlegg/replikker
Parti	Nøytral	Svekkes	Styrkes	Nøytral	Svekkes	Styrkes	Nøytral	Svekkes	Styrkes		
AP	21	4	1	2	0	31	3	0	29	91	69
FrP	1	26	0	0	9	0	7	12	1	56	38
H	9	5	1	0	1	13	1	0	20	50	39
KrF	0	9	0	0	1	1	2	2	0	15	18
SP	0	16	0	3	5	3	5	3	0	35	26
SV	1	14	0	1	6	1	1	1	0	25	21
V	0	4	0	0	2	0	1	2	0	9	8
Total	32	78	2	6	24	49	20	20	50	281	219

⁸ Nvivo Pro 11 er lastet ned fra UiS' nettsider. Informasjon om analyseverktøyet fra produsenten: <http://www.qsrinternational.com/nvivo-product/nvivo11-for-windows/pro>

Datainnsamlingen er kvalitetssikret ved å gjennomføre den beskrevne prosedyren to ganger, og deretter er hvert enkelt utsagn igjen kvalitetssikret, enkeltvis. Ved kvalitetssikringen ble åtte utsagn fjernet, og ytterligere to utsagn lagt til etter en nærmere vurdering av utsagnene.

4.6.1 Metodiske problemstillinger

Hvert enkelt innlegg (eller replikk) under stortingsdebatten kan inneholde flere utsagn som kan tolkes innenfor en og samme kategori. Det er derfor valgt å være konsekvent og kun tillatte maksimalt en kodingsenhet innenfor hver av kategoriene, per innlegg. Dette gjøres for at innlegg fra representanter som gjentar seg selv flere ganger i ett og samme innlegg, ikke skal gi flere utslag enn representanter som er kortere og mer konsise i sine innlegg. Dersom en representant uttrykker seg på en slik måte at det verken er mulig å identifisere hvorvidt vedkommende mener direktivet bidrar til *styrking* eller *svekking*, kategoriseres innlegget som *nøytralt*. Ved tvilstilfeller valgte jeg å avstå fra å kategorisere utsagn som gav liten eller ingen indikasjon på hvilken kategori utsagnet burde befinne seg i. I oppgavens diskusjonsdel (kapittel 6) vil sitater som er kategorisert i de ulike underkategoriene (styrkes, svekkes og nøytral), presenteres fortløpende.

Når det gjelder bruk av referat fra stortingsdebatter som analyseenhet, så vil antallet innlegg under stortingsdebatten fra hvert enkelt politiske parti – påvirkes av det totale antallet representanter som partiet har i Stortinget for øvrig. Partier med flere representanter på Stortinget vil derfor kunne fremføre flere innlegg i en og samme debatt. For å utjevne de metodiske utfordringene når det gjelder ulikhet i antallet innlegg fra partiene, har jeg valgt å konvertere om kodingsenhetene (utsagn) fra antall til prosent. Kodingsenhetene vises dermed som prosentvis fordeling. Det blir på denne måten enklere å sammenlikne de ulike partiene.

Tabellene nedenfor viser antall utsagn per parti, konvertert til prosent (for det enkelte partiet) i to av kategoriene som undersøkes (frihet svekket og sikkerhet styrkes). Den øverste tabellen (tabell 2) viser antall, den nederste tabellen (tabell 3) viser prosent, etter konverteringen.

Tabell 2 (antall) og 3 (prosent): Konvertering av stortingsdebatten fra antall utsagn til prosent

Parti	Totalt antall	Frihet svekkes	Sikkerhet styrkes
AP	91	4	29
H	50	5	20
FrP	56	26	1
KrF	15	9	0
SP	35	16	0
SV	25	14	0
V	9	4	0
Total	281	78	50

Parti	Totalt antall	Frihet svekkes	Sikkerhet styrkes
AP	100 %	4 %	32 %
H	100 %	10 %	40 %
FrP	100 %	46 %	2 %
KrF	100 %	60 %	0 %
SP	100 %	46 %	0 %
SV	100 %	56 %	0 %
V	100 %	44 %	0 %
Total	100 %	28 %	18 %

Replikker under stortingsdebatten kan være preget av den enkelte stortingsrepresentants ønske om å kommentere et forutgående innlegg. Dette ser ikke ut til å ha medført noen vesentlige utfordringer for datainnsamlingen. Antallet innlegg fra hvert enkelt parti, tidsdisponering og replikkfordeling styres av Stortingets egne retningslinjer (Stortinget, 2016). Dersom datagrunnlaget er lite i enkelte av kategoriene, vil det kommenteres ved presentasjon av funnet.

En kvalitativ analyse av utsagnene fra stortingsdebatten er utført etter den kvantitative innholdsanalysen. Den kvalitative analysen gjennomføres ved å vise til utsagn og sitater som bidrar til å forklare funnene fra den kvantitative innholdsanalysen. Sitatene som har til hensikt å gi en mer presis besvarelse av problemstillingen, vil presenteres løpende i diskusjonen. De kvalitative vurderingene som er gjennomført i analysen er synlig i kapittel 6.

4.7 Innholdsanalyse av partiprogrammene

Kodingen i innholdsanalysen består ifølge Krippendorf, (2004, s. 220) som nevnt av transkribering, kategorisering og tolkning av bestemte enheter. Ved analyse av partiprogrammene (*analyseenheter*), vil hvert enkelt delkapittel eller avsnitt i

partiprogrammene utgjøre *kontekstenhetene*. Kontekstenhetene må inneholde informasjon som er relevant i lys av de etablerte definisjonene (frihet, sikkerhet, personvern), dersom de skal benyttes til datainnsamling. Videre vil det være *setninger* som bidrar til besvarelse av oppgavens problemstilling, som vil utgjøre *kodingsenhetene*.

En normativ kartlegging (svettes, styrkes, nøytral) som gjennomføres ved analyse av stortingsdebatten, vil ikke gjennomføres ved analyse av partiprogrammene. Årsaken er at de politiske partiene i hovedsak kun skriver om *hva* de ønsker å få til. I liten grad skriver partiene spesifikt om hvordan datalagringsdirektivet ville påvirket verdiene som undersøkes. Partiprogrammene kan dermed kreve noe større grad av tolkning sammenliknet med analyse av stortingsdebatten. Det er derfor vurdert som mer hensiktsmessig å kartlegge *i hvilket omfang* partiene omtaler de tre verdiene (frihet, sikkerhet og personvern). Tversky & Kahnemann (1981, s. 453) viser til at beslutninger påvirkes av måten ulike problemstillinger formuleres på. Ifølge Tversky & Kahnemann er det mulig å forutse handlingsalternativer, basert på måten beslutningsproblemet fremføres på. Ettersom partiprogrammene er en forpliktelse mellom velgerne og det politiske partiet, er det naturlig at omfanget og måten de tre verdiene (frihet, sikkerhet og personvern) omtales på i partiprogrammene – også legger føringer for partienes vurderinger under stortingsdebatten.

Tabell 4 bidrar til en oversikt over omfanget de ulike partiene omtaler de tre verdiene i sine partiprogrammer. På denne måten kan graden av omtale fra de politiske partiene, enkelt sammenliknes. Tabellen viser resultatet av kodingen ved hjelp av fremgangsmåten som er beskrevet ovenfor og er kategorisert basert på variablene *parti*, *verdi* og *grad av omtale*. Graden av omtale som det politiske partiet gir til verdiene i partiprogrammet, kategoriseres etter skalaen *ingen (rød)*, *lite (oransje)*, *noe (gul)* eller *mye (grønn)* omtale.

Tabell 4: Datainnsamling fra partiprogrammene

Verdi	Frihet	Sikkerhet	Personvern
Dokument	Partiprogram	Partiprogram	Partiprogram
AP	Lite omtale	Noe omtale	Ingen omtale
Høyre	Noe omtale	Mye omtale	Mye omtale
FrP	Mye omtale	Mye omtale	Noe omtale
KrF	Noe omtale	Mye omtale	Noe omtale
SP	Mye omtale	Noe omtale	Mye omtale
SV	Mye omtale	Lite omtale	Noe omtale
Venstre	Mye omtale	Noe omtale	Mye omtale

Skalaen (ingen, lite, noe og mye) er basert på omfanget den enkelte av de tre verdiene har blitt omtalt, og innebærer en kvalitativ vurdering av innholdet i partiprogrammene. Ettersom analysen er kvalitativ, vil det i hovedsak være *hva* de politiske partiene skriver om verdiene, og tolkningen av dette – som er mest interessant. Hva partiene skriver kan leses i kapittel 6, og vil bidra til å besvare problemstillingen om *hvordan* partiprogrammene kan bidra til å forklare politikernes syn under stortingsdebatten.

4.7.1 Metodiske problemstillinger

Partiprogrammene er vesentlig ulikt oppbygget fra parti til parti, noe som gjør det utfordrende å ha en helt identisk tilnærming til analyse og datainnsamling fra samtlige partiprogrammer. Ved at oppgaven forholder seg til de etablerte definisjonene av begrepene frihet, sikkerhet, personvern og overvåkning for undersøkelsen, har datainnsamlingen likevel blitt gjennomført med en forholdsvis enhetlig tilnærming. Fremgangsmåten er i tråd med hva Krippendorf (2004, s. 19) påpeker som viktig for å ivareta undersøkelsens gyldighet ved å møte eksterne kriterier satt av annen forskning.

4.8 Fremstilling av data

En oversikt over funnene i undersøkelsen, og sammenlikning av de ulike partienes standpunkt – vil presenteres kort i kapittel 5. I kapittel 6, som også utgjør oppgavens diskusjonsdel, vil funnene presenteres mer inngående fordelt på hvert enkelt parti. Funnene vil presenteres tematisk, hvor hvert enkelt av de syv partiene har sitt eget delkapittel. Ved presentasjon av funnene, vil det benyttes tabeller og grafer for å fremstille dataene på en lett forståelig måte for leseren. En slik temasentrert tilnærming innebærer ifølge Thagaard (2014, s. 181) at informasjon om hvert enkelt tema studeres hver for seg, hvor hovedpoenget er å gå i dybden på de enkelte temaene. Innenfor hvert enkelt parti, vil funnene fra hver av de tre verdiene som undersøkes (frihet, sikkerhet og personvern), diskuteres i eget underkapittel. Her vil partienes standpunkt under stortingsdebatten sammenliknes med hva det samme partiet skrev i eget partiprogram for perioden. På denne måten diskuteres funnene fra de ulike kildene opp imot hverandre, i lys av den introduserte teorien – for å besvare oppgavens problemstilling.

Med bakgrunn i de beskrevne fremgangsmåtene, vil noen sentrale funn fra innholdsanalysene nå presenteres.

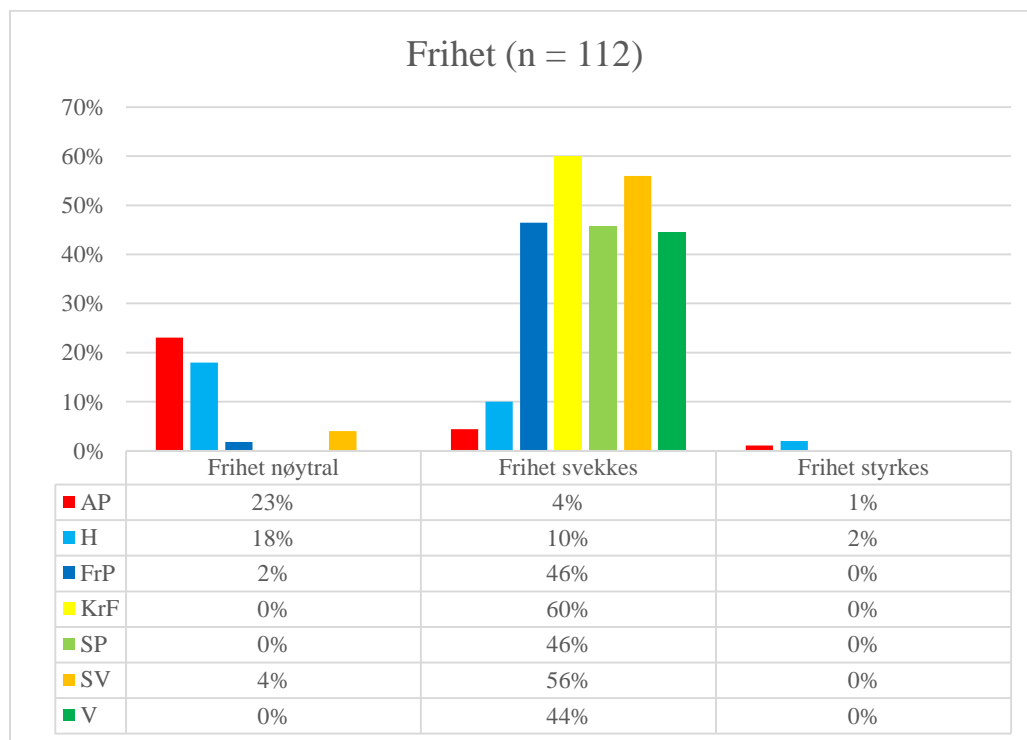
5 Empiriske funn fra innholdsanalysene

Funnene som har fremkommet gjennom innholdsanalysene vil oppsummeres og presenteres kort. Kapittelet vil gi en oversikt og dermed også et grunnlag for sammenlikning mellom hvordan de ulike partiene har uttrykt seg under stortingsdebatten og i sine partiprogrammer. En mer detaljert beskrivelse av hva hvert enkelte parti har uttrykt, presenteres i kapittel 6.

5.1 Kvantitativ innholdsanalyse av stortingsdebatten

Ved analyse av stortingsdebatten fra 4. april 2011, fremkom det med tydelighet at det er to meningsbærende sider i saken om innføringen av datalagringsdirektivet. AP og Høyre stilte seg positive til lovforslaget, mens FrP, KrF, SP, SV og Venstre stilte seg negative. Voteringen over lovforslaget avslutningsvis i stortingsdebatten, bekrefter dette (Stortinget, 2011, s. 3269). Til tross for at det i hovedsak var to meningsbærende sider, fremstår partienes standpunkter likevel noe mer nyanserte når innholdet analyseres nærmere.

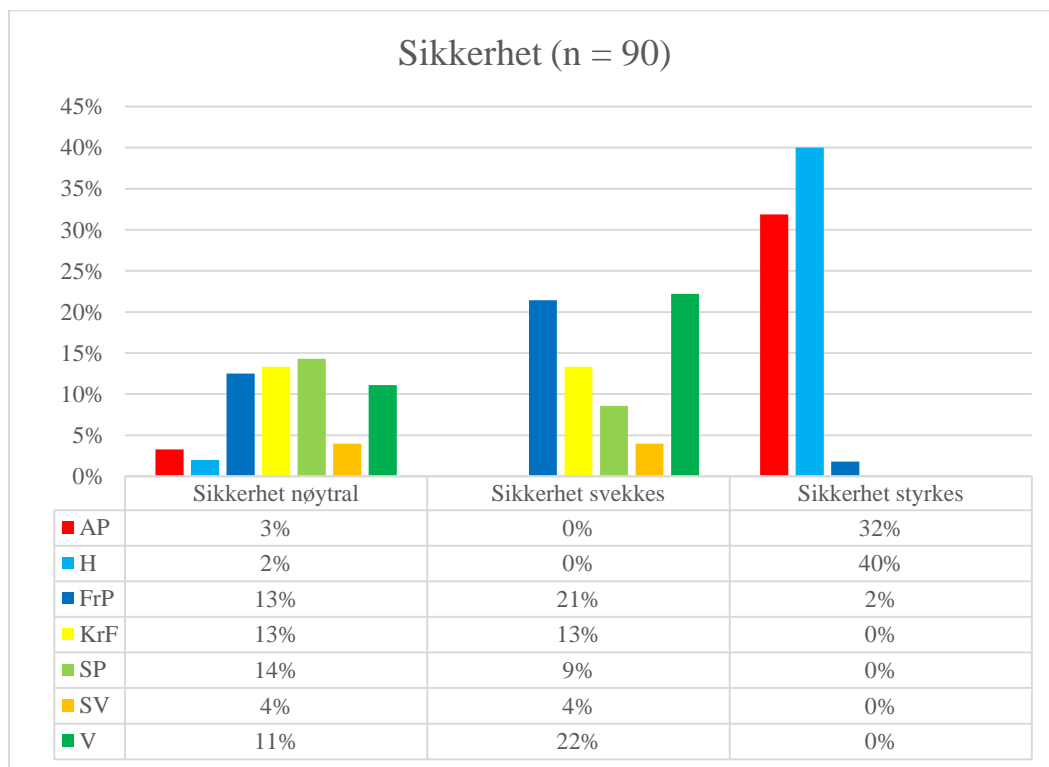
Den kvantitative analysen av stortingspartienes utsagn om verdien frihet, viser at AP og Høyre mener direktivet ville forholdt seg nøytralt til verdien. SP, KrF, FrP, SV og Venstre uttrykker derimot at direktivet i stor grad ville svekket frihet. Graf 1 nedenfor viser hvordan partiene fordeler seg på skalaen nøytral, svekkes og styrkes, med hensyn til verdien.



Graf 1: Frihet

Hvordan de ulike partiene har uttrykt seg for at resultatene i analysen har blitt som i grafene, presenteres i kapittel 6. Der vil funnene innenfor hvert av de syv stortingspartiene presenteres og diskuteres i lys av oppgavens problemstilling.

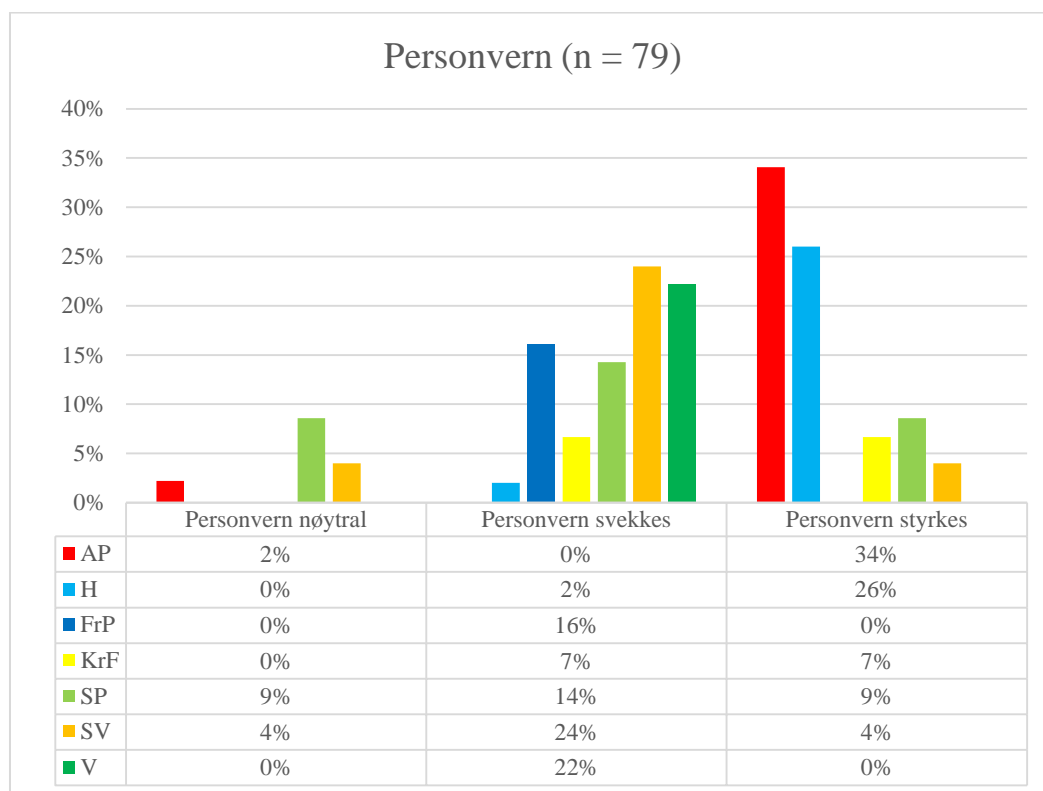
Når det gjelder verdien sikkerhet, viser graf 2 nedenfor at AP og Høyre mener at verdien ville blitt styrket med innføringen av datalagringsdirektivet. På den motsatte siden viser grafen at FrP og Venstre mener at datalagringsdirektivet vil føre at sikkerheten svekkes. KrF og SP uttrykker at direktivet både vil svekke og forholde seg nøytralt til verdien sikkerhet. KrF har imidlertid noe høyere andel utsagn i kategorien sikkerhet svekkes sammenliknet med SP. SV uttrykker i liten grad hvordan direktivet ville påvirket verdien sikkerhet, da datagrunnlaget er svært lavt. Likevel tyder SVs utsagn på at de i større grad uttrykker at sikkerheten vil svekkes eller forholde seg nøytralt fremfor at verdien vil styrkes.



Graf 2: Sikkerhet

Mønsteret som fremkommer fra partienes standpunkter når det gjelder verdien personvern, skiller seg imidlertid noe fra frihet og sikkerhet. Når det gjelder personvern, viser graf 3 at partienes utsagn i stor grad korrelerer med partiets øvrige syn når det gjelder frihet og sikkerhet, med unntak av partiene SP og KrF. For AP og Høyres del, som uttrykte at sikkerheten ville

styrkes med innføringen av datalagringsdirektivet, uttrykker de også at personvern vil styrkes. FrP, SV og Venstre uttrykker at både frihet og personvern vil svekkes. SP har en noe annerledes tilnærming hvor partiet uttrykker at *enkelte deler* i direktivet vil bidra til å styrke personvernet, samtidig som at andre vil bidra til å svekke personvernet, og KrF omtaler i mindre grad hvordan personvernet ville blitt påvirket. Både SP og KrF er derfor tolket i retning av at de mener datalagringsdirektivet vil forholde seg nøytralt til verdien personvern.



Graf 3: Personvern

Partienes standpunkter under diskusjonen om datalagringsdirektivet oppsummeres i tabell 5:

Tabell 5: Oppsummering av partienes standpunkt under stortingsdebatten

Verdi	Frihet	Sikkerhet	Personvern
Dokument	Stortingsdebatten	Stortingsdebatten	Stortingsdebatten
AP	Nøytral	Styrkes	Styrkes
Høyre	Nøytral	Styrkes	Styrkes
FrP	Svekkes	Svekkes	Svekkes
KrF	Svekkes	Svekkes/nøytral	Ingen påvirkning
SP	Svekkes	Nøytral/svekkes	Nøytral/svekkes
SV	Svekkes	Ingen påvirkning	Svekkes
Venstre	Svekkes	Svekkes	Svekkes

Funnene som presenteres i graf 1, 2 og 3, samt tabell 5 i dette kapittelet, tyder på at stortingsdebatten kan betegnes som konfliktfylt. Innholdsanalysen som er gjennomført, viser at partiene *for* innføringen (AP og Høyre) betraktet virkningene av datalagringsdirektivet vesentlig annerledes enn partiene som var imot innføringen (FrP, KrF, SP, SV og Venstre). Funnene fra innholdsanalyse av partiprogrammene vil nå presenteres kortfattet.

5.2 Kvalitativ innholdsanalyse av partiprogrammene

Ved datainnsamling og analyse av partiprogrammene fra 2009, fremkom det med tydelighet at det var svært varierende i hvilken grad partiene omtalte de tre verdiene frihet, sikkerhet og personvern. Det var også variabelt hvorvidt partiene omtalte de nevnte verdiene i konteksten *overvåkning*, som er undersøkelsens hovedanliggende. Eksempelvis skriver AP flere steder om frihet i partiprogrammet, men hvor det samtidig fremgår at det i all hovedsakelig er det Isaiah Berlin (1969, s. 128 – 130) omtaler som positive friheter (mulighet til) AP omtaler. De negative frihetene (fravær av tvang) som er gjenstand for denne undersøkelsen, er derimot i liten grad beskrevet i APs partiprogram. Høyre har også i liten grad beskrevet frihet i tråd med definisjonen «fravær av tvang». Likevel har Høyre vesentlig mer oppmerksomhet om både sikkerhetstiltak for å styrke politiets evne til *kriminalitetsbekjempelse*, og om personvern i tråd med definisjonen av *personopplysningsvern* – sammenliknet med AP. FrP, SP, SV og Venstre har alle forholdsvis mye oppmerksomhet om verdien frihet, også i form av fravær av tvang.

FrP og KrF som har mye omtale av verdien sikkerhet, gir i motsetning til de andre partiene, oppmerksomhet om terror som en internasjonal utfordring i sitt partiprogram. Interessant nok har også Høyre mye oppmerksomhet om verdien sikkerhet – til tross for at Høyre inntok motsatt standpunkt av FrP og KrF under stortingsdebatten. På motsatt side av skalaen når det gjelder sikkerhet, finner vi SV som har lite oppmerksomhet om verdien sikkerhet, og uttrykker at terror ikke er en spesielt stor utfordring internasjonalt. SV uttrykker derimot at undertrykkelsen av borgernes frihet som har oppstått under «krigen mot terror», er en mye større utfordring sammenliknet med terror. Verdien personvern er mest fremtredende i partiprogrammene til Høyre, SP og Venstre. Også her er det interessant å merke seg at SP og Venstre under stortingsdebatten var imot innføringen av datalagringsdirektivet, mens Høyre var for. Arbeiderpartiet befinner seg i den andre enden av skalaen og har ingen omtale av personvern i sitt partiprogram.

Partiene Høyre, FrP, KrF, SP, SV og Venstre uttrykker i partiprogrammene at de ønsker en restriktiv overvåkningspraksis. KrF og SV uttrykker videre at overvåkning av hele befolkningen ikke aksepteres. Venstre og SV uttrykker eksplisitt i sine partiprogrammer at de stiller seg imot innføringen av EUs datalagringsdirektiv. Ingen av partiene i undersøkelsen uttrykker i partiprogrammene at de stiller seg positive til økt overvåkning, eller omtaler datalagringsdirektivet som et positivt virkemiddel for kriminalitetsbekjempelse.

Tabell 4 viser i hvilket omfang partiene omtaler verdiene frihet, sikkerhet og personvern i sine partiprogrammer fra 2009:

Tabell 4: Datainnsamling fra partiprogrammene

Verdi	Frihet	Sikkerhet	Personvern
Dokument	Partiprogram	Partiprogram	Partiprogram
AP	Lite omtale	Noe omtale	Ingen omtale
Høyre	Noe omtale	Mye omtale	Mye omtale
FrP	Mye omtale	Mye omtale	Noe omtale
KrF	Noe omtale	Mye omtale	Noe omtale
SP	Mye omtale	Noe omtale	Mye omtale
SV	Mye omtale	Lite omtale	Noe omtale
Venstre	Mye omtale	Noe omtale	Mye omtale

Funnene fra de to innholdsanalysene som er presentert i kapittelet 5, vil nå diskuteres inngående i neste kapittel. Ettersom det er redegjort for *omfanget* av hvordan partiene mener verdiene ville blitt påvirket, er det tid for å undersøke nærmere *hvordan* de ville blitt påvirket.

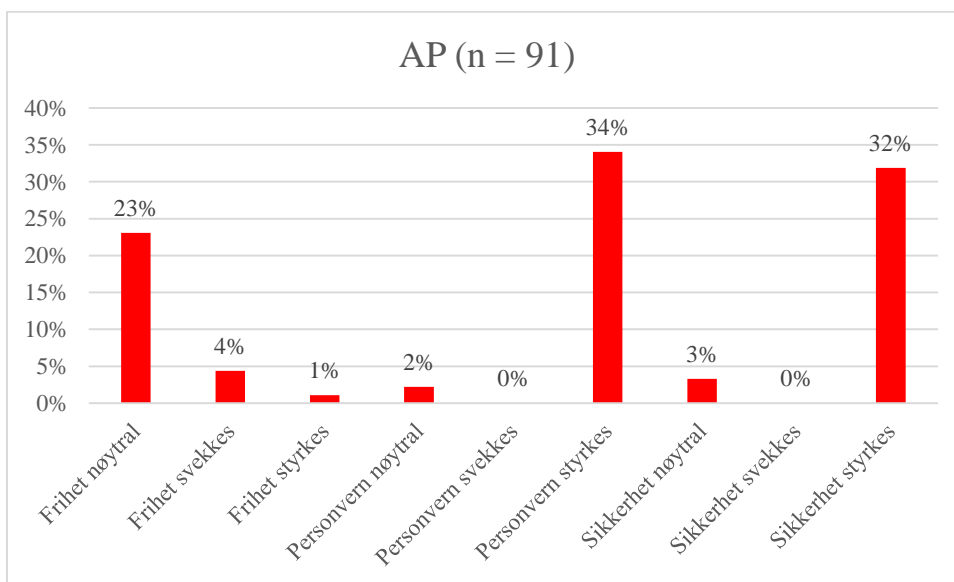
6 Diskusjon

I dette kapittelet vil de mest sentrale funnene fra innholdsanalysene diskuteres. Diskusjonen er delt inn i tre ulike underkapitler, med utgangspunkt i undersøkelsens problemstilling. Kapittel 6.1 viser til partier med et partiprogram som *i liten grad* kan forklare deres standpunkt under stortingsdebatten. Her finner vi kun partiet AP. Kapittel 6.2 viser til partier med partiprogram som *i noen grad* kan forklare deres standpunkt. Her finner vi Høyre, FrP, KrF og SP. Kapittel 6.3 viser til partier med partiprogram som *i stor grad* kan forklare deres standpunkt under stortingsdebatten. Her finner vi SV og Venstre.

Hvert parti har sitt eget underkapittel, hvor partiets standpunkt under stortingsdebatten fra 2011 vil diskuteres opp imot hva de skriver i eget partiprogram fra 2009. På denne måten vil det undersøkes nærmere *hva* partiene uttrykte under debatten, og hvordan partiprogrammet kan forklare deres standpunkt. Teorien redegjort for i kapittel 2 vil bidra til å forklare funnene som presenteres fortløpende, og problemstillingen vil dermed kunne besvares i kapittel 7.

6.1 Partiprogrammet kan i liten grad forklare partiets standpunkt

6.1.1 Arbeiderpartiet (AP)



Graf 4: Arbeiderpartiets utsagn under stortingsdebatten

Tabell 6: Sammenlikning av Arbeiderpartiets partiprogram og standpunkt under stortingsdebatten

Verdi	Frihet	Frihet	Sikkerhet	Sikkerhet	Personvern	Personvern
Dokument	Partiprogram	Stortingsdebatten	Partiprogram	Stortingsdebatten	Partiprogram	Stortingsdebatten
AP	Lite omtale	Nøytral	Noe omtale	Styrkes	Ingen omtale	Styrkes

Frihet

AP skiller seg noe fra de andre politiske partiene med hensyn til hvordan de uttrykker seg, både under stortingsdebatten og i partiprogrammet *Skape og dele*. Et sentralt funn er at AP i svært liten grad omtaler overvåkning, datalagring eller verdiene som undersøkes, i sitt partiprogram for perioden 2009 – 2013. I det hele gir AP lite omtale til verdien frihet, forstått som «fravær av tvang», slik Isaiah Berlin (1969, s. 128 – 130) redegjør for de negative frihetene. AP skriver likevel om frihet flere steder i sitt partiprogram, men i liten grad om de friheter som er relevante for denne undersøkelsen. Frihet i form av positiv frihet og muligheter for alle – slik Isaiah Berlin redegjør for, er derimot et tema som AP gir stor oppmerksomhet, i partiprogrammet (Arbeiderpartiet, 2009).

Under stortingsdebatten er AP det eneste partiet sammen med Høyre som uttrykker at de negative frihetene ikke vil svekkes. AP gir likevel forholdsvis mye oppmerksomhet til verdien frihet som vi kan se av grafen ovenfor. Hele 28 % av de kodede utsagnene fra AP befinner seg i kategorien, i tråd med Isaiah Berlins negative frihetsbegrep. Spesielt interessant er det at hele 23 % av innleggene til AP er kategorisert under fanen frihet nøytral. At et så stort antall utsagn fra AP er tolket inn i kategorien nøytral, tyder på at AP mener frihet er en viktig verdi. Likevel kan det faktum at innleggene er tolket inn i kategorien nøytral tyde på at AP mener at datalagringsdirektivet ikke vil bidra til å svekke borgernes friheter. Et sitat som understøtter dette funnet fremkommer fra stortingsrepresentant Anne Marit Bjørnflaten, som forsøker å imøtegå påstander om at datalagringsdirektivet vil bidra til økt overvåkning. Ifølge representanten Bjørnflaten innebærer ikke datalagringsdirektivet overvåkning, ettersom *innholdet* i kommunikasjonen ikke vil lagres.

Innholdet i kommunikasjonen skal ikke lagres. I saksframlegget hevder opposisjonen at dette er overvåkning. Det er det ikke. Overvåkning innebærer aktivt og kontinuerlig å følge med på hva noen foretar seg. Vårt forslag har ingenting med overvåkning å gjøre (Stortinget, 2011, s. 3197).

Hvor grensene går for hva som er og hva som ikke er overvåkning, kan fremstå som uklart. Noe sitatet fra Bjørnflaten ovenfor viser. David Lyon (2001, s. 2) definerer *overvåkning* som

«systematisk og rutinemessig innsamling og behandling av personopplysninger med det formål å utøve innflytelse, administrasjon, styring og kontroll». Datalagringsdirektivet hadde til hensikt å innsamle trafikk- og lokasjonsdata fra alle individer som benyttet tilbydere av elektronisk kommunikasjon underlagt norsk jurisdiksjon (Graver, 2015, s. 37). Derfor kan innsamlingen gjennom direktivet fremstå som rutinemessig og systematisk. Innsamlingen av trafikk- og lokasjonsdata fremstår også som personsensitive nettopp fordi opplysningene vil kunne benyttes til kriminalitetsbekjempelse, mot enkeltindivider – på et senere tidspunkt. Justisdepartementet skriver i lovforslaget (Prop. 49L, 2010, s. 8) at hensikten med datalagringsdirektivet er *kriminalitetsbekjempelse*. Kriminalitetsbekjempelse handler om «å hindre at samfunnet og borgerne utsettes for kriminelle handlinger» (NOU 2009:15, s. 68). For å hindre at samfunnet utsettes for kriminelle handlinger er politiet avhengig av tilstrekkelig med opplysninger for å gripe inn før (forebygge) eller etter (etterforske) at slike handlinger har funnet, eller vil finne sted (Dragu, 2011, s. 4, Nordenhaug & Engene 2008, s. 124 – 125). Kriminalitetsbekjempelse er dermed også nært tilknyttet tvangsutøvelse, som kan ansees som en mer inngripende form for innflytelse, styring og kontroll som er begrepene Lyon (2001, s. 2) benytter i sin definisjon av begrepet overvåkning.

Til tross for at Bjørnflaten og AP hevder at datalagringsdirektivet ikke vil medføre overvåkning, er det vanskelig å se for seg at dette faktisk vil være tilfellet dersom man tar utgangspunkt i Lyons definisjon av begrepet. Lyon (2014, s. 2) påpeker imidlertid at dagens overvåkningspraksiser har i større grad flyttet seg fra overvåkning av enkeltindivider til massemonitorering av hele befolkningen. Noe som ifølge Lyon også medfører store etiske utfordringer. Det kan se ut til at AP forholder seg til en noe utdatert og gammeldags forståelse av overvåkningsbegrepet ettersom Bjørnflaten uttaler at «overvåkning innebærer aktivt og kontinuerlig å følge med på hva noen foretar seg» (Stortinget, 2011, s. 3197). Sitatet fra Bjørnflaten antyder nærmest at enkeltindivider ikke overvåkes før de fotfølges av en agent eller blir telefonavlyttet. En slik forståelse ser imidlertid ikke ut til å passe spesielt godt overens med verken den teknologiske utviklingen eller overvåkningspraksiser som er fremtredende i dagens høyteknologiske samfunn.

Sikkerhet

I likhet med verdien frihet, skiller også AP sammen med Høyre seg ut når det gjelder verdien sikkerhet. AP og Høyre er de eneste partiene som under stortingsdebatten uttrykker at verdien sikkerhet vil styrkes. Hele 32% av APs innlegg er tolket inn i kategorien sikkerhet styrkes, og

3 % i kategorien sikkerhet nøytral. Dette indikerer at AP mener direktivet vil bidra til å hindre at samfunnet og borgerne utsettes for kriminelle handlinger, i tråd med definisjonen for sikkerhet etablert til bruk ved denne undersøkelsen. Knut Storberget, som var justisminister ved tidspunktet for stortingsdebatten, uttrykte at det for politiets del var avgjørende å følge samfunnsutviklingen. Etersom samfunnet ifølge Storberget blir digitalisert, må også politiet følge den digitale utviklingen. Politiet må derfor få tilgang på digitale virkemidler til kriminalitetsbekjempelse, som eksempelvis datalagringsdirektivet.

Det er teoretisk og urealistisk å tro at kriminalitet i dagens samfunn kan bekjempes på tilfredsstillende vis uten dette verktøyet [...] Jeg vil illustrere behovet til politiet med et sitat fra Politidirektoratets høringsuttalelse i saken: «Med hus kom innbruddstyver, med pengesedler kom pengefalsk, med toget kom togrøverier, med bilen kom promillekjøring og med velferdsstaten kom trygdebedragerier.» Kriminaliteten følger samfunnsutviklingen, og politiet må følge samfunnsutviklingen, også når det gjelder metodikk. Samfunnet er gjennomdigitalisert, og politiet må også få adgang til digitale medier i arbeidet for å bekjempe kriminalitet (Stortinget, 2011, s. 3206).

AP omtaler verdien sikkerhet i noen grad i sitt partiprogram, men svært lite av omtalen dreier seg om temaene overvåkning og datalagring. Det blir derimot gitt mer oppmerksomhet mot «tradisjonelt» politiarbeid som patruljevirkosomhet, etterforskning og styrking av politiets innsats for utsatte-, sårbare grupper og barn. AP gir ikke oppmerksomhet til terrorisme i sitt partiprogram, noe som kan tolkes i retning av at partiet ikke anså terror som et stort samfunnsproblem i forkant av partiprogrammets lansering i 2009 (Arbeiderpartiet, 2009).

Et interessant funn når det gjelder AP i denne undersøkelsen, er at partiet i liten grad omtaler verdiene frihet, sikkerhet og personvern i konteksten av datalagringsdirektivet i sitt partiprogram. Likevel uttrykker AP at datalagringsdirektivet vil være et *absolutt nødvendig* virkemiddel. Representanten Storberget går så langt som å si at «det er teoretisk og urealistisk å tro at kriminalitet i dagens samfunn kan bekjempes på tilfredsstillende vis uten dette verktøyet» (Stortinget, 2011, s. 3206). Storbergets syn, som ser ut til å være representativt for partiet for øvrig, tyder i hovedsak på at AP mener at datalagringsdirektivet burde innføres. Ifølge AP er direktivet nødvendig for at staten skal ha evne til å sørge for borgernes sikkerhet. I sammenheng med representanten Bjørnflatens utsagn, hvor hun påpeker at «vårt forslag har ingenting med overvåkning å gjøre» (Stortinget, 2011, s. 3197) er det spesielt interessant å

betrakte APs syn på datalagringsdirektivet. Partiet mener at direktivet *ikke omhandler overvåkning*, og dermed heller ikke vil påvirke borgernes frihet. Samtidig mener de at direktivet er nødvendig for at staten skal evne å sørge for borgernes sikkerhet. AP ser dermed ikke ut til å erkjenne at det eksisterer et dilemma mellom verdiene frihet og sikkerhet ved innføringen av datalagringsdirektivet.

Richards (2013, s. 1935 – 1937) viser til at demokratisk valgte myndigheter i vesten i større grad har akseptert overvåkning av egen befolkning i etterkant av 11. september 2001. Denne utviklingen har også vist seg å være tilstede i Norge (Hammerlin, 2009, s. 17 – 43, Nordenhaug & Engene 2008, s. 147). Ifølge Richards (2013, s. 1935 – 1937) har kontra-terrorisme, cybersikkerhet og beskyttelse av barn fra overgripere vært sentrale begrunnelser for økt overvåkning fra myndighetenes side. AP ser i denne undersøkelsen i stor grad ut til å akseptere økt overvåkning av egen befolkning. I særdeleshet for styrke sikkerheten ved å beskytte barn og sårbare individer mot kriminelle handlinger. Det kan derfor være interessant å merke seg studien til Bergen m.fl. (m.fl., 2014, 2 – 3) av NSAs overvåkningspraksis. Studien viste at generell overvåkning mot befolkningen som helhet gav svært liten uttelling til sammenlikning med mer målrettede etterforskningsmetoder.

Personvern

Personvern er et tema som AP ikke gir noen oppmerksomhet i sitt partiprogram. Begrepet personvern eller nært beslektede begreper som personopplysningsvern, nevnes ikke én eneste gang i partiprogrammet (Arbeiderpartiet, 2009). Det fremstår med tydelighet i både partiprogram og stortingsdebatten at personvern er et tema som ikke er fremtredende i APs politikk. Likevel viser APs utsagn under stortingsdebatten at partiet i all hovedsak mener at datalagringsdirektivet vil bidra til å styrke personvernet. Hele 35 % av APs utsagn er tilknyttet verdien personvern med utgangspunkt i definisjonen personopplysningsvern. 34 % av utsagnene fra AP er plassert i kategorien personvern styrkes, og 2 % i personvern nøytral. Personvern er altså den kategorien hvor flest utsagn fra AP er tolket inn, til tross for at partiet ikke har uttrykt oppmerksomhet om personvern i eget partiprogram.

Som både Alessandro Acquiciti (2004, s. 1) og Schartum & Byrgrave (2016, s. 19) viser til, er en sentral utfordring at personvern er et begrep som ofte kan ha ulikt innhold og som kan bety ulike ting for ulike mennesker. Sitatet til Eirik Sivertsen nedenfor viser tydelig begrepsutfordringene. Sivertsen påpeker at personvern for han handler om både det som i denne

oppgaven defineres som frihet (beskyttelse mot overvåkning), sikkerhet (beskytte innbyggerne mot grov kriminalitet) og personvern (beskyttelse mot at opplysningene kan komme på avveie). For representanten Sivertsen betraktes altså begrepet *personvern* som det vi i denne undersøkelsen omtaler med tre ulike begrep, nemlig frihet, sikkerhet og personvern. Verdier som ofte står i et *motsetningsforhold* til hverandre. Ifølge Bing (2010, s. 28) kan den systematiske innsamlingen av opplysninger om individet senere benyttes til å utøve makt ovenfor det samme individet. På denne måten fremstår verdiene frihet og personvern på den ene, og sikkerhet på den andre – nokså åpenbart som motsetninger i konteksten av datalagringsdirektivet.

For meg handler ikke personvern bare om beskyttelse mot overvåking og at opplysningene kan komme på avveie. Personvern handler for meg også om at innbyggerne beskyttes mot grov kriminalitet. Personvern er også å sikre at organisert kriminalitet kan bekjempes i samfunnet. Personvern er også å anstrenge seg til det ytterste for å beskytte våre barn mot seksuelle overgrep og grov utnyttning. Derfor må vi finne balanserte løsninger, sånn at vi også kan skape et trygt samfunn i framtiden (Stortinget, 2011, s. 3241).

Representanten Sivertsen og AP viser her til en tolkning av begrepet personvern som er langt bredere og mer omfattende enn hva som er tilfellet for de andre partiene i denne undersøkelsen. I større grad kan det se ut til at Sivertsen omtaler det som Schartum & Bygrave (2016, s. 19) omtaler som *personlig integritet* fremfor *personopplysningsvern*. Personlig integritet er bredere i sin definisjon, og dermed også kan inkludere flere elementer enn det som i IKT-samfunnet omtales som personopplysningsvern. Begrepsunøyaktigheter som dette fører til at stortingsdebatten i enkelte tilfeller kan oppfattes som upresis og uryddig.

Arbeiderpartiet oppsummert

APs partiprogram kan i liten grad bidra til å forklare partiets standpunkt om at datalagringsdirektivet ville bidratt til å styrke både sikkerhet og personvern. Hovedårsaken til dette, er at AP i svært liten grad skriver om forhold relatert til verdiene frihet, sikkerhet og personvern i konteksten av overvåkning.

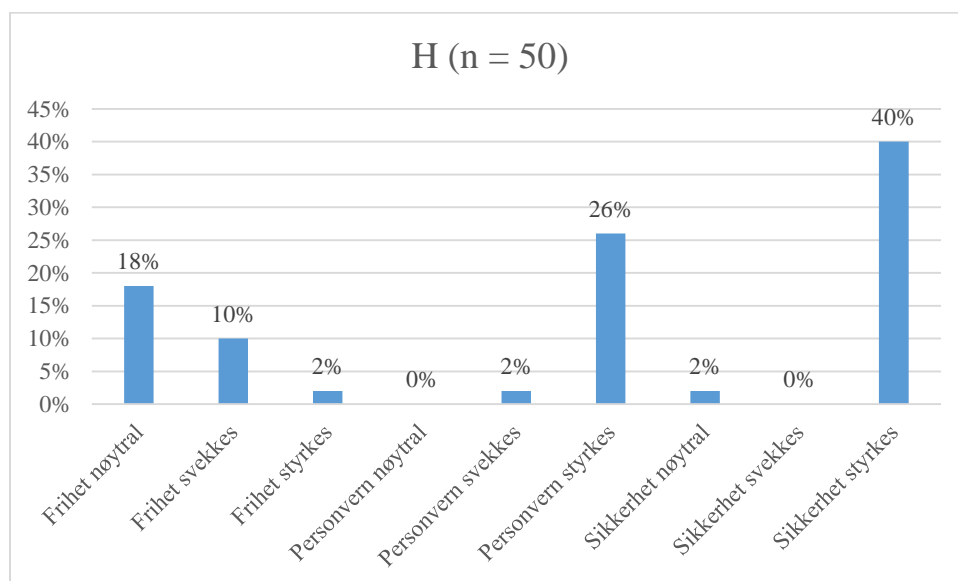
Partiprogrammet kan imidlertid *indirekte* bidra til å forklare APs standpunkter på enkelte områder. Ettersom partiet hadde lite oppmerksomhet om verdien frihet, og ingen oppmerksomhet om verdien personvern i partiprogrammet – kan den manglende

oppmerksomheten om verdiene forklare at AP verken hadde forpliktet seg *for* eller *imot* innføringen av datalagringsdirektivet. I tillegg kan den manglende oppmerksomheten om personvern i partiprogrammet bidra til å forklare begrepsunøyaktigheten som representanten Sivertsen viser under stortingsdebatten.

Til tross for lite omtale av verdien sikkerhet, hadde AP likevel noe fokus på ivaretagelse og beskyttelse av unge og sårbare individer i partiprogrammet. Under stortingsdebatten uttrykte representanten Bjørnflaten at datalagringsdirektivet ikke ville bidratt til overvåkning, og dermed ville direktivet heller ikke bidra til å svekke borgernes frihet. Funnene bidrar på denne måten *indirekte* til å forklare hvorfor AP i større grad ønsket å prioritere sikkerhet fremfor frihet under stortingsdebatten. Dette til tross for at partiet på ingen måte hadde tatt aktivt stilling til temaet *overvåkning* eller EUs datalagringsdirektiv da de utformet partiprogrammet i 2009.

6.2 Partiprogrammet kan i noen grad forklare partiets standpunkt

6.2.1 Høyre (H)



Graf 5: Høyres utsagn under stortingsdebatten

Tabell 6: Sammenlikning av Høyres partiprogram og standpunkt under stortingsdebatten

Verdi	Frihet	Frihet	Sikkerhet	Sikkerhet	Personvern	Personvern
Dokument	Partiprogram	Stortingsdebatten	Partiprogram	Stortingsdebatten	Partiprogram	Stortingsdebatten
Høyre	Noe omtale	Nøytral	Mye omtale	Styrkes	Mye omtale	Styrkes

Frihet

Høyre gir i sitt partiprogram for perioden 2009 – 2013 – *Muligheter for alle*, noe omtale av verdien frihet. Sammenliknet med AP viser Høyre til at frihet i større grad er et individuelt ansvar enn et fellesskapsanliggende. Likevel kan det også i Høyres partiprogram se ut til at partiet ikke skiller mellom ulike former for frihet. Høyre omtaler både det området hvor staten bør tilrettelegge for borgernes muligheter (positive friheter) og det området hvor borgerne skal være frie fra statens tvangsbruk (negative friheter), under ett (Høyre, 2009). Sitatet nedenfor viser hvordan Høyre både ønsker å tilrettelegge for at enkeltindividet skal ha frihet til å foreta egne valg, samtidig som de påpeker at staten skal være sterk og pålitelig på sine kjerneområder. Det omtales imidlertid ikke nærmere hvordan individenes frihet skal sikres, eller hvilke kjerneområder staten skal være sterk og tilgjengelig på.

Staten skal være sterk, pålitelig og tilgjengelig på sine kjerneområder. Men staten må ikke bli så altomfattende at den mister evnen til virkelig å hjelpe dem som trenger den mest. Staten må heller ikke bli så stor at den stjeler menneskers mulighet til å stå på egne ben eller bryter ned friheten til selv å velge hvordan man vil leve sitt liv (Høyre, 2009, s. 5).

Videre er det interessant å merke seg hva Høyre skriver i sitt partiprogram under overskriften *for å sikre personvern og ytringsfrihet*, hvor det står det følgende: «[Høyre vil] stille seg kritisk til innføringen av nye lover som øker adgangen til, eller omfanget av, overvåkning i samfunnet» (Høyre, 2009, s. 50). Sitatet tyder på at Høyre hadde tatt et mer aktivt standpunkt enn AP til det faktum at overvåkning kan bidra til å svekke borgernes friheter og særdeleshet ytringsfrihet som helt eksplisitt står nevnt i overskriften. Richards (2013, s. 1935) forklarer at våre samfunn mangler forståelse om hvorfor og når myndighetenes overvåkning er skadelig. Videre påpeker Richards at overvåkning er skadelig fordi det kan nedkjøle individenes vilje til utøvelse av fundamentale borgerrettigheter som menings- og ytringsfrihet.

Under stortingsdebatten er hele 30 % av utsagnene fra Høyre kodet inn under kategorien frihet. Flertallet av utsagnene (18 %) tyder på at Høyre mener at datalagringsdirektivet vil forholde seg nøytralt til verdien frihet. I likhet med AP ser antallet innlegg i kategorien frihet nøytral ut til å være et uttrykk for at Høyres representanter ikke ser på datalagringsdirektivet som overvåkning. Direktivet vil ifølge Høyre dermed ikke bidra til å svekke borgernes friheter. Likevel er det interessant at også 10 % av utsagnene fra Høyre tolket inn i kategorien frihet svekkes. Dette tyder på at det innad i Høyre finnes ulike meninger om hvordan

datalagringsdirektivet ville påvirket verdien frihet. Et sitat fra Michael Tetzschner understøtter menings ulikhetene innad i Høyre, hvor representanten påpeker at staten bryter med viktige frihetsprinsipper ved å innføre datalagringsdirektivet.

Med det avviker Stortinget fra to prinsipper, for det første grunnregelen om at personopplysninger kun skal brukes til det formålet de er innsamlet for. Det som hittil har vært forbudt for private, blir nå en norm for staten. For det andre etterforskningsprinsippet: at ingen forberedelse til straffeforfølgning skal gjøres uten konkret mistanke (Stortinget, 2011, s. 3238).

Tetzschners utsagn om at staten nå vil utføre *forberedelse til straffeforfølgning* uten konkret mistanke mot individene det innsamles opplysninger om, er interessant i lys av John Stuart Mills' argumentasjon. Mill (2010, s. 89 – 90) påpekte allerede i år 1859 at det å forebygge kriminelle handlinger kunne i langt større grad føre til misbruk av borgernes frihetsrettigheter sammenliknet med det å ilegge straff. Mill stilte det retoriske spørsmålet: «hvor store innhugg i borgernes frihet kan vi gjøre for å forebygge forbrytelser og ulykker?» Som Mill (2010, s. 113 – 114) påpeker, er det nettopp det faktum at vi er frie individer som også gjør det lettere for oss å begå forbrytelser. Flertallet av Høyres representanter ser dermed ut til å akseptere større innskrenkninger i borgernes friheter sammenliknet med representanten Tetzschner. Blant annet ved å tillate lagring av trafikk- og lokasjonsdata om borgerne allerede *før* en kriminell handling har funnet sted. Nordenhaug & Engene (2008, s. 40, 41, 147) forklarer at det har vært tilstede en utvikling i Norge, hvor *pre-aktive* straffebud er innført for å forhindre blant annet terrorisme. Til tross for at flertallet i Høyre ser ut til å ønske en slik utvikling, og mener at datalagringsdirektivet ikke vil svekke borgernes friheter – mener enkeltrepresentanter som Michael Tetzschner at direktivet likevel vil svekke borgernes friheter, og dermed ikke bør innføres.

Sikkerhet

Også når det gjelder verdien sikkerhet, uttrykte Høyre i likhet med AP under stortingsdebatten at datalagringsdirektivet ville bidratt til å styrke borgernes sikkerhet. Hele 40 % av de kodede utsagnene tyder på at Høyre mente at sikkerheten ville blitt styrket. Sitatet nedenfor fra Øyvind Halleraker viser hvordan partiet mener at direktivet ville bidratt positivt til at politiet fikk tilstrekkelige virkemidler til å bekjempe terrorisme og annen alvorlig kriminalitet.

Ved avtalen mellom Høyre og Arbeiderpartiet sikres politiet virkemidlene som gjør at alvorlig organisert kriminalitet, omreisende vinningskriminelle, spredning av overgrepssbilder av barn og terrorisme kan avverges eller oppklares mer målrettet og effektivt enn i dag (Stortinget, 2011, s. 3213).

Hallerakers utsagn viser at det forelå en avtale mellom partiene Høyre og AP. Det er ikke overraskende at de to partiene uttrykte seg positivt om innføringen av datalagringsdirektivet, da begge partiene også voterte for innføringen av direktivet. Derimot er det interessant å betrakte de 40 % av utsagnene fra Høyre om at datalagringsdirektivet vil bidra til å styrke sikkerheten i lys av hva partiet skriver i sitt eget partiprogram. Under overskriften *trygge lokalsamfunn* skriver Høyre (2009, s. 47) at de «ønsker å vri den offentlige ressursbruken innen justissektoren til tiltak som har vist dokumenterbar effekt på kriminalitetsforebyggende arbeid.» Hvorvidt datalagringsdirektivet ville hatt *dokumenterbar effekt* på det kriminalitetsforebyggende arbeidet, fremstår som usikkert. Studien til Bergen m.fl. (2014) dokumenterer at overvåkningsprogrammer som amerikanske myndigheter forvaltet, ikke hadde noen vesentlig effekt på oppklaring av saker relatert til terrorisme. Det fremstår som utfordrende å dokumentere positive sikkerhetsgevinster av overvåkningsprogram som innsamler data om hele befolkningen, slik datalagringsdirektivet ville tilrettelagt for. Likevel ble det, spesielt fra politiets side, uttrykt et nokså unisont ønske om å innføre direktivet. Høringsuttalelsene fra etaten, hvor blant annet Politidirektoratet, PST, KRIPOS, Økokrim m.fl. var representert, bekrefter dette (Prop. 49L, 2010, s. 8). Ifølge Lewis (2005, s. 104) utøver politiet lobbyvirksomhet innen lov og politikk for å muliggjøre innsamling, lagring og deling av informasjon. Noe som også ser ut til å ha vært tilfellet ved behandling av lovforslaget om innføring av datalagringsdirektivet i norsk rett.

Det fremstår som uklart om det å innsamle data om hele befolkningen, og ikke kun de som er mistenkt for kriminalitet – i det hele tatt vil ha noen positiv effekt på kriminalitetsbekjempelse. Som nevnt, påpeker David Lyon (2014, s. 9) at det i mange tilfeller vil bli som å lete etter nåla i høystakken når man forsøker å finne terrorister i store datamengder. På bakgrunn av utfordringene med å dokumentere positive effekter ved overvåkningsprogrammer generelt, kan det stilles spørsmål om Høyre trosser forpliktelsene i eget partiprogram ved å ønske datalagringsdirektivet innført. Det fremgår ikke av datagrunnlaget i denne undersøkelsen om Høyre har fremskaffet dokumentasjon som underbygger at datalagringsdirektivet har positive effekter på kriminalitetsbekjempelse, utover høringsuttalelsene. Det kan dermed fremstå som

at Høyre baserte sitt ønske om innføring av datalagringsdirektivet på bakgrunn av blant annet høringsuttalelser fra politiet, noe som bekreftes av Ingjerd Schou i sitatet nedenfor.

Uttalelser fra Politiets sikkerhetstjeneste, PST, under komiteens høringer går på at Norge uten datalagringsdirektivet blir mer utsatt for terror, og at PST bruker trafikkdata i alle sine saker (Stortinget, 2011, s. 3192).

Personvern

Et interessant funn fra Høyre, er at partiet er det eneste som gir verdien personvern mye omtale i sitt partiprogram – og samtidig under stortingsdebatten uttrykker at datalagringsdirektivet ville ført til at personvernet styrkes. Denne tilnærmingen skiller seg fra Venstre og SP som er de to andre partiene som også har mye oppmerksomhet om personvern i sine partiprogrammer. Venstre og SP uttrykte derimot at personvernet ville blitt svekket. Et interessant funn i denne sammenheng er at Høyres representanter under stortingsdebatten, i likhet med AP, ser ut til å mene at datalagringsdirektivet ikke ville ført til mer overvåkning av den norske befolkningen.

Høyre ser med andre ord ikke ut til å erkjenne at innsamling og lagring av opplysninger som kan knyttes til et enkeltindivid (personopplysninger) er å anse som overvåkning, så lenge disse dataene er lokasjons- og trafikkdata, altså ulike former for metadata. Dersom det ville vært aktuelt å lagre *innholdsdata*, altså innholdet i selve kommunikasjonen til individene – kan det være at Høyre ville inntatt en helt annen tilnærming til direktivet. Innholdsdata kan anses som mer krenkende for personopplysningsvernet sammenliknet med trafikk- og lokasjonsdata. Ifølge Schartum & Bygrave (2016, s. 31 – 35) handler *kommunikasjonsintegritet* om at individer skal ha retten til å kommunisere uforstyrret med andre. Likevel er Høyres standpunkt under stortingsdebatten interessant, da partiet i motsetning til AP uttrykker i sitt partiprogram at «personvernet må sikres på alle samfunnsområder. Ved vurderingen av behovet for nye etterforskningsmetoder må personvern hensyn veie tungt» (Høyre, 2009, s. 48).

Med datalagringsdirektivet ville det blitt innført en domstolskontroll som politiet måtte gjennom for å få tillatelse til utlevering av dataene som ble lagret ved hjelp av direktivet (Graver, 2015, s. 37). Representanten Øivind Halleraker viser til at domstolskontroll ville blitt en styrkning av personopplysningsvernet, ettersom politiet også har tilgang på de nevnte dataene i dag – uten et strengt regelverk som regulerer slik tilgang.

Oppbevaring, tilgang og sletting av lagringspliktige data blir det langt strengere regler for enn i dag. Fire ulike utredninger i løpet av de siste ti årene har dokumentert at regelverket inntil nå har vært uklart, uryddig og ulikt praktisert av de ulike teletilbyderne. Ved at det innføres en domstolskontroll før data kan utleveres til politiet, og vilkår om at data kun skal kunne utleveres ved mistanke om alvorlig kriminalitet, styrkes denne sikkerheten (Stortinget, 2011, s. 3213).

Det ser ut til at Høyre i stor grad argumenterer for at datalagringsdirektivet ville styrket personvernet nettopp fordi kontrollen med oppbevaring, tilgang, sletting og tilsyn ved dataene ville blitt strengere og mer regulert ved hjelp av det foreslåtte lovverket. Høyre og APs tilnærming til personvernet skiller seg dermed vesentlig fra FrP, SV og Venstres tilnærming, som i stor grad ser ut til å mene at personvernet ville blitt svekket. Årsaken til at personvernet ville blitt svekket, er at datalagringsdirektivet ville pålagt lagring av en stor mengde opplysninger som kan knyttes til enkeltindividet. At datalagringsdirektivet ville bidratt til å svekke personvernet, er det imidlertid kun én representant fra Høyre som uttrykker under stortingsdebatten. Michael Tetzschners sitat nedenfor, hvor representanten påpeker at personopplysninger kan misbrukes – tyder på at også han har en vesentlig annen forståelse av datalagringsdirektivets *virksomheter* på personvernområdet, sammenliknet med de fleste av hans partikolleger i Høyre for øvrig.

Om vi antok at ingen opplysninger ville komme på avveie og kunne misbrukes av de kriminelle man sier man vil bekjempe, om vi antok at ingen i forvaltning og politi kunne gjøre feil eller begå urett, om vi antok at en demokratisk ledet stat virkelig kunne sikre at ingen ville bryte dens egne sikkerhetsregler, selv da ville vi fortsatt stå overfor et virkemiddel som har en kostnadsside større enn penger (Stortinget, 2011, s. 3231).

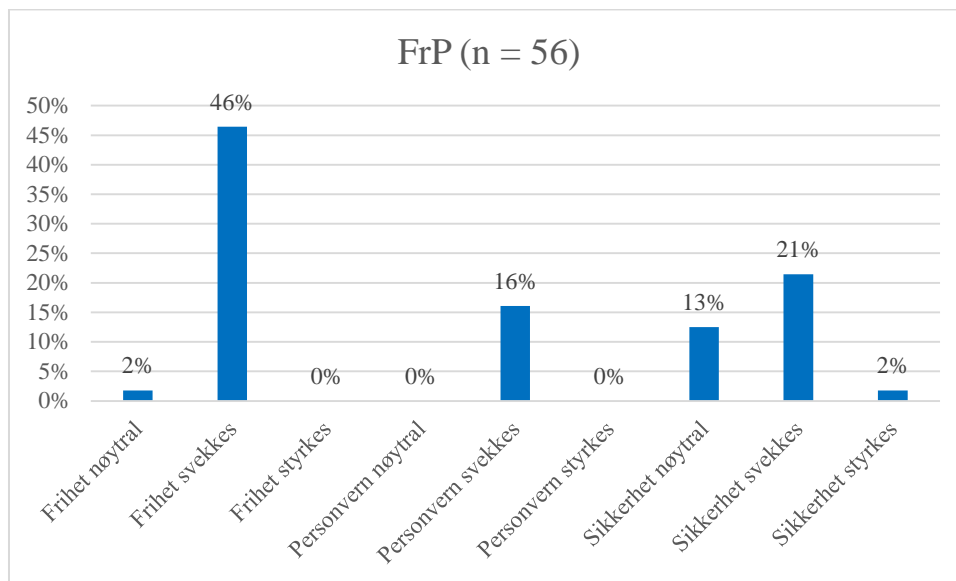
Til tross for at Høyre i stor grad hevder at datalagringsdirektivet ville bidratt til å styrke personvernet, er det interessant å merke seg hva Citron & Gray (2014, s. 270 – 271) skriver om sammenhengen mellom personvern og fremveksten av stordatateknologien. Citron og Gray viser til at det nettopp er *mengden* av opplysninger som kan tilknyttes et enkeltindivid som i dag utgjør den store trusselen mot personvernet. Fagfeltet *kvantitativt personvern* omtaler problemstillinger som vokser frem når myndighetene har mulighet til å analysere store mengder metadata. Stordata tilnærmingen som kvantitativt personvern tar utgangspunkt i, tilsier at det er mulig å få tak i store mengder detaljert informasjon om enkeltindividenes liv ved innsamling av små bruddstykker med informasjon fra mange ulike datakilder. Datakildene kan være i form

av trafikk- og lokasjonsdata slik datalagringsdirektivet hadde til hensikt å pålegge lagring. Analyseverktøyene i stordata tilnærmingen som kan sammenstille de små og mange bruddstykkene med data, kan bidra til å trekke statistiske slutninger om individet, og på den måten gi analytikerne tilgang på ny informasjon som i utgangspunktet ikke er synlig før analysen gjennomføres (Citron & Gray 2014, s. 264). Utfordringen er imidlertid at analyseverktøyene kan ta feil, og er ofte basert på generaliserende kategorier som ikke alltid vil være representative for identiteten til det enkelte individ. Ifølge David Lyon (2014, s. 9) er sannsynligheten stor for at uskyldige individer vil bli rammet av mistanke ved bruk av stordata teknologien.

Høyre oppsummert

Høyres partiprogram kan i noen grad forklare partiets synspunkt på datalagringsdirektivet. Partiprogrammet kan forklare at Høyre ønsker å styrke sikkerhet og personvern, men det kan ikke bidra til å forklare at Høyre ønsker å innføre et lovverk som vil tilrettelegge for økt overvåkning. Høyre (2009, s. 50) skriver eksplisitt i sitt partiprogram at de vil «stille seg kritisk til innføringen av nye lover som øker adgangen til, eller omfanget av, overvåkning i samfunnet.» Det interessante i denne sammenheng, er at flertallet av Høyres representanter under stortingsdebatten, uttrykker at datalagringsdirektivet *ikke* ville bidratt til å svekke borgernes frihet. Likevel fremgår det relativt tydelig av stortingsdebatten at det også finnes meninger innad i Høyre som tyder på at datalagringsdirektivet ville bidra til å svekke borgernes frihet. At Høyre i eget partiprogram uttaler at de ønsker å *stille seg kritisk* til økt overvåkning og samtidig under stortingsdebatten uttrykker at direktivet ikke vil bidra til å svekke borgernes frihet, kan dermed virke noe paradoksalt. Det kan være at partiets innstilling til datalagringsdirektivet i større grad er et strategisk politisk valg, fremfor en reell oppfatning fra Høyres representanter. Michael Tetzschners argumentasjon i strid med eget parti, hvor representanten uttrykker at direktivet vil bidra til å svekke borgernes friheter og personvern – underbygger en slik påstand.

6.2.2 Fremskrittspartiet (FrP)



Graf 6: Fremskrittspartiets utsagn under stortingsdebatten

Tabell 7: Sammenlikning av Fremskrittspartiets partiprogram og standpunkt under stortingsdebatten

Verdi	Frihet	Frihet	Sikkerhet	Sikkerhet	Personvern	Personvern
Dokument	Partiprogram	Stortingsdebatten	Partiprogram	Stortingsdebatten	Partiprogram	Stortingsdebatten
FrP	Mye omtale	Svekkes	Mye omtale	Svekkes	Noe omtale	Svekkes

Frihet

FrP gir i sitt partiprogram *FrP fornyer Norge*, mye omtale av verdien frihet. Når det gjelder frihet i konteksten overvåkning, uttaler partiet seg relativt konkret om utfordringen med å balansere verdiene frihet og sikkerhet da de skriver følgende under overskriften *politiet*.

Innbyggerne skal ha trygghet for at det offentlige ikke kontrollerer privatlivet. Vi ønsker derfor å begrense bruken av overvåkning med unntak av i de saker som gjelder rikets sikkerhet og alvorlig kriminalitet (FrP, 2009, s. 26).

Sitatet ovenfor tyder på at FrP i utgangspunktet ønsker å være restriktive ved bruk av overvåkning. Likevel åpner partiet for at det i enkelte saker som gjelder *rikets sikkerhet* og *alvorlig kriminalitet*, kan åpnes for bruk av slike metoder. Ifølge Richards (2013, s. 1935 – 1937) er kontra-terrorisme, cybersikkerhet og beskyttelse av barn fra overgripere, ofte begrunnelser for økt overvåkning fra myndighetenes side. På denne måten skiller FrP seg ikke vesentlig ut fra de andre partiene, da FrP åpner for overvåkning ved alvorlig kriminalitet. Likevel stilte partiet seg under stortingsdebatten negativ til innføringen av

datalagringsdirektivet. Hele 46 % av partiets utsagn i denne undersøkelsen, tyder på at FrP mente direktivet ville bidra til å svekke borgernes sikkerhet. Ettersom datalagringsdirektivet ifølge Justisdepartementet (Prop. 49L, 2010, s. 8) er et virkemiddel for å forhindre og oppklare terrorisme og annen alvorlig kriminalitet, er det interessant å bemerke at FrP likevel ikke ønsket innføringen. En forklaring kan finnes i partiprogrammet, hvor FrP (2009, s. 26) skriver at de «ser på prinsippet om at man er uskyldig inntil det motsatte er bevist, som grunnleggende for rettssikkerheten.»

Innføringen av datalagringsdirektivet ville til dels endret det ovenfor nevnte prinsippet gjennom innsamling av trafikk- og lokasjonsdata fra samtlige borgere, og ikke bare de individene som mistenkes for å ha begått eller planlegger å begå kriminelle handlinger. Lyon (2014, s. 4 – 6) forklarer at fokuset på nasjonal sikkerhet har skapt et skifte i måten sikkerhet- og etterretningstjenester arbeider på. Fra å fokusere på fortid til å undersøke fremtid. Gjennom statistiske analyseteknikker som omtales *forutseende overvåkning*⁹, kan kriminalitet avverges selv før hendelsen finner sted. Basert på historiske data kan kriminalitetsutviklingen predikeres og beslutninger kan fattes i forsøket på å forebygge fremtidig kriminalitet. Det fremgår ikke av datalagringsdirektivets beskrivelse i Prop. 49L (2010) at forutseende overvåkning slik Lyon beskriver det ville blitt muliggjort. Likevel reises det sammenliknbare prinsipielle utfordringer. I begge tilfeller ville lagring av trafikk- og lokasjonsdata fra borgere som ikke mistenkes for å ha begått kriminalitet, være sentralt for myndighetenes informasjonstilgang. Innsamlingen av slike data fra uskyldige individer bryter med sentrale rettssikkerhetsprinsipper, ifølge FrP.

Myndighetene argumenterer ifølge Dragu (2011, s. 4) ofte med at forebygging av terrorangrep krever mer inngripende virkemidler, på grunn av terrorens skadepotensiale. Til tross for dette ser det ut til at FrP mener at overvåkning og innsamling av opplysninger fra alle borgere ikke er akseptabelt. Ettersom FrP i sitt partiprogram nettopp åpnet for overvåkning i saker som omhandler *rikets sikkerhet og alvorlig kriminalitet*, kan det tolkes som et tegn på at partiet kunne stilt seg positiv til andre sikkerhetstiltak. Et sitat fra stortingsdebatten som understøtter en slik påstand finner vi fra representanten Arne Sortevik som uttaler følgende:

⁹ Citron & Gray (2013, s. 263) forklarer hvordan delstaten Alabama (USA) i samarbeid med Department of Homeland Security og Google, benytter massiv datainnsamling i forsøket på å forutsi fremtidig kriminalitet. Prosjektet som omtales «Virtual Alabama» innhenter kontinuerlig data fra mange ulike kilder som GPS, mobiltelefoner, videoovervåkning, politibiler, kartdata, etc. og lager fremtidsanalyser basert på dataene.

Norge trenger ikke EUs datalagringsdirektiv. Norge trenger ikke mer overvåkning av sine borgere. Norge trenger styrking av personvernet. Norge trenger mer effektiv innsats mot terror og organisert kriminalitet. Det kan og bør gjøres uten datalagringsdirektivet (Stortinget, 2011, s. 3223).

Sikkerhet

Når det gjelder verdien sikkerhet, så er 21 % av utsagnene under stortingsdebatten fra FrP kategorisert som sikkerhet svekkes og 13 % i kategorien sikkerhet nøytral. Det faktum at et såpass stort antall utsagn befinner seg i kategorien sikkerhet svekket, tyder på at flere av FrPs representanter er svært kritiske til datalagringsdirektivet. Andre representanter fra partiet uttaler seg mer nøkternt og mindre spissformulert, slik at utsagnet verken gir inntrykk av at sikkerheten vil svekkes eller styrkes – og dermed kategoriseres som nøytralt. Anders Anundsen forklarer hvordan sikkerheten vil svekkes ved at personer med kriminelle hensikter vil ta forhåndsregler mot overvåkingen.

Det er naturligvis bare de mest naive som tror at dette vil bidra til økt oppklaring av alvorlig kriminalitet. Kriminelle planlegger sin lovstridige aktivitet. De vet at trafikken deres lagres. De er de nærmeste til å finne nye måter å kommunisere på. De trenger ikke å ta hensyn til dette på noen spesiell måte (Stortinget, 2011, s. 3241).

Anundsens sitat er interessant i lys av at David Lyon (2014, s. 9) påpeker vanskelighetene med å lokalisere kriminelle individer i store datamengder. De som ønsker å unndra seg slik overvåking, vil ifølge Lyon fint klare det. Samtidig er sannsynligheten for falske funn et større problem, ettersom dette vil ramme konkrete personer umiddelbart og intenst. Innføringen av datalagringsdirektivet ville åpenbart også ha et kostnadsaspekt, noe representanten Bård Hoksrud påpeker da han uttaler at «her skal man implementere og ha ansvaret for lagring, uten at man egentlig vet konsekvensene og kostnadene ved dette» (Stortinget, 2011, s. 3235). Sitatet til Hoksrud er interessant i lys av sitatet fra Anundsen. Kostnadene som ville blitt brukt på datalagringsdirektivet kunne derfor trolig blitt benyttet på andre sikkerhetstiltak som ifølge FrP ville vært mer egnet til å styrke borgernes sikkerhet. I partiprogrammet til FrP som for øvrig har mye omtale av verdien sikkerhet, skriver partiet blant annet at «politiet må ha nødvendig utstyr og lovmessig grunnlag for å kunne gjøre jobben sin på en effektiv måte. Investeringer i audiovisuelt utstyr og IT utstyr kan bidra til effektivisering av politiets arbeidsmetoder» (FrP, 2009, s. 26). Sitatet ovenfor tyder på at FrP anser teknisk IT-utstyr som et viktig bidrag for å

effektivisere politiets arbeidsmetoder og dermed også statens evne til å bekjempe kriminalitet. Dette til tross for at FrP stiller seg negative til innføringen av datalagringsdirektivet.

FrP var ett av få partier som eksplisitt uttalte i eget partiprogram at terror var en vesentlig sikkerhetspolitisk utfordring da de skriver: «Det er viktig at Norge tar aktiv del i kampen mot terror med deltakelse i internasjonalt samarbeid og internasjonale operasjoner» (FrP, 2009, s. 36). Sitatet er interessant fordi partiet fortsatt er negativt innstilt til datalagringsdirektivet, og mente det ville bidratt til å svekke sikkerheten. Videre skriver FrP i partiprogrammet (2009, s. 38) at «det nye sikkerhetspolitiske bildet er preget av internasjonal terrorisme, spredning av masseødeleggelsesvåpen og uforutsigbare trusler.» Med beskrivelsene av en slik sikkerhetspolitisk situasjon som utgangspunkt, ville det vært naturlig å forvente at FrP i større grad ville stilt seg positiv til innføringen av datalagringsdirektivet. Ifølge Aradau & van Munster (2012, s. 2) blir politikere i dag bedt om å ta sine forhåndsregler, ha fokus på unngåelse, beredskap og å skape robusthet for å håndtere fremtidige uventede hendelser. Videre skriver Lyon (2014, s. 4 – 6) at større informasjonstilgang gjennom etterretningsarbeidet også vil kunne gi myndighetene bedre forutsetninger til å forebygge terrorangrep. Likevel ser det ut til at brudd på prinsipper som FrP anser som viktige, blant annet overvåkning av også uskyldige individer, gjør at partiet likevel velger å gå imot innføringen av datalagringsdirektivet.

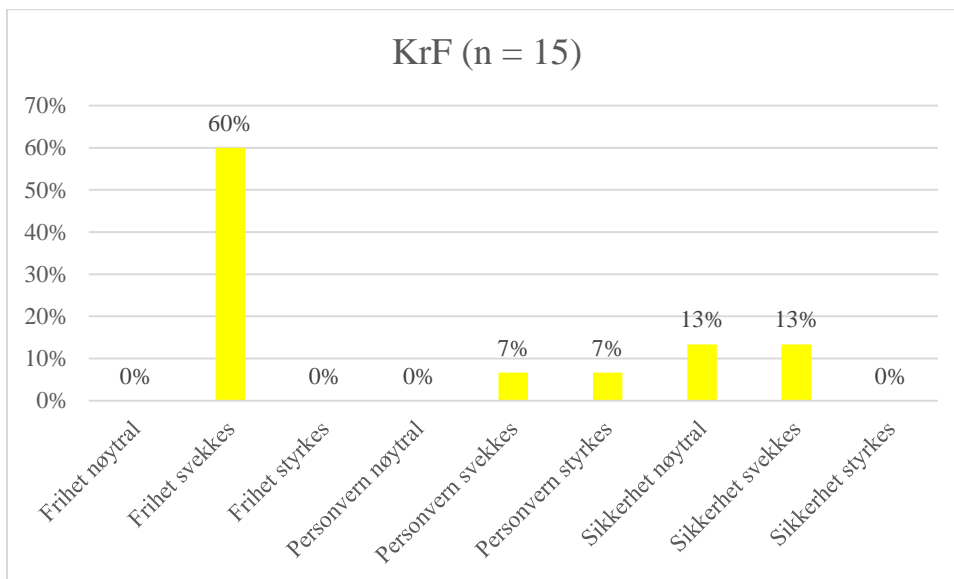
Personvern

FrP uttaler i 16 % av sine innlegg under stortingsdebatten at personvernet vil svekkes. I partiprogrammet for stortingsperioden gir FrP noe omtale til verdien personvern, og skriver blant annet at «innbyggerne skal ha trygghet for at det offentlige ikke kontrollerer privatlivet». Videre presiseres det at saker som gjelder *rikets sikkerhet* og *alvorlig kriminalitet*, kan gi grunnlag for overvåkning (FrP, 2009, s. 26). I enkelte tilfeller kan politiet dermed ha adgang til å foreta legitime inngrep i innbyggernes privatliv ifølge FrP. Partiet skriver ikke konkret om hvor grensen for inngrep skal gå, eller hvilke former for inngrep som vil være legitime. I etterkant av terrorangrepene mot USA den 11. september 2001 har det ifølge Hammerlin (2009, s. 17 – 43) og Engene & Nordenhaug (2008, s. 147) vært en tendens, også i Norge – til å godta innsamling av personopplysninger i hensikt å forebygge terrorangrep. FrP viser til tross for dette at de ønsker en restriktiv praksis når det gjelder innsamling av personopplysninger. Standpunktet til partiet om at direktivet vil bidra til å svekke personvernet, er derfor ikke overraskende.

Fremskrittspartiet oppsummert

FrPs partiprogram kan i noen grad bidra til å forklare partiets synspunkter om at datalagringsdirektivet ville bidra til å svekke borgernes frihet og personvern. Partiprogrammet kan i mindre grad bidra til å forklare hvorfor FrP uttrykker at også sikkerheten vil svekkes som følge av direktivet. Etersom FrP har forholdsvis mye oppmerksomhet om sikkerhetspolitikk og terrorisme som både nasjonal og internasjonal utfordring i sitt partiprogram, ville det vært i naturlig å se for seg at FrP under stortingsdebatten uttrykte seg mer positivt med tanke på innføringen. Til tross for at FrP ikke hadde tatt eksplisitt standpunkt imot datalagringsdirektivet i partiprogrammet fra 2009, kan partiets motstand under stortingsdebatten i 2011 imidlertid forklares av oppmerksomheten om verdien frihet i deres partiprogram. Spesielt forpliktelsen vi finner i setningen «innbyggerne skal ha trygghet for at det offentlige ikke kontrollerer privatlivet» (FrP, 2009, s. 26).

6.2.3 Kristelig Folkeparti (KrF)



Graf 7: Kristelig Folkepartis utsagn under stortingsdebatten

Tabell 8: Sammenlikning av Kristelig Folkepartis partiprogram og standpunkt under stortingsdebatten

Verdi	Frihet	Frihet	Sikkerhet	Sikkerhet	Personvern	Personvern
Dokument	Partiprogram	Stortingsdebatten	Partiprogram	Stortingsdebatten	Partiprogram	Stortingsdebatten
KrF	Noe omtale	Svekkes	Mye omtale	Svekkes/nøytral	Noe omtale	Ingen påvirkning

Frihet

KrF har i sitt partiprogram noe omtale av verdien frihet. Det er spesielt ett sitat i partiprogrammet som går direkte inn i kjernen av dilemmaet mellom frihet og sikkerhet, ved

innføringen av nye overvåkningsmetoder. Sitatet nedenfor tilsier at KrF indirekte, i likhet med FrP – hadde tatt standpunkt mot innføring av datalagringsdirektivet. Dette til tross for at KrF i ikke nevner direktivet eksplisitt i sitatet, eller i partiprogrammet forøvrig.

Politiets Sikkerhetstjeneste (PST) har økende oppgaver i forbindelse med kriminalitet over landegrensene og overvåking mellom landene. Nye overvåkningsmetoder må utformes slik at de ikke krenker personvernet, og overvåking må rettes mot mistenkte, ikke befolkningen som helhet (KrF, 2009, s. 26).

Under stortingsdebatten er hele 60 % av KrFs utsagn kategorisert som frihet svekket. Frihet er altså en verdi som KrF med tydelighet mener vil svekkes. KrFs partiprogram kan bidra til å forklare partiets synspunkter om at datalagringsdirektivet ville bidratt til å svekke borgernes friheter. I lys av sitatet fra KrFs partiprogram «overvåkingen må rettes mot mistenkte, ikke befolkningen som helhet», er det interessant å merke seg hva Dagfinn Høybråten uttaler under stortingsdebatten.

Datalagringsdirektivet – og la oss holde oss til fakta – pålegger alle teleselskaper å lagre hvem du ringer til, hvor du ringer fra, når du ringer, hvor lenge du snakker, hvem du sender SMS til, hvor mottakeren befinner seg, når du er på Internett – hvor lenge – og hvem du sender e-post til [...] Datalagringsdirektivet betyr at alle innbyggerne i Norge i praksis blir fulgt i alle sine bevegelser i disse mediene. Man kan kalle det overvåking eller ikke, men dette er et faktum (Stortinget, 2011, s. 3202).

Sikkerhet

KrF har mye omtale av verdien sikkerhet i partiprogrammet. Under kapittelet *justispolitikk* påpeker partiet at «en av statens viktigste oppgaver er å sørge for trygghet for sine innbyggere», og videre at «KrF vil bekjempe kriminalitet i alle former» (KrF, 2009, s. 24). De to sitatene går inn i kjernen av sikkerhetsdefinisjonen i denne oppgaven, som tar utgangspunkt i begrepet *kriminalitetsbekjempelse*. Kriminalitetsbekjempelse er i NOU 2009:15 (s. 68) definert som «den virksomhet som drives for å hindre at samfunnet og borgerne utsettes for kriminelle handlinger». Når KrF viser til at staten må sørge for sine borgeres trygghet, og partiet samtidig vil bekjempe kriminalitet i alle former – kan kriminalitetsbekjempelse anses som en viktig bidragsyter til nettopp å skape denne tryggheten for borgerne. Når det gjelder forholdet mellom begrepene *sikkerhet* og *trygghet* vises det i NOU 2006:6 (s. 227) *Når sikkerheten er viktigst* til at de to ordene er synonyme, og bærer begge betydningen av det å være sikker eller trygg.

Likevel kan trygghet ifølge Eriksen (2006) sies å være en mer subjektiv følelse sammenliknet med sikkerhet som kan knyttes til mer håndfaste og objektive tiltak.

Under stortingsdebatten tyder 13 % av KrFs innlegg på at de mener sikkerheten vil svekkes, og 13 % av innleggene forholder seg nøytralt til verdien sikkerhet. Datagrunnlaget er likevel noe lite i denne delen av den innholdsanalysen, slik at ingen sikre konklusjoner trekkes fra materialet. Den kvalitative analysen av utsagnene underbygger likevel det faktum at KrF uttaler seg i retning av at datalagringsdirektivet vil påvirke borgernes sikkerhet i negativ retning. Knut Arild Hareide uttaler i en replikk under stortingsdebatten at datalagringsdirektivet ikke er et egnet virkemiddel for å bekjempe enkelte former for kriminalitet. Replikken er svar til et forutgående innlegg av Susanne Bratli (AP), hvor sistnevnte hevder at direktivet vil være egnet til bekjempelse av overgrepsmateriale på internett (Stortinget, 2011, s. 3216). Sitatet fra Hareide, er interessant i lys av hva KrF skriver i partiprogrammet der partiet uttrykker at «KrF vil bekjempe kriminalitet i alle former» (KrF, 2009, s. 24). Hareide ser altså ut til å mene at datalagringsdirektivet ikke vil være et egnet virkemiddel for å bekjempe barnepornografi og overgrepsmateriale da han uttaler:

[...] ein bør bruke andre verkemiddel nettopp for å kjempe mot denne typen kriminalitet. Kristeleg Folkeparti og personvernalliansen har valt å lytte til Redd Barna og til barneombodet, for me trur at det vil kunne gi eit tryggare samfunn (Stortinget, 2011, s. 3216).

Hareides utsagn om at det vil gi et tryggere samfunn ved å bruke andre virkemidler for å bekjempe spredning av overgrepsmateriale, tolkes som et uttrykk for at KrF mener det finnes andre virkemidler enn datalagringsdirektivet til å bekjempe slik kriminalitet. Hareide som uttaler eksplisitt at *andre virkemidler* vil være *bedre egnet*, tolkes i retning av at han mener datalagringsdirektivet vil bidra til å svekke sikkerheten. Nettopp fordi det ifølge Hareide finnes bedre egnede virkemidler å bruke ressursene på, sammenliknet med datalagringsdirektivet. Uten at de alternative virkemidlene er nærmere spesifisert. Argumentasjonen har likheter med FrPs, hvor Anders Anundsen også påpekte at de kriminelle ville unngått slik overvåkning, og at kostnadene derfor burde benyttes på andre sikkerhetstiltak (Stortinget, 2011, s. 3241).

Personvern

KrF gir noe oppmerksomhet til verdien personvern i partiprogrammet, men skriver i mindre grad om konkrete tiltak som vil bidra til å styrke personopplysningsvernet. Ved ett relevant sitat

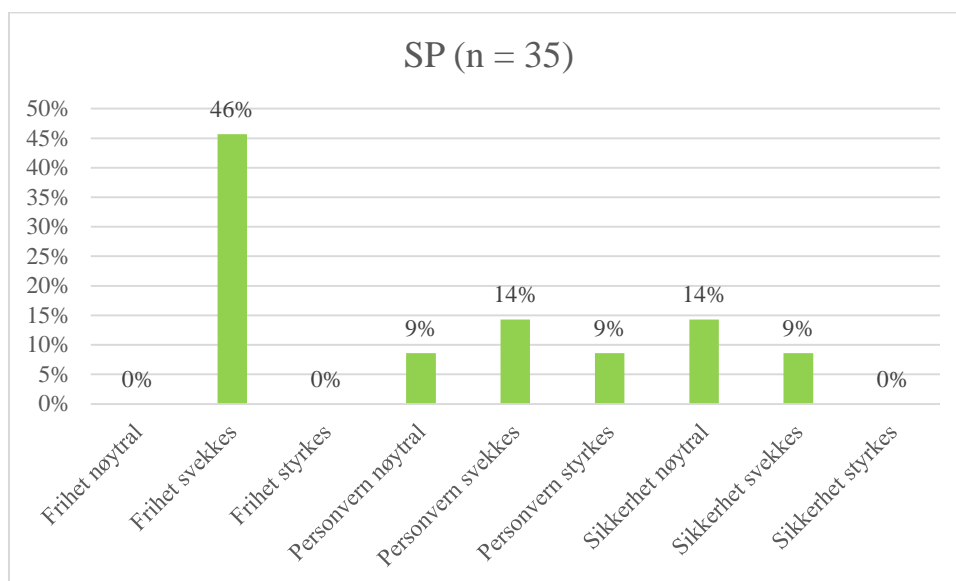
fra partiprogrammet (2009, s. 24), uttrykker KrF at «overvåkning må skje innenfor rammen av forsvarlig personvern». Sitatet viser at partiet hadde et bevisst forhold til at overvåkning påvirker personvernet, til tross for at oppmerksomheten om verdien for øvrig var liten. Den manglende oppmerksomheten om personvern hos KrF kan også spores i stortingsdebatten. Når det gjelder stortingsdebatten er datagrunnlaget for å trekke noen slutninger om KrFs standpunkt når det gjelder personvern, svært lavt. KrF har ett utsagn i hver av kategoriene personvern svekkes (7 %) og personvern styrkes (7 %), hvilket er to motstridene syn om ett og samme tiltak. Likevel kan den begrensede oppmerksomheten som KrF ser ut til å ha om verdien personvern i både partiprogram og stortingsdebatten, i seg selv være et interessant funn fra undersøkelsen. Det kan med andre ord fremstå som at verdien personvern ikke fremstår som spesielt viktig for partiet, til tross for at KrF i partiprogrammet skriver at overvåkingen må foregå innen rammen av forsvarlig personvern. Hva som ifølge KrF vil være forsvarlig med hensyn til personvernet, gir hverken stortingsdebatten eller partiprogrammet noe videre svar på.

Kristelig Folkeparti oppsummert

KrFs partiprogram kan i noen grad se ut til å forklare partiets standpunkt under stortingsdebatten om datalagringsdirektivet. Utsagnet «overvåkning må rettes mot mistenkte, ikke befolkningen som helhet» (KrF, 2009, s. 26) korresponderer med partiets syn på at datalagringsdirektivet vil bidra til å svekke borgernes friheter. Hele 60 % av partiets utsagn under stortingsdebatten tyder på at borgernes frihet vil svekkes ved innføringen av direktivet. Til tross for mye oppmerksomhet om verdien frihet, hadde heller ikke KrF eksplisitt tatt stilling til innføringen av datalagringsdirektivet i eget partiprogram. Når det gjelder personvern, fremgår det av partiprogrammet at KrF kun gir verdien noe oppmerksomhet. Også under stortingsdebatten gir KrF i liten grad uttrykk for hvordan datalagringsdirektivet ville påvirket personvernet, slik at det fremstår som om personvern er en mindre viktig verdig for partiet.

Fra KrFs partiprogram fremgår det at sikkerhet er en viktig verdi for partiet. I partiprogrammet (2009, s. 24) skriver de at «KrF vil bekjempe kriminalitet i alle former». Likevel ser ikke KrF under stortingsdebatten ut til å betrakte datalagringsdirektivet som et egnet virkemiddel for kriminalitetsbekjempelse. Det kan tenkes at KrF ville akseptert sikkerhetstiltak som var mer målrettet, sammenliknet med datalagringsdirektivet. Først og fremst fordi direktivet ville bidratt til innsamling og lagring av trafikk- og lokasjonsdata om alle borgere, og ikke kun de som mistenkes for å planlegge eller å ha begått kriminalitet.

6.2.4 Senterpartiet (SP)



Graf 8: Senterpartiets utsagn under stortingsdebatten

Tabell 9: Sammenlikning av Senterpartiets partiprogram og standpunkt under stortingsdebatten

Verdi	Frihet	Frihet	Sikkerhet	Sikkerhet	Personvern	Personvern
Dokument	Partiprogram	Stortingsdebatten	Partiprogram	Stortingsdebatten	Partiprogram	Stortingsdebatten
SP	Mye omtale	Svekkes	Noe omtale	Nøytral/svekkes	Mye omtale	Nøytral/svekkes

Frihet

I Senterpartiets partiprogram for perioden 2009 – 2013, gir de mye oppmerksomhet til verdien frihet. I partiprogrammet fremgår det innledningsvis at frihet er en viktig verdi for SP (2009, s. 7), da de skriver at «Senterpartiet vil ha frihet for enkeltmennesket. Individet har visse retter i kraft av å være et menneske og borger». Uten at det er gjort skille mellom de to formene for frihet som Berlin (1969, s. 128 – 130) viser til.

Senere i SPs partiprogram (2009, s. 117) omtaler de derimot mer konkret hvordan de negative frihetene blir utfordret. Partiet viser til at «det bør etableres klare grenser for styresmaktens kontroll med den enkelte borgers gjøremål.» SP erkjenner at styresmaktens kontroll med enkeltindividet står i et motsetningsforhold til individets frihet, og at reell ytringsfrihet er en forutsetning for et åpent samfunn – og dermed også et velfungerende demokratisk samfunn. Ifølge Mill (2010, s. 21) er det nettopp friheten til å ytre sine meninger fritt som gir borgerne muligheter til å korrigere hverandres oppfatninger, og dermed kan borgerne bidra til å løfte frem nye sannheter og skape god demokratisk samfunnsutvikling. Til tross for at SP ønsker å ivareta borgernes friheter ved å sette klare grenser for styresmaktens kontroll, ser partiet

samtidig ut til å akseptere innskrenkninger i ytringsfriheten dersom «sterke personvernomsyn og omsyn til privatlivets fred gjør seg gjeldende» (SP, 2009, s. 117). Det fremgår ikke av SPs partiprogram i hvilke situasjoner de mener at ytringsfriheten bør kunne begrenses av personvernomsyn eller hensyn til privatlivets fred. Likevel er SPs tilnærming interessant, fordi partiet uttrykker en tilnærming som er annerledes sammenliknet med de andre stortingspartiene. Frihet og personvern fremstår ved måten som SP argumenterer, som motsetninger. Dette gjelder i tilfeller hvor ytringer kan være til skade for andre enkeltindividers krav på vern fra å få eksponert opplysninger om dem selv. Personvern slik SP omtaler det ved sitatet ovenfor, ser imidlertid i større grad ut til å omhandle det Schartum & Bygrave (2016, s 19) omtaler som *personlig integritet fremfor personopplysningsvern*.

Hobbes (2012, s. 183) argumenterte for at en hersker burde kunne forby ytringer dersom det var nødvendig for å bevare fred, forsvar og statens sikkerhet. SP går på ingen måte like langt som Hobbes i argumentasjonen når partiet skriver at de ønsker å avgrense ytringsfriheten av hensyn til individenes personvern. Til forskjell fra Hobbes er det nettopp enkeltindividet som ifølge SP, skal vernes. Ikke herskeren (staten), slik Hobbes tok til orde for. Likevel er det interessant at SP uttrykker at de ønsker å forby ytringer i visse tilfeller, og på denne måten uttrykker at de er villige til å svekke borgernes ytringsfrihet av hensyn til enkeltindividenes personvern. Likevel ser SPs hovedbudskap ut til å være at det må etableres klare grenser for styresmaktens kontroll med den enkelte borger, og at partiet derfor er restriktive med hensyn til økt overvåkning og svekkelse av borgernes frihet.

Under stortingsdebatten fremgår det av hele 46 % av SPs utsagn at borgernes friheter vil svekkes som følge av datalagringsdirektivet. Stortingsrepresentant Janne Sjelmo Nordås (SP) holder et innlegg under stortingsdebatten hvor hun viser til at overvåkingen kan bli mer omfattende i fremtiden, og at SP derfor ønsker å ha en «føre-var» tilnærming.

Et slags «føre var»-prinsipp tilsier at listen for å iverksette et tiltak ikke kan legges for lavt, da det vil medføre at mange senere tiltak vil kunne bli ansett for å være like nødvendige. Konsekvensen kan bli at den samlede overvåkingen utvikler seg til å bli massiv (Stortinget, 2011, s. 3262).

Paul Larsson (2014, s. 53) viser til at det i Norge har vært tilstede en utglidningseffekt ved bruken av utradisjonelle politimetoder. Politimetoder som tidligere var begrenset til bruk for

etterforskning av alvorlig kriminalitet, anses nå som legitime til bruk for etterforskning av mindre alvorlig kriminalitet. Skillet mellom det forebyggende og det etterforskende politiarbeidet blir ifølge Larsson (2014, s. 54) mer utydelig. Utradisjonelle etterforskningsmetoder som ransaking av personer uten skjellig grunn til mistanke, spaning, postkontroll, telefon- og romavlytting og bruk av informanter benyttes i større grad som forebyggende politimetoder mot potensielle terrorister (Nordenhaug & Engene, s. 2008, s. 40 – 41). Utglidningseffekten som Larsson beskriver, er også interessant i lys av Nancy Lewis' (2005, s. 109 - 111) påstand om at sikkerhetsmiljøene ønsker å ta i bruk mer overvåkningsteknologi ettersom den blir lettere tilgjengelig, billigere og mer brukervennlig. Det kan dermed se ut til at SP også har vurdert mer langsiktige forhold ved datalagringsdirektivet, som kunne bidratt til å svekke borgernes friheter over tid. Partiets syn på frihet under stortingsdebatten ser dermed ut til å korresponderer godt med partiets øvrige syn på frihet i partiprogrammet.

Sikkerhet

Senterpartiet har noe omtale av verdien sikkerhet i sitt partiprogram for stortingsperioden. Det ser imidlertid ut til å være frihet og personvern som er verdiene partiet vier størst oppmerksomhet. Under stortingsdebatten er 14 % av SPs utsagn kategorisert som sikkerhet nøytral, og 9 % av utsagnene som sikkerhet svekkes. Partiet ser dermed ut til å hevde at datalagringsdirektivet først og fremst vil forholde seg nøytralt til verdien sikkerhet, eventuelt ført til en liten svekkelse av sikkerheten.

Personvern

Når det gjelder verdien personvern, fremstår SP som et interessant parti. Under stortingsdebatten er partiet delt i synet på hvordan datalagringsdirektivet ville påvirket verdien. 14 % av utsagnene tyder på at verdien ville blitt svekket, men 9 % tyder på at direktivet ville forholdt seg nøytralt og 9 % at verdien ville blitt styrket. Partiet har et sprikende standpunkt når det gjelder personvern, hvor ingen av de tre nevnte kategoriene utmerker seg nevneverdig. Dataene er dermed tolket i retning av at SP mener direktivet ville forholdt seg nøytralt til verdien personvern.

I partiprogrammet skriver SP (2009, s 117) at «personvern er viktig i et samfunn der mulighetene for overvåkning og kontroll er sterkt økende.» Partiet erkjenner at det er en sammenheng mellom bruk av tvangsmidler som overvåkning, og at slike tvangsmidler vil

påvirke personvernet. Jon Bing (2010, s. 28) skriver at personvern i det moderne samfunn handler om en erkjennelse av at personopplysninger kan danne grunnlag for beslutninger med konsekvenser for enkeltpersoner, og dermed også for utøvelsen av makt. Slik ser argumentasjonen i SPs partiprogram ut til å korrespondere godt med Bings synspunkter. Et eksempel fra stortingsdebatten på en slik tilnærming fremgår også av innlegget til Magnhild Meltveit Kleppa:

Kvifor er innføringa av datalagringsdirektivet ei svekking av personvernet? Svaret er så enkelt som at det blir lagra meir data av fleire aktørar og over lengre tid samanlikna med i dag. Det kan ikkje kallast ei styrking av personvernet. Direktivet inneber ein kraftig auke i registrering av kommunikasjonen vår (Stortinget, 2011, s. 3224).

Samtidig som Kleppa uttaler at direktivet ville bidratt til å svekke personvernet, ser det ut til at SP mener andre elementer av datalagringsdirektivet ville bidratt til å styrke (9 %), eller forholde seg nøytralt (9 %) til personvernet. Janne Sjelmo Nordås uttrykker i sitatet nedenfor at direktivet har enkeltelementer (eksempelvis domstolskontroll) som ville bidratt til å styrke personvernet. Dette til tross for at direktivet i seg selv, slik Kleppa påpeker, ville bidratt til å svekke det samme personvernet igjennom lagring av flere opplysninger som kunne blitt knyttet til enkeltindividet.

Domstolskontroll er en forbedring av personvernet. Men det virker for Senterpartiet merkelig at man først skal gjøre et alvorlig inngrep i personvernet ved å godta direktivet, for så igjen å se om en kan finne måter å løse utfordringene rundt det man nettopp har gjort vedtak om (Stortinget, 2011, s. 3201).

Solove (2008, s. 362) skriver at overvåkningsteknologi ofte vil innføres på bekostning av både frihet og personvern, i hensikt å styrke sikkerheten. Likevel påpeker Solove at det er viktigere å holde oversikt med programmene, forhindre urettmessig bruk av personlige data, og sørge for at programmene utøves på en kontrollert måte – fremfor å tilintetgjøre dem. Når SP uttrykker at datalagringsdirektivet både ville bidratt til å styrke, men samtidig også svekke personvernet – kan partiet fremstå som ambivalent i sitt syn på direktivets virkninger. Likevel kan det være viktig å ta det følgende i betraktning. Til tross for at enkelte elementer i datalagringsdirektivet vil bidra til å svekke personvernet, som eksemplvis ukritisk lagring av trafikk- og lokasjonsdata om alle enkeltindivider, så kan direktivet også inneholde enkeltelementer som styrker kontrollen med de samme dataene. Det er spesielt kontrollen med dataene som er

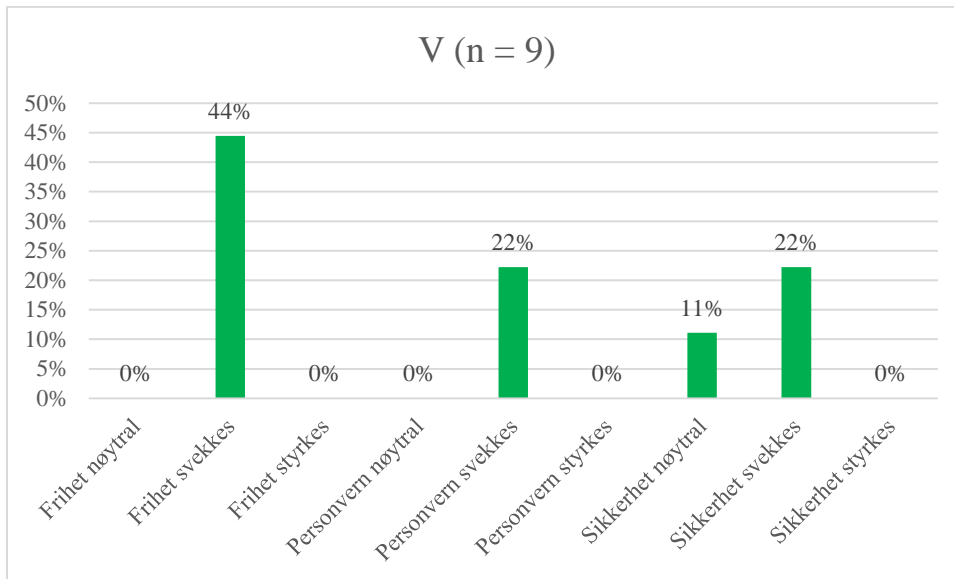
sentralt i Høyre og APs argumentasjon for at personvernet vil styrkes. Et syn som også Bing (2010, s. 28) påpeker viktigheten av, da han argumenterer for kontroll med innsamling, behandling og bruk av personopplysninger i takt med informasjonssamfunnets fremvekst. Likevel viser SP ved Kleppas utsagn at til tross for økt kontroll med lagring av opplysningene, så rettfærdiggjør ikke kontrollen med opplysningene den kraftige økningen i registrering av borgernes kommunikasjon totalt sett.

Senterpartiet oppsummert

Partiprogrammet kan i noen grad forklare SPs standpunkt i stortingsdebatten. At SP uttrykker under stortingsdebatten at direktivet vil bidra til å svekke borgernes friheter, er ikke overraskende. I partiprogrammet har partiet mye omtale av verdiene frihet og personvern, og uttrykker blant annet at «personvern er viktig i et samfunn der mulighetene for overvåkning og kontroll er sterkt økende» (SP, 2009, s. 117). SP viser i det forutgående sitatet at det er en tett kobling mellom personvern, overvåkning og kontroll. Overvåkning og kontroll er ifølge Richards (2013, s. 1948) virkemidler for å utøve makt, og vil dermed bidra til å svekke borgernes friheter. Ettersom SP har mye omtale av verdien personvern i partiprogrammet, og uttrykker under stortingsdebatten at verdien frihet vil svekkes – ville det vært naturlig å se for seg at SP i større grad ville uttrykt at også personvernet ville svekkes. Partiet ser imidlertid ut til å erkjenne at det finnes elementer i datalagringsdirektivet som ville bidratt til å styrke personvernet, eksempelvis domstolskontroll. Samtidig ville direktivet i sin helhet bidratt til å svekke personvernet, gjennom mer omfattende lagring av personopplysninger.

6.3 Partiprogrammet kan i stor grad forklare partiets standpunkt

6.3.1 Venstre (V)



Graf 9: Venstres utsagn under stortingsdebatten

Tabell 10: Sammenlikning av Venstres partiprogram og standpunkt under stortingsdebatten

Verdi	Frihet	Frihet	Sikkerhet	Sikkerhet	Personvern	Personvern
Dokument	Partiprogram	Stortingsdebatten	Partiprogram	Stortingsdebatten	Partiprogram	Stortingsdebatten
Venstre	Mye omtale	Svekkes	Noe omtale	Svekkes	Mye omtale	Svekkes

Frihet

Venstre vier i sitt partiprogram for 2009 – 2013 *Frihet og ansvar* vesentlig oppmerksomhet til verdiene frihet og personvern, og i noen mindre grad verdien sikkerhet. Venstre (2009, s. 5) innleder i sitt partiprogram med at de er «Norges sosialliberale parti.» Partiet er ett av få som i større grad ser ut til å omtale negative friheter (fravær av tvang) fremfor positive (muligheter til). Venstre (2009, s. 5) skriver at «mennesker som gis frihet er best i stand til å ta ansvar for seg selv, sine medmennesker og livsgrunnlaget til våre etterkommere». Partiet fremhever også viktigheten av et velfungerende demokrati ved at staten og interesseorganisasjoner ikke får for stor makt på bekostning av enkeltmennesket og mangfoldet i sivilsamfunnet. Argumentasjonen til Venstre har flere likhetstrekk med Mill (2010, s. 12) sin argumentasjon, hvor borgernes kontroll med myndighetenes maktutøvelse står sentralt.

Demokratiet gir borgerne den endelige makten i samfunnet, og politikkenes spilleregler skal gjøre det mulig å kontrollere myndighetenes maktutøvelse og forandre samfunnet på fredelig vis (Venstre, 2009, s. 6).

Under stortingsdebatten påpekte Venstres representanter at borgernes frihet ville blitt svekket med innføringen av datalagringsdirektivet. Hele 44 % av utsagnene fra partiet er kategorisert som frihet svekkes. Datagrunnlaget fra Venstre under stortingsdebatten er svært lite (n = 9). Likevel uttaler Venstre seg konsekvent under debatten, noe som gjør at den kvalitative innholdsanalysen er med på å utdype funnene. Trine Skei Grande viser i sitatet nedenfor til at samfunnet vil bli mer *usikkert* med datalagringsdirektivet.

Det er faktisk sånn at kriminalitet alltid bekjempes med tradisjonelt, godt politiarbeid, og det er en illusjon å tro at det å samle all informasjon om alle borgere til enhver tid skal gjøre oss til et sikrere samfunn. Jeg er sikker på at det blir et mer usikkert samfunn (Stortinget, 2011, s. 3204).

I tråd med sitatet fra partiprogrammet, hvor Venstre (2009, s. 6) skriver at «demokratiet gir borgerne den endelige makten i samfunnet», er grunn til å tolke Grande at hun mener samfunnet vil bli mer *usikkert* ettersom datalagringsdirektivet vil påvirke maktforholdet mellom borgerne og myndighetene. Myndighetene vil i større grad ha mulighet til å kontrollere borgerne ved innføringen av datalagringsdirektivet. Richards (2013, s. 1935) påpeker at overvåkning er skadelig fordi det nedkjøler individenes vilje til utøvelse av fundamentale borgerrettigheter og deres vilje til å eksperimentere med nye og kontroversielle ideer. I tillegg påvirker overvåkningen maktbalansen mellom de som overvåker og de overvåkede. For Venstre som beskriver seg selv som et liberalt parti, er det nettopp fraværet av reguleringer og tvang fra myndighetenes side som kan beskrives som utgangspunktet for ønsket samfunnsutvikling (Store Norske Leksikon, 2017b).

Venstre er det partiet som i partiprogrammet ser ut til å uttrykke seg mest skeptisk til innføringen av lovhjemler som øker overvåkingen i samfunnet. Partiet som er negativt innstilt til datalagringsdirektivet, er ett av få partier som omtaler EUs datalagringsdirektiv direkte. Venstre viser til at «friheten trues av utilbørlig registrering, overvåkning og inngrep i privatlivet» (Venstre, 2009, s. 67). Partiet uttrykker også forståelse for at det eksisterer et dilemma mellom politiets behov for metoder til kriminalitetsbekjempelse og borgernes krav på frihet. Partiet inntar likevel en posisjon hvor de mener at verdien frihet må veie *tyngre* enn sikkerhet, da de påpeker at overvåkningspraksisen må være restriktiv og borgerne må ha sterke rettssikkerhetsgarantier – også når det kommer til bekjempelse av alvorlig organisert kriminalitet.

Sikkerhet

I Venstres partiprogram for perioden viser partiet til at en rettsstat må ivareta både borgernes frihet og trygghet. *Trygghet* kan i dette tilfellet tolkes å ligge nært begrepet *kriminalitetsbekjempelse* som definert innledningsvis, da overskriften er *justispolitikk*. Justispolitikk handler blant annet handler om å skape trygghet for borgerne gjennom politisk prioritering av sikkerhetstiltak. Ifølge Venstre (2009, s. 67) trues både friheten og tryggheten «av at kriminaliteten har blitt mer organisert og profesjonalisert». Sitatet kan tolkes slik at ved å sørge for bedre kriminalitetsbekjempelse vil altså sikkerheten til borgerne øke, og dermed kan også tryggheten deres øke. Trygghet kan imidlertid sies å være en subjektiv følelse som hvert enkeltindivid innehar, mens sikkerhet i større grad er knyttet til objektive og målbare tiltak (Eriksen, 2006). Innføringen av datalagringsdirektivet eller oppjustering av politiets bemanning, er eksempler på konkrete tiltak for å øke politiets evne til kriminalitetsbekjempelse og dermed også borgernes sikkerhet. Hvorvidt de nevnte tiltakene vil føre til økt trygghet for den enkelte borger, er imidlertid et spørsmål som kun kan besvares ut fra hvert enkelt borgers subjektive ståsted. Benthams fengselsstudie tyder imidlertid på at mennesker som vet at de kan bli overvåket, men som ikke vet når de blir det, opplever liten grad av trygghet. Individene vil ifølge Bentham internalisere selvdisiplinerende væremåter som individene *tror* lever opp til overvåkerens forventninger (Lewis, 2005, s. 101). I en slik sammenheng kan borgernes trygghet paradoksalt nok også svekkes av sikkerhetstiltak og overvåkning. Noe også Engen m.fl. (2016, s. 73 – 74) påpeker at har vært tilfellet i Norge i etterkant av terrorangrepene 22. juli 2011. Trine Skei Grande argumenterer nettopp for et slikt syn under stortingsdebatten, da hun påpeker at samfunnet blir mer *usikkert* ved innføringen av datalagringsdirektivet.

Venstre hevder at borgernes sikkerhet vil svekkes i 22% av utsagnene under stortingsdebatten. I tillegg er ett utsagn (11 %) kategorisert som sikkerhet nøytral. Til tross for et lite datagrunnlag, bidrar utsagnene under stortingsdebatten til å understøtte den kvantitative innholdsanalysen. Sitatet ovenfor, hvor Grande påpeker at det er en illusjon å tro at overvåkning vil bidra til å skape sikkerhet og at kriminalitet bekjempes best med «tradisjonelt» politiarbeid – understøtter funnene.

Personvern

Venstre uttrykker under stortingsdebatten at personvernet vil svekkes med datalagringsdirektivet, da 22 % av utsagnene tyder på dette. Datagrunnlaget er også her noe lite,

men den kvalitative undersøkelsen understøtter funnene. Trine Skei Grande redegjør nedenfor om personvernutfordringer som Venstre mener at innføringen ville medført.

Det kommer også til å føre til at teleselskapene kommer til å prøve å finne den lagringskapasiteten som er billigst. Den er ikke i Norge, den er antageligvis utenfor Norge. Er det slik at Datatilsynet som skal håndheve dette ifølge avtalen – håndheve dette regelverket, sjekke at dette går riktig for seg – også skal få myndighet utenfor Norge? Hvis et teleselskap velger å lagre alle disse opplysningene i Romania – på den serveren som er billigst for det selskapet – skal da Datatilsynet få myndighet til å gå inn overfor rumenske myndigheter for å sikre at dette blir gjennomført på riktig måte? Eller er Datatilsynet begrenset til Norge? (Stortinget, 2011, s. 3236).

Grande uttrykker en bekymring for hvordan kontrollen med norske borgers personopplysninger vil utvikle seg dersom direktivet medfører lagring på dataservere i utlandet. Hvorvidt norske myndigheter, i dette tilfellet Datatilsynet – vil ha juridiske fullmakter til å bedrive tilsyn med lagringen, fremstår ifølge Venstre som uklart. Solove (2008, s. 362) viser til at det er viktig for både personvernet og friheten at myndighetene holder oversikt med overvåkningsprogrammer og at de utøves på en kontrollert måte. Ettersom myndighetenes fokus på forebyggende sikkerhet vokser (Dragu, 2011, s. 4, Aradau & van Munster 2012, s. 2), og overvåkningsteknologien blir bedre, billigere og enklere å ta i bruk (Lewis, 2005, s. 109 - 111), er kontroll med overvåkningsprogrammene viktig. Kontrollen må forhindre urettmessig bruk av innbyggernes personlige data (Solove, 2008, s. 362). Ut fra Grandes utsagn og partiets standpunkt, kan det utledes at kontrollen med personopplysningene ikke vil være tilstrekkelig for Venstre.

Venstre har en egen overskrift for temaet personvern i sitt partiprogram. Under overskriften skriver partiet at informasjonsteknologien og overvåkingen som bedrives av både private og offentlige aktører i dagens samfunn, setter personvernet under press. Venstre (2009, s. 85) skriver videre at de ønsker å «begrense internettleverandørenes mulighet til å lagre og benytte informasjon om data de formidler», og beveger seg slik sett i kjernen av hva datalagringsdirektivet omhandler. Sitatet er nært hva både Schartum og Bygrave (2016, s. 20) og Personvernkommisjonen i NOU 2009:1 (s. 32) beskriver som personopplysningsvern. Altså regler, standarder og normer for behandling av personopplysninger. Trafikk- og lokasjonsdataene som internettleverandørene formidler, er å anse som *personsensitiv* i tråd med tilnærmingen i fagfeltet kvantitativt personvern. Datalagringsdirektivet ville medført en

plikt for internettleverandørene til å lagre disse trafikk- og lokasjonsdataene, og på den måten bidratt til en svekkelse av personopplysningsvernet. Dagens lovverk tilsier at internettleverandørene har plikt til å slette, og ingen plikt til å lagre de nevnte opplysningene (Prop. 49L, 2010, s. 73).

Ettersom det fremgår av Venstres partiprogram (2009, s. 85) at de ønsket «å begrense internettleverandørenes mulighet til å lagre og benytte informasjon om data de formidler», så ville politiets mulighet til å hente ut dataene blitt begrenset. Venstre (2009, s. 72) som eksplisitt uttrykker at de vil «arbeide for å hindre at EUs datalagringsdirektiv blir en del av norsk lov», utelater ingen tvil om partiets standpunkt. Det fremgår av Venstres partiprogram at de ønsker å styrke personvernet samtidig som verdien ifølge partiet også er under press.

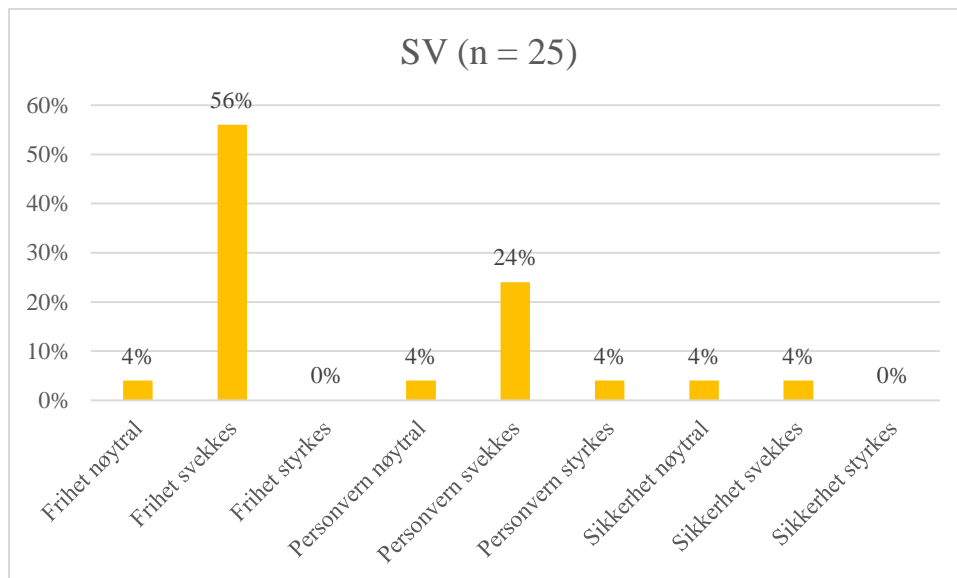
Venstre mener at en stadig utvidelse av politiets metoder kan føre til at individets rettigheter, privatlivets fred og rettssikkerhet bekjempes mer enn kriminalitet og terror (Venstre, 2009, s. 68).

Venstre oppsummert

Venstres partiprogram kan i stor grad forklare partiets synspunkt på datalagringsdirektivet. Partiet gir i partiprogrammet mye oppmerksomhet om verdien frihet og personvern, og noe omtale av verdien sikkerhet. Venstre har i partiprogrammet tatt aktivt standpunkt imot innføringen av EUs datalagringsdirektiv, og skriver at «friheten trues av utilbørlig registrering, overvåkning og inngrep i privatlivet» (Venstre, 2009, s. 67). Under stortingsdebatten fremgår det tydelig at Venstre mener frihet og personvern er verdier som vil svekkes med datalagringsdirektivet. Videre skriver de i partiprogrammet under overskriften *personvern* at partiet vil «begrense internettleverandørenes mulighet til å lagre og benytte informasjon om data de formidler» (Venstre, 2009, s. 85). Når det gjelder sikkerhet, har Venstre kun noe oppmerksomhet om verdien i partiprogrammet. Under stortingsdebatten uttrykker partiet imidlertid at sikkerheten vil svekkes ved innføringen av direktivet. At sikkerheten vil svekkes med innføringen av datalagringsdirektivet, kan fremstå som noe paradoksalt. Ettersom direktivet ifølge både EU (2006) og Justisdepartementet (Prop. 49L, 2010, s. 7) nettopp hadde til hensikt å styrke politiets evne til kriminalitetsbekjempelse. Synspunktet om at direktivet ifølge Venstre vil svekke sikkerheten, forklares av Grandes utsagn hvor representanten påpeker at «kriminalitet alltid bekjempes med tradisjonelt, godt politiarbeid» (Stortinget, 2011, s. 3204).

Ressursene burde ifølge Venstre benyttes på andre måter for å styrke politiets arbeidskapasitet og metoder, fremfor å innføre EUs datalagringsdirektiv i Norge.

6.3.2 Sosialistisk Venstreparti (SV)



Graf 10: Sosialistisk Venstrepartis utsagn under stortingsdebatten

Tabell 11: Sammenlikning av Sosialistisk Venstrepartis partiprogram og standpunkt under stortingsdebatten

Verdi	Frihet	Frihet	Sikkerhet	Sikkerhet	Personvern	Personvern
Dokument	Partiprogram	Stortingsdebatten	Partiprogram	Stortingsdebatten	Partiprogram	Stortingsdebatten
SV	Mye omtale	Svekkes	Lite omtale	Ingen påvirkning	Noe omtale	Svekkes

Frihet

SVs partiprogram fra 2009 gir stor oppmerksomhet til verdien frihet, og noe mindre oppmerksomhet om verdien personvern. Det gis liten oppmerksomhet fra SV til verdien sikkerhet. Partiet som i likhet med både AP og KrF har en tilnærming til fellesskapet fremfor enkeltindividet, innleder i sitt partiprogram med følgende:

[SV vil skape] et samfunn hvor den enkeltes frihet og trygghet garanteres av et sterkt fellesskap. SV arbeider for en verden der alle mennesker har samme menneskeverd, rettigheter og frihet til å ta de viktigste valgene i sitt liv (SV, 2009, s. 3).

I motsetning til de andre partiene med unntak av Venstre, viser SV med tydelighet at de mener verdien frihet taper oppslutning i kampen mot terror. SV (2009, s. 27) skriver under overskriften *demokrati og menneskerettigheter* at «demokratiseringsprosessen ser ut til å ha stanset opp og

autoritære tendenser har vokst frem». Spesielt interessant er SVs utsagn om at også vestlige land har angrepet demokratiske rettigheter under et «dekke av en såkalt krig mot terror». I partiprogrammet skriver de videre at «SV kan ikke akseptere at frykt for terror brukes til å undergrave grunnleggende rettigheter.» Under stortingsdebatten uttrykker SV at frihet vil svekkes i hele 56 % av utsagnene. Bård Vegard Solhjell holder et innlegg hvor han belyser hvordan brudd på uskyldspresumpsjonen vil bidra til å svekke borgernes friheter. Fordi alle borgere vil overvåkes, ikke kun de som mistenkes for å planlegge å begå eller de som har begått kriminalitet.

For det første er det vår sterke overtyding at kvart enkelt menneske er uskuldig til det motsette er bevist. Vi bør ikkje basere oss på ein tankegang i vår rettsstat der vi gir pålegg om å samle spor om kvar nordmann, sidan vi kan kome til å bli skuldige. Då bidreg vi til å endre statusen til kvart menneske, frå uskuldig til potensielt skuldig (Stortinget, 2011, s. 3198).

Solhjell påpeker at vi ikke bør innføre en plikt til å samle spor om alle nordmenn, med begrunnelse om at individene på et senere tidspunkt – kan bli skyldig i kriminalitet. Partiene som stilte seg negative til innføringen av datalagringsdirektivet fordi det ville bidra til å samle trafikk- og lokasjonsdata fra alle borgere, bryter med det Lyon omtaler som en trend. Ifølge Lyon (2014, s. 11) henger ønsket om sterkere nasjonal sikkerhet sammen med fokuset på konsekvenstenking og umiddelbar aktualitet. Lovhjemlede beskyttelser som uskyldighetspresumpsjonen og bevis utover rimelig tvil, risikerer å eroderes. Den fremskridende troen i vestlige samfunn på at mistenkte individer kan isoleres ved hjelp av algoritmer, representerer ifølge Lyon sentrale utfordringer for borgernes friheter. Det fremstår imidlertid av både partiprogrammet og utsagnene til SV under stortingsdebatten, at partiet ønsker å opprettholde borgernes friheter. I særdeleshet gjelder dette ved å nekte tillatelse til innsamling av opplysninger fra individer, som ikke kan mistenkes for å ha begått kriminalitet.

Sikkerhet

Sikkerhet er et tema som SV gir lite oppmerksomhet i partiprogrammet. Under overskriften *velferd* omtaler SV kriminalitetsbekjempelse og sikkerhetspolitikk. Ett av få sitater fra SVs (2009, s. 12) partiprogram tilknyttet verdien sikkerhet, er følgende: «en god politikk for forebygging er det viktigste virkemiddelet mot kriminalitet». Det fremstår imidlertid ukjent hvilke tiltak som SV mener bør settes inn ved forebygging av kriminalitet. Ettersom SV uttrykker seg negativt om datalagringsdirektivet, og går aktivt imot innføringen – er det nokså

åpenbart at SV mener direktivet ikke vil være et godt forebyggende virkemiddel. Under stortingsdebatten gir SV imidlertid i liten grad uttrykk for hvordan direktivet ville påvirket verdien sikkerhet. Kun 4 % av utsagnene er kategorisert som sikkerhet svekkes, og 4 % er kategorisert som sikkerhet nøytral. Ettersom datagrunnlaget er såpass lavt, fremstår det som mindre klart hvordan SV mener at verdien sikkerhet ville blitt påvirket. At SV stilte seg negative til innføringen kan derimot bidra til å forklare at SV ikke gir oppslutning om at direktivet ville bidra til å styrke sikkerheten, slik AP og Høyre uttrykte. På denne måten kan SVs partiprogram bidra til å forklare partiets standpunkt under stortingsdebatten.

Personvern

Personvern er et tema som SV kun gir noe oppmerksomhet i sitt partiprogram. Partiet skriver i kapitlet *mye mer demokrati* at de går imot innføringen av EUs datalagringsdirektiv. SV hadde altså allerede før debatten forpliktet seg til å stemme mot innføringen av direktivet. Videre omtaler partiet problemstillinger rundt overvåkning og personvern generelt, uten at det knyttes til temaene sikkerhet eller kriminalitetsbekjempelse. SV (2009, s. 32) uttrykker blant annet at de ønsker «streng restriksjoner når det gjelder adgang til datalagring av opplysninger om innbyggernes kommunikasjon og bevegelser», noe som tyder på at *personopplysningsvern* i tråd med Schartum og Bygrave (2016, s. 20) og Personvernkommisjonen i NOU 2009:1 (s. 32) definisjoner, fremstår som viktig for partiet. Kommunikasjon og bevegelser er opplysninger som kan anses å være personsensitive da de omhandler det som Schartum og Bygrave (2016, s. 31 – 35) omtaler som *stedlig integritet* og *kommunikasjonsintegritet*. Stedlig integritet handler om respekten for enkeltindividenes private geografiske og fysiske områder. Kommunikasjonsintegritet handler om individenes rett til å kommunisere uforstyrret med andre individer. Ettersom datalagringsdirektivet ville innført en plikt for leverandører av elektronisk kommunikasjon til å lagre lokasjonsdata, ville den stedlige integriteten som SV her ønsker å verne om – blitt svekket. Det samme kan sies om kommunikasjonsintegriteten ettersom direktivet ville innført en plikt til å lagre *trafikkdata*, altså opplysninger om hvem de ulike individene har kommunisert med. Til tross for at datalagringsdirektivet ikke ville bidratt til å lagre selve innholdet i telefonsamtaler eller e-post, så vil det likevel være en svekkelse av personvernet å pålegge lagring som bidrar til å undergrave de ulike integritetsfærene som Schartum og Bygrave beskriver.

Under stortingsdebatten uttrykker SV i 24 % av utsagnene at personvernet vil svekkes. Kun 4 % av utsagnene befinner seg i hver av kategoriene personvern styrkes og personvern nøytral.

Bård Vegard Solhjell tar under stortingsdebatten opp utfordringer rundt integritetskrenkelser tilknyttet personvernet. I likhet med Schartum og Bygrave påpeker Solhjell at registrering av *hvem* man kommuniserer med, kan være integritetskrenkende. Ikke nødvendigvis kun *innholdet* i kommunikasjonen.

Kven du ringer til, kven du sender e-post til, er informasjon som på avvegar kan krenkje din integritet – eksempel: ein mail frå ein tilsett i SV si gruppe til Arbeidstilsynet om tilhøvet i gruppa, fire telefonar til krisesenteret sist helg frå ein kvinneleg representant, eit hemmeleg tips til ein journalist, gjentekne mailer til ei adresse som sluttar med swingersnorge.com. På avvegar kan slike opplysningar krenkje integriteten til dei involverte (Stortinget, 2011, s. 3199).

Ifølge Schartum & Bygrave (2016, s. 31 – 35) ble personvernet i stor grad oppfunnet for å beskytte mot integritetskrenkelser. Fremvekst og bruk av ny teknologi vil imidlertid kunne bidra til å krenke vår integritet, og personvernet må derfor følge den teknologiske utviklingen. Integritetskrenkelser som Solhjell og SV er opptatt av, ville i større grad kunne forekomme ved innføring av datalagringsdirektivet. Schartum & Bygrave (2016, s. 31 – 35) påpeker imidlertid at graden av beskyttelse avhenger av sfærens intimitet og sensitivitet. Jo større grad av intimitet og sensitivitet sfæren representerer, desto viktigere er det å beskytte enkeltmenneskers personopplysninger. Det kan hevdes at opplysningene som ville blitt lagret gjennom datalagringsdirektivet, ikke er av den mest integritetskrenkende arten. Dersom direktivet også lagret *innholdet* i kommunikasjonen, ville det trolig vært å betrakte som mer graverende. Likevel kan direktivet oppfattes som brudd på borgernes rett til beskyttelse av stedlig- og kommunikasjonsintegritet, slik SV påpeker.

Sosialistisk Venstreparti oppsummert

SVs partiprogram kan i stor grad forklare partiets synspunkter. Partiet hadde i likhet med Venstre, allerede i partiprogrammet eksplisitt tatt standpunkt imot innføring av EUs datalagringsdirektiv, og skriver at «SV kan ikke akseptere at frykt for terror brukes til å undergrave grunnleggende rettigheter» (SV, 2009, s. 27). At SV under stortingsdebatten mener at verdien frihet vil svekkes ved innføringen av direktivet, er dermed ikke overraskende. Sikkerhet er en verdi som SV i svært liten grad omtaler i partiprogrammet, og som de gir lite oppmerksomhet under stortingsdebatten. Videre er personvern en verdi som SV gir noe omtale i sitt partiprogram, og som de gir stort uttrykk for at vil svekkes ved innføringen av datalagringsdirektivet. Sitatet om at SV (2009, s. 32) ønsker «strenge restriksjoner når det

gjelder adgang til datalagring av opplysninger om innbyggernes kommunikasjon og bevegelser», kan også tolkes som et tydelig signal på at SV ikke ønsker å bidra til økt overvåkning og datalagring – og dermed også stiller seg kritiske til innføring av datalagringsdirektivet.

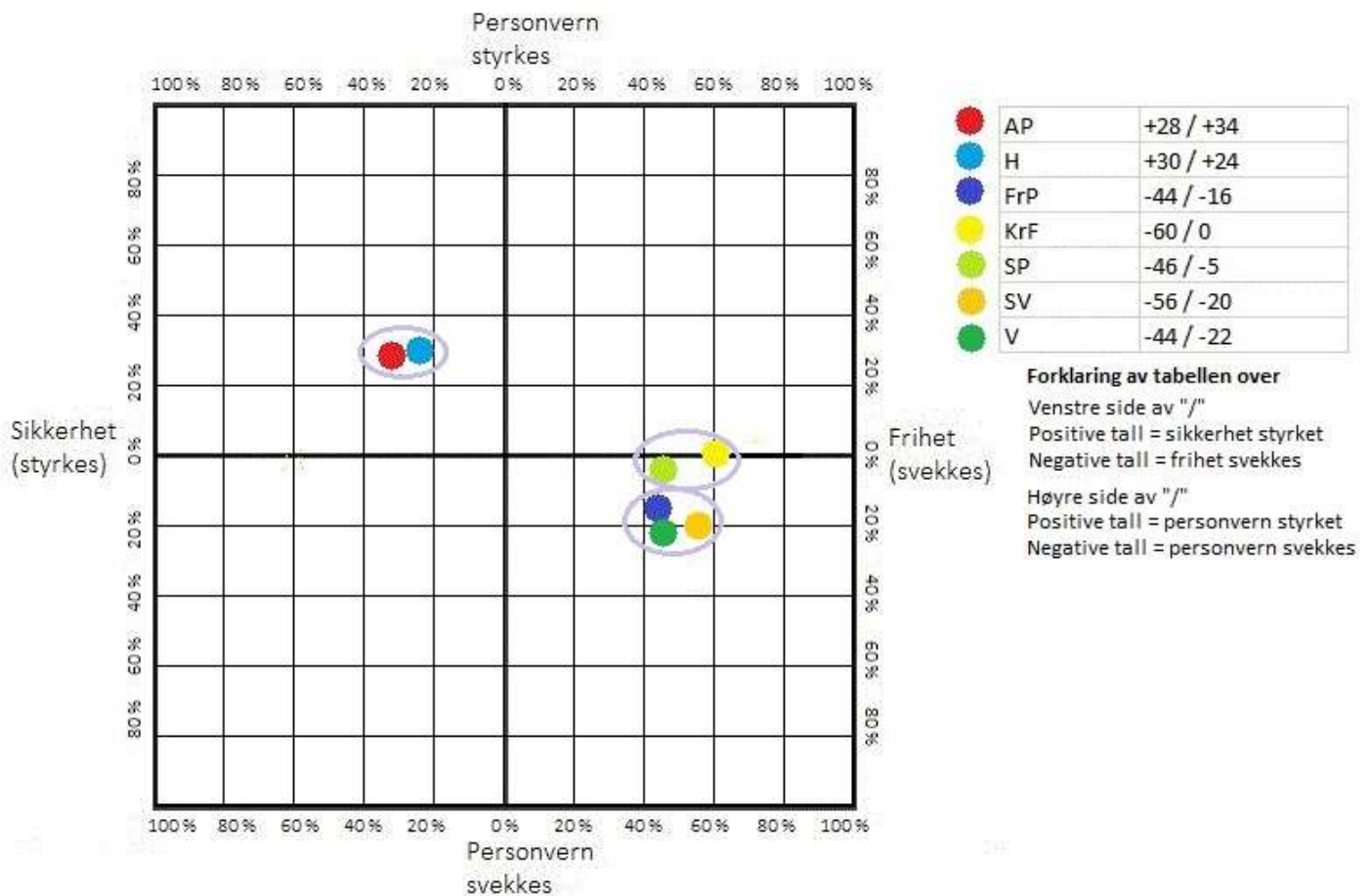
7 Konklusjon

I dette kapitlet vil problemstillingen besvares. Etersom problemstillingen er består av to deler, vil også besvarelsen være todelt. Kapittel 7.1 vil besvare den første delen av problemstillingen: «Hvordan uttrykte de politiske partiene på Stortinget at datalagringsdirektivet ville påvirket verdiene frihet, sikkerhet og personvern under stortingsdebatten i 2011?». Kapittel 7.2 vil besvare den andre delen av problemstillingen: «Hvordan kan partiprogrammene fra 2009 bidra til å forklare stortingspartienes standpunkt under debatten?». Avslutningsvis vil det i kapittel 7.3 knyttes noen kommentarer til begrepsbruk under stortingsdebatten, og i kapittel 7.4 vil det gjøres rede for noen tanker fra forfatteren, om veien videre innen det undersøkte temaet.

7.1 Partienes verdivurderinger

Innholdsanalysen av stortingsdebatten viser at partiene i hovedsak deler seg i tre grupperinger. Figur 4 nedenfor, viser hvordan partiene fordeler seg med utgangspunkt i funnene fra undersøkelsen. På den ene siden finner vi AP og Høyre som uttrykte at både sikkerhet og personvern ville blitt styrket ved innføringen av direktivet. På den motsatte siden finner vi FrP, SV og Venstre som uttrykte at frihet og personvern ville blitt svekket. I mellom de to grupperingene, men med større likhet med FrP, SV og Venstre finner vi partiene SP og KrF som uttrykte at direktivet ville bidratt til å svekke friheter, og samtidig forholde seg nøytralt til verdien personvern. Figuren nedenfor viser hvordan partiene fordeler seg i tre grupperinger, med utgangspunkt i hva partiene uttrykte under stortingsdebatten om datalagringsdirektivet.

I tillegg uttrykte både FrP og Venstre under stortingsdebatten at sikkerheten ville blitt svekket med innføringen av datalagringsdirektivet, uten at dette fremkommer av de utvalgte dimensjonene som representeres i figuren nedenfor.



Figur 4: Partienes verdivurderinger under stortingsdebatten

Ettersom partiene deler seg på en akse hvor de enten mente at sikkerhet styrkes (AP og Høyre) eller frihet svekkes (FrP, KrF, SP, SV og Venstre), tyder dette på at partiene oppfatter verdiene sikkerhet og frihet som motsetninger. Funnet gjelder først og fremst i konteksten av overvåkning og datalagring, som er denne undersøkelsens hovedanliggende. Et slikt syn korresponderer med Hobbes og Mills tilnærminger, hvor også de to politiske tenkerne ser ut til å betrakte verdiene frihet og sikkerhet som motsetninger. I Hobbes (2012, s. 174) tilfelle var det nettopp fravær av sikkerhet som gav grunnlag for at borgerne burde frasi seg noe av friheten, til fordel for sikkerheten som en hersker kunne garantere. Senere mente Mill (2010, s. 31 – 33) at herskeren hadde fått uforholdsmessig mye makt over borgerne, slik at borgerne ble undertrykket og ikke lengre var i stand til å bedrive fri meningsutveksling og sannhetssøken. En debatt med dilemmaet mellom frihet og sikkerhet slik Hobbes og Mill reiste i henholdsvis 1651 og 1859, ser ut til å ha utspilt seg den 4. april 2011, ved stortingsdebatten om datalagringsdirektivet. Denne gangen i en mer høyteknologisk kontekst med innføringen av et lovverk som ville pålagt innsamling og lagring av tele- og lokasjonsdata fra alle individer som benytter elektronisk kommunikasjon.

Personvern har en nær tilknytning til både frihet- og sikkerhetsbegrepet slik Bing (2010, s. 28) påpeker, ettersom personopplysninger kan danne grunnlag for beslutninger med konsekvenser for enkeltpersoner, og dermed også for utøvelsen av makt. I motsetning til verdiene frihet og sikkerhet, hvor partiene deler seg ved standpunktet om at enten så styrkes sikkerheten eller så svekkes friheten – uttrykker partiene i stor grad at personvernet både kan styrkes og svekkes. AP og Høyre uttrykker at personvernet ville blitt styrket, FrP, SV og Venstre uttrykker at personvernet ville blitt svekket, SP uttrykker at personvernet ville forholdt seg nøytralt og KrF uttrykker i mindre grad hvordan personvernet ville blitt påvirket. Partiene tolker de fremtidige *virkningene* når det gjelder personvern svært ulikt som følge av datalagringsdirektivet, slik direktivet er beskrevet i lovforslaget Prop 49L (2010). Blant annet ville innføringen av domstolskontroll, regler for utlevering av opplysninger til politiet og strengere tilsyn med ekomtilbyderne, bidratt til å styrke personopplysningsvernet. Denne tilnærmingen gir AP og Høyre oppslutning til. På den andre siden ville lagring av flere personopplysninger om alle borgere i seg selv kunne betraktes som en svekkelse av personvernet. Et syn som spesielt FrP, SV og Venstre tar til orde for når de påpeker uttrykker at personvernet ville blitt svekket som følge av datalagringsdirektivet. Et sitat under stortingsdebatten som beskriver personverndilemmaet på en interessant måte, uttrykkes fra Janne Sjelmo Nordås (SP):

Domstolskontroll er en forbedring av personvernet. Men det virker for Senterpartiet merkelig at man først skal gjøre et alvorlig inngrep i personvernet ved å godta direktivet, for så igjen å se om en kan finne måter å løse utfordringene rundt det man nettopp har gjort vedtak om (Stortinget, 2011, s. 3201).

7.2 Partiprogram som forklaringsmodell

Partiprogrammene til stortingspartiene kan i de fleste tilfeller bidra til å forklare partienes standpunkter under debatten om innføringen av datalagringsdirektivet. Likevel er det interessant å merke seg at partiprogrammene til motstanderne av direktivet (FrP, SV, SP, Venstre og KrF) i større grad ser ut til å kunne forklare partienes standpunkt, sammenliknet med partiene som var for innføringen av direktivet (AP og Høyre). Det ser ut til at motstanderne av direktivet hadde tatt ett mer *aktivt standpunkt* mot datalagring, overvåkning og innføringen av EUs datalagringsdirektiv, allerede i forkant av stortingsperioden 2009 – 2013. Partiene som i partiprogrammene uttrykte motstand mot overvåkning rettet mot befolkningen som helhet, var også konsistente i det samme budskapet under stortingsdebatten. AP og Høyre som ønsket

innføring av datalagringsdirektivet, var derimot ikke like konsistente i sitt budskap når partiprogram og utsagn fra stortingsdebatten sammenliknes. De to sistnevnte partiene ser ikke i noen grad ut til å ha forpliktet seg til innføringen av direktivet gjennom sine partiprogrammer for stortingsperioden.

I APs partiprogram uttrykte partiet i liten grad hvordan de stilte seg til overvåkning, datalagring, frihet og personvern. AP kan dermed se ut til å ha spilt med «åpne kort» og i liten grad ha forhåndsforpliktet seg, sammenliknet med de øvrige partiene. Derfor bidrar APs partiprogram i liten grad til å forklare partiets standpunkt under stortingsdebatten. Den manglende oppmerksomheten i APs partiprogram om de undersøkte verdiene, kan imidlertid *indirekte* bidra til å forklare hvorfor enkelte av partiets representanter brukte begreper som overvåkning og personvern på en annerledes og mer upresis måte, sammenliknet med de øvrige partiene.

Høyres partiprogram kan, som det fremgår av den kvalitative undersøkelsen, i noen grad forklare partiets standpunkt under stortingsdebatten. Spesielt gjelder dette Høyres standpunkt under stortingsdebatten om at direktivet ville bidratt til å styrke både sikkerhet og personvern. Likevel er det enkelte setninger i Høyres partiprogram, som gjør deres standpunkt for innføring av direktivet, problematisk. Til dels kan det se ut til at Høyre går imot egne forpliktelser da de i partiprogrammet uttrykker at partiet «stiller seg kritisk til innføringen av nye lover som øker adgangen til, eller omfanget av, overvåkning i samfunnet» og at de ønsker «dokumenterbar effekt» ved innføringen av nye forebyggende tiltak. Under stortingsdebatten uttrykker Michael Tetzschner at datalagringsdirektivet ville økt overvåkningen og dermed også svekke borgernes friheter. Høyre som parti ser på denne måten ut til å tale med to tunger under debatten da partiets representanter inntar to motstridende standpunkter. Motsigelsene får Høyres ønske om å innføre direktivet til å fremstå som et strategisk politisk valg, fremfor en reell overbevisning om at tiltaket ville bidratt til å styrke personvern og sikkerhet, uten å svekke borgernes friheter.

Venstre og SV er de eneste partiene som eksplisitt uttrykker i partiprogrammene at de stiller seg imot innføringen av EUs datalagringsdirektiv. Etersom Venstre og SV under stortingsdebatten uttrykker seg i tråd med forpliktelsene i egne partiprogrammer, er det kun partiprogrammene to de to nevnte partiene som i stor grad kan forklare deres standpunkt under stortingsdebatten. FrP, KrF og SP uttrykker også i sine partiprogrammer at de stiller seg negative eller kritiske til overvåkningstiltak som rettes mot befolkningen som helhet. På denne måten hadde også FrP, KrF og SP tatt stilling imot innføringen av EUs datalagringsdirektiv,

uten at de tre partiene omtalte direktivet eksplisitt i sine respektive partiprogram. Ettersom både FrP og KrF også hadde mye omtale av verdien sikkerhet i sine partiprogrammer, og i tillegg omtalte *terror* som en konkret utfordring, ville det vært naturlig at også de to nevnte partiene uttrykte seg mer positivt om datalagringsdirektivet. Likevel stiller også de to sistnevnte partiene seg negative til innføringen, til tross for deres fokus på sikkerhet. I hovedsak ser både FrP og KrFs begrunnelse ut til å være at direktivet ville bidratt til økt overvåkning og lagring av tele- og lokasjonsdata, om samtlige borgere. Ettersom sikkerhet fremstår som en viktig verdi i partiprogrammene til FrP og KrF og til dels for SP og Venstre, er det tenkelig at innføringen av mer *målrettede tiltak* for å bekjempe kriminalitet, ville vært akseptabelt for de nevnte partiene.

7.3 Begrepsbruk

Det kan fremstå som legitimt å stille spørsmål ved enkelte stortingsrepresentanters bruk av begreper. Som denne undersøkelsen dokumenterer, benyttes eksempelvis begrepet personvern til å forklare fenomener som ofte kan betraktes som motstridende. Eivind Sivertsen (AP) uttrykker under stortingsdebatten at med begrepet personvern, så omtaler han også det som ofte defineres som begrepene frihet og sikkerhet (Stortinget, 2011, s. 3241). Datalagringsdirektivet fremstår som både et teknisk og juridisk svært komplisert tiltak. Det bør ikke forventes at alle og enhver har forutsetninger og kunnskap til å sette seg godt inn i hva tiltaket *er*, og hvilke *virknings* det ville medført for samfunnet. Om våre fremste folkevalgte på Stortinget burde ha forutsetninger til dette, er et legitimt spørsmål å stille. Det som imidlertid bør kunne forventes av våre stortingspolitikere, er et ryddig og presist språk. Et språk som ikke bidrar til å vanskeliggjøre en allerede svært komplisert og dilemmafull debatt. Uppresis begrepsbruk kan fremstå som et hinder for at stortingspolitikerne fører en ryddig debatt, og dermed også handler så godt som overhode mulig – på den norske befolkningens vegne.

Det må også kunne aksepteres at stortingspolitikerne er uenige om hvilke *virknings* direktivet ville medført i det norske samfunnet. Fremtidige virkninger av datalagringsdirektivet er utfordrende å beregne nøyaktig, ettersom det hefter stor usikkerhet med utviklingen som ville fulgt i etterkant av en eventuell innføring. Det faktum at partiene AP og Høyre på den ene siden, og FrP, KrF, SP SV, Venstre betraktet de mulige virkningene såpass forskjellig, er med på å understøtte en slik påstand. Til tross for svært ulikt syn på *virkningene*, burde det innledningsvis før stortingspolitikerne går inn i en slik komplisert debatt – både forventes at de har samme utgangspunkt om hva tiltaket *faktisk er*, og hva *de mener* med de ulike begrepene. På denne

måten ville det vært enklere å diskutere hva de fremtidige *virkningene* av direktivet vil være, og om virkningene er ønskelige, eller ikke. For å få dette til, kan det være nødvendig å øke kunnskapsnivået til våre fremste folkevalgte, i forkant av en slik komplisert debatt. Slik at deltakerne er i stand til å diskutere det konkrete tiltaket, i dette tilfellet datalagringsdirektivet – på de samme premissene. Stortingspolitikere trenger ikke nødvendigvis være tunge fagekspertter innenfor alle politikkområder. Likevel burde det forventes at de innehar tilstrekkelig med kunnskap til å føre en presis og saklig debatt, som til syvende og sist har store konsekvenser for den samme befolkningen som de folkevalgte er gitt mandat til å representere.

7.4 Veien videre

Ifølge Hobbes, (2012, s. 174) var det nettopp naturtilstanden og «alles kamp mot alle» som førte til at borgerne frasa seg noe av sin frihet til fordel for sikkerheten som en hersker kunne garantere. Til tross for at det verken i 2009 eller i dag kan sies å være noen naturtilstand innenfor Norges territoriale landegrenser, kan det likevel argumenteres for at terror og alvorlig kriminalitet, utfordrer statens evne til å sørge for borgernes sikkerhet. For AP og Høyres del, var kriminalitetsbildet i 2011 tilsynelatende tilstrekkelig alvorlig for å tillate innføringen av EUs datalagringsdirektiv, og dermed også innsamlingen av tele- og lokasjonsdata fra samtlige borgere. FrP, KrF, SP, SV og Venstre så derimot ikke ut til å akseptere innføringen av et tiltak som ville bidratt til å samle opplysninger fra samtlige borgere, uten at tiltaket var målrettet og forholdsmessig til bruk for statens kriminalitetsbekjempelse. Et interessant spørsmål til partiene som stilte seg negative til innføringen av datalagringsdirektivet i 2011, er om terror- og kriminalitetsbildet noen gang vil kunne bli så alvorlig at også disse partiene vil tillate overvåkning og datainnsamling fra hele befolkningen. Flere av studiene som er benyttet i den teoretiske gjennomgangen av denne undersøkelsen viser at den statlige overvåkingen har blitt mer omfattende etter terrorangrepene i USA 11. september 2001. Likevel viser denne undersøkelsen at flere av de politiske partiene i Norge stilte seg negative til slik storstilt overvåkning under stortingsdebatten om innføringen av datalagringsdirektivet i 2011. I etterkant av stortingsdebatten den 4. april 2011, har befolkningen i Norge og flere sammenliknbare europeiske land, blant annet Sverige og England, blitt rammet av terror. Et viktig spørsmål i dette henseendet er om partiene ville inntatt et tilsvarende standpunkt dersom innføringen av et tilsvarende sikkerhetstiltak, hadde funnet sted i dag.

Grensen for hvilken makt staten kan utøve ovenfor individet av hensyn til både staten og borgernes egen sikkerhet, er under konstant politisk debatt. Villigheten til å flytte disse grensene og dermed også redusere individets frihet, kan fremstå som mer presserende i etterkant av terrorangrep og andre alvorlige hendelser hvor menneskeliv går tapt. En slik grenseforflytning kan imidlertid over tid vise seg å være negativt i et demokratisk samfunn, hvor ytringsfrihet og meningsutveksling er selve grunnfundamentet for samfunnsutviklingen. Måltrettet bruk av overvåkning og fysiske sikringstiltak som begrenser muligheten til å begå terrorhandlinger, kan derimot vise seg å være effektive, samtidig som at borgernes rett på frihet fra tvang, ivaretas.

Vi vil trolig også i fremtiden se både teknisk og juridisk svært kompliserte stortingsdebatter innen temaet overvåkning. Den 26. august 2016 ble Digitalt Grenseforsvar (DGF) – et noen lunde tilsvarende tiltak, lagt frem for Forsvarsdepartementet. DGF har til hensikt å gi Forsvarets Etterretningstjeneste mulighet for innsyn i digitale datastrømmer som krysser den norske landegrensen (Lysne, 2016, s. 5). DGF kan i likhet med datalagringsdirektivet fremstå som nokså kontroversielt, noe som blant annet bekreftes ved flere av de 126 innleverte høringsuttalelsene (Regjeringen, 2017a). DGF har ulikheter både juridisk og teknisk sammenliknet med datalagringsdirektivet, og skal ifølge Regjeringen (2017b) i utgangspunktet beskytte Norge mot ytre trusler i det digitale rom. Til tross for at politiet i utgangspunktet ikke skal få tilgang til å søke i opplysningene som lagres ved bruk av DGF, vil det likevel kunne oppstå situasjoner hvor informasjonsdeling mellom Etterretningstjenesten, PST og Politiet er nødvendig. Regjeringen (2017b) viser til «kommunikasjon mellom terrorister som planlegger aksjoner i Norge» som et eksempel hvor slik informasjonsutveksling kan være aktuelt. Ifølge Regjeringen (2017b) vil et lovforslag basert på DGF legges frem i løpet av 2018.

Dersom lovforslaget senere vil bli debattert i Stortinget, er det grunn til å anta at tilsvarende dilemmaer og problemstillinger som dokumenteres i denne undersøkelsen, også vil reises ved stortingsbehandlingen av Digitalt Grenseforsvar.

8 Litteraturliste

- Acquisti, A. (2004). *Privacy and security of personal information: Economic incentives and technological solutions*. Publisert i Camp, J. & Lewis, S. *The Economics of Information Security*. Kluwer, Dordrecht.
- Aradau, C. & van Munster, R. (2012). *The Time/Space of Preparedness: Anticipating the "Next Terrorist Attack"*. *Space and Culture* 15 (s. 98-109)
- Bergen, P. Serman, D., Schneider, E. & Calhall, B. (2014). *Do NSA's Bulk Surveillance Programs Stop Terrorists?* New America Foundation.
- Berlin, I. (1969). *Four Essays on Liberty*. Oxford University Press. [Nedlastet 10.02.2017 fra <http://spot.colorado.edu/~pasnau/seminar/berlin.pdf>]
- Bratberg, Ø. (2014). *Tekstanalyse for samfunnsvitere*. Cappelen Damm. Oslo.
- Citron, D. & Gray, D. (2013). *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*. *Harvard Law Review Forum*, Vol. 126.
- Dragu, T. (2011). *Is There a Trade-off Between Security and Liberty? Executive Bias, Privacy Protections, and Terrorism Prevention*. *American Politican Science Review* 105 (s. 64-78)
- Engen, O. A., Kruke, B.I., Lindøe, P., Olsen, K., Olsen, O.E., & Pettersen, K. (2016). *Perspektiver på samfunnssikkerhet*. Cappelen Damm Akademisk. Oslo.
- Graver, H. P. & Harborg, H. (2015). *Datalagring og menneskerettighetene. Utredning til Justisdepartementet og samferdselsdepartementet*. [Nedlastet 10.01.2017 fra https://www.regjeringen.no/contentassets/93528bcf984a48a2a89c89cf757b35ef/utredningdlds_djd2015.pdf]
- Hammerlin, J. (2009). *Terrorindustrien*. Forlaget Manifest. Oslo.
- Hobbes, T. (2012). *Leviathan*. Vidarforlaget. Oslo.
- Hylland Eriksen, T. (2006). *Tryggheten og dens motstandere*. [Nedlastet 11.05.2017 fra <https://www.uio.no/forskning/tverrfak/culcom/publikasjoner/boker/2006/trygghet.html>]
- Jamtvedt, A. (2011). *Datalagringsdirektivets fremstilling i norsk offentlighet* (Masteroppgave). Universitetet i Oslo, Oslo. [Nedlastet 26.02.2017 fra

<https://www.duo.uio.no/bitstream/handle/10852/27321/AnettexJamtvedt.pdf?sequence=1&isAllowed=y>

Krippendorff, K. (2004). *Content Analysis: An Introduction to Its Methodology*. Sage Publications. UK.

Larsson, P. (2014). *Normaliseringen av det unormale*. Nordisk politiforskning 1 (s. 41-57).

Larsson, P. (2011). *Pass opp! Alvorlig organisert kriminalitet*. [Nedlastet 07.08.2017 fra <https://brage.bibsys.no/xmlui/bitstream/handle/11250/174555/pass%20opp.pdf?sequence=1&isAllowed=y>]

Lavik, T. & Fjørtoft, K. (2008). *Filosofi for samfunnsvitere*. Universitetsforlaget. Oslo.

Lewis, N. (2005). *Expanding Surveillance: Connecting biometric information systems to international police cooperation*. Publisert i Zuerik, E. & Salter, M. *Global Surveillance and Policing. Borders, Security, Identity*. Willan Publishing. Cullompton Devon, UK.

Lyon, D. (2014). *Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique*. *Big Data & Society 1*.

Marx, G. (2005). *Some conceptual issues in the study of borders and surveillance*. Publisert i Zuerik, E. & Salter, M. *Global Surveillance and Policing. Borders, Security, Identity*. Willan Publishing. Cullompton Devon, UK.

Mill, J. S. (2010). *On Liberty*. Vidarforlaget. Oslo.

Nordenhaug, I. & Engene, J. O. (2008). *Norge i kamp mot terrorisme*. Universitetsforlaget. Oslo

Nicolaysen, M. (2011). *Datalagringsdirektivet: En diskurs og aktøranalyse av høringsuttalelsene i Norge* (Masteroppgave). Norges tekniske- og naturvitenskapelige universitet, Trondheim. [Nedlastet 26.02.2017 fra https://brage.bibsys.no/xmlui/bitstream/handle/11250/268445/457662_FULLTEXT01.pdf?sequence=1]

Refvik, H. (2011). *Demokrati, personvern og samfunnstryggleik – Ei analyse av deliberativ kvalitet i den norske debatten om EU sitt datalagringsdirektiv* (Masteroppgave). Universitetet i Bergen, Bergen. [Nedlastet 26.02.2017 fra <http://bora.uib.no/bitstream/handle/1956/7364/85229705.pdf?sequence=1&isAllowed=y>]

- Reinan, A. (2016). *Straffbar deltagelse i terrororganisasjon, jf. straffeloven 2005 § 136a* (Masteroppgave). Universitetet i Oslo, Oslo. [Nedlastet 28.08.2017 fra <https://www.duo.uio.no/bitstream/handle/10852/50829/716.pdf?sequence=1&isAllowed=y>]
- Renn, O. (2008). *Risk Governance: Coping with Uncertainty in a Complex World*. Earthscan. London.
- Richards, N. (2013). *The Dangers of Surveillance*. Harvard Law Review 1934.
- Schartum, D. & Bygrave, L. (2016). *Personvern i informasjonssamfunnet, 3. utgave. En innføring i vern av personopplysninger*. Fagbokforlaget. Bergen.
- Solove, D. (2008). *Data Mining and the Security-Liberty Debate*. University of Chicago Law Review: Vol. 75.
- Thagaard, T. (2014). *Systematikk og innlevelse: En innføring i kvalitativ metode*. Fagbokforlaget. Bergen.
- Tversky, A., & Kahneman, D. (1981). *The framing of decisions and the psychology of choice*. Science 21. (s. 453-58)
- Warren, S. & Brandeis, L. (1890). *The Right to Privacy*. Harvard Law Review, Vol. 4, No. 5. (s. 193-220)
- Weber, M. (1997). *Makt og Byråkrati: Essays om politikk og klasse, samfunnsforskning og verdier*. Red Egil Fivelsdal. Gyldendal. Oslo.
- Zuerik, E. & Salter, M. (2005). *Global Surveillance and Policing. Borders, Security, Identity*. Willan Publishing. Cullompton Devon, UK.

8.1 Offentlige dokumenter

- NOU 2009:15. (2009). *Skjult informasjon: Åpen Kontroll: Metodekontrollutvalgets evaluering av lovgivning om politiets bruk av skjulte tvangsmidler og behandling av informasjon i straffesaker*. Oslo. Departementenes servicesenter.
- NOU 2009:1. (2009). *Individ og integritet: Personvern i det digitale samfunnet*. Oslo. Departementenes servicesenter.
- NOU 2012:14. (2012). *Rapport fra 22. juli-kommisjonen*. Oslo. Departementenes servicesenter.

Prop. 49L. (2010 – 2011). *Endringer i ekomloven og straffeprosessloven mv. (Gjennomføring av EUs datalagringsdirektiv i norsk rett)*. Oslo. Justis- og politidepartementet. [Nedlastet 10.01.2017 fra <https://www.regjeringen.no/contentassets/e57fab756ba84b72af8b970327c8ad04/no/pdfs/prp201020110049000dddpdfs.pdf>]

Stortinget. (2011). *Referat fra Stortingsmøtet 4. april 2011*. [Nedlastet 10.01.2017 fra <https://www.stortinget.no/globalassets/pdf/referater/stortinget/2010-2011/s110404.pdf>]

8.2 Andre kilder

Aftenposten. (2017a). *London politiet: 12 pågrepet etter terrorangrepet*. <http://www.aftenposten.no/verden/London-politiet-12-pagrepet-etter-terrorangrepet-622499b.html>

Aftenposten. (2017b). *Lastebilangriper i Stockholm hadde bånd til IS*. <http://www.aftenposten.no/verden/-Lastebilangriper-i-Stockholm-hadde-band-til-IS-619236b.html>

European Union. (2006). *Directive 2006/24/EC of The European Parliament and of The Council*. [Nedlastet 24.04.2017 fra <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006L0024>]

Grunnloven. (1814). *Kongeriket Norges Grunnlov av 17. Mai 1814*. [Nedlastet 20.02.2017 fra <https://lovdata.no/dokument/NL/lov/1814-05-17>]

Lysne, O. (2016). *Digitalt Grenseforsvar* [Nedlastet 19.06.2017 fra <https://www.regjeringen.no/contentassets/ca1f705dbebd48cb9a61889d4cfee6bf/digitalt-grenseforsvar-lysne-ii-utvalget.pdf>]

Politi-loven. (1995). *Lov om politiet av 4. August 1995*. [Nedlastet 20.02.2017 fra <http://www.lovdata.no/all/hl-19950804-053.html>]

Store Norske Leksikon. (2017a). *Verdi*. [Nedlastet 24.04.2017 fra <https://snl.no/verdi>]

Store Norske Leksikon. (2017b). *Liberal*. [Nedlastet 11.05.2017 fra <https://snl.no/liberal>]

Store Norske Leksikon. (2017c). *Normativ*. [Nedlastet 13.06.2017 fra <https://snl.no/normativ>]

Store Norske Leksikon. (2017d). *Uskyldspresumpsjonen*. [Nedlastet 16.06.2017 fra <https://snl.no/uskyldspresumpsjonen>]

Store Norske Leksikon. (2017e). *Paternalisme*. [Nedlastet 07.08.2017 fra <https://snl.no/paternalisme>]

Store Norske Leksikon. (2017f). *Stordata*. [Nedlastet 25.08.2017 fra <https://snl.no/Stordata>]

Store Norske Leksikon (2017g). *Abstrakt*. [Nedlastet 29.08.2017 fra <https://snl.no/abstrakt>]

Stortinget. (2016). *Stortingets forretningsorden: Regler for saksbehandlingen i Stortinget*. [Nedlastet 24.04.2017 fra <https://www.stortinget.no/Stortinget-og-demokratiet/Lover-og-instrukser/Stortingets-forretningsorden/#Kap7>]

Regjeringen. (2017a). *Høring av rapport avgitt av Lysne-II utvalget om Digitalt Grenseforsvar*. [Nedlastet 19.06.2017 fra <https://www.regjeringen.no/no/dokumenter/horing-av-rapport-avgitt-av-lysne-ii-utvalget-om-digitalt-grenseforsvar/id2513635/>]

Regjeringen. (2017b). *Utredet et digitalt grenseforsvar*. [Nedlastet 29.08.2017 fra <https://www.regjeringen.no/no/aktuelt/utredet-et-digitalt-grenseforsvar/id2539809/>]

8.3 Partiprogram

Arbeiderpartiet. (2009). *Skape og dele*. [Nedlastet 28.04.2017 fra <http://www.nsd.uib.no/polsys/data/filer/parti/10337.pdf>]

Fremskrittspartiet. (2009). *FrP fornyer Norge*. [Nedlastet 28.04.2017 fra <http://www.nsd.uib.no/polsys/data/filer/parti/10338.pdf>]

Høyre. (2009). *Muligheter for alle*. [Nedlastet 28.04.2017 fra <http://www.nsd.uib.no/polsys/data/filer/parti/10339.pdf>]

Kristelig Folkeparti. (2009). *KrFs program 2009 – 2013*. [Nedlastet 28.04.2017 fra <http://www.nsd.uib.no/polsys/data/filer/parti/10340.pdf>]

Senterpartiet. (2009). *Ingen tittel*. [Nedlastet 28.04.2017 fra <http://www.nsd.uib.no/polsys/data/filer/parti/10347.pdf>]

Sosialistisk Venstreparti. (2009). *SVs arbeidsprogram for perioden 2009 – 2013*. [Nedlastet 28.04.2017 fra <http://www.nsd.uib.no/polsys/data/filer/parti/10348.pdf>]

Venstre. (2009). *Frihet og ansvar. Et sosialliberalt samfunn*. [Nedlastet 28.04.2017 fra <http://www.nsd.uib.no/polsys/data/filer/parti/10349.pdf>]