Datalagringsdirektivet

En diskurs og aktøranalyse av høringsuttalelsene i Norge

Mikael Nicolaysen

std. nr 692518

SOS3009

Masteroppgave i Sosiologi

Institutt for statsvitenskap og sosiologi

Innholdsfortegnelse

Forord

Jeg vil gjerne takke min veileder Hendrik Spilker for hans evne til å veilede meg under arbeidet med denne oppgaven. Under prosessen har han gitt meg positive og konstruktive tilbakemeldinger. Det har føltes beroligende og motiverende hver gang. I stunder hvor jeg har sittet fast har Spilker hjulpet meg å se potensialer i oppgaven. Samarbeidet har tidvis vært preget perioder med lite kommunikasjon, men det var alltid en motivert veileder som tok i mot meg når jeg tok kontakt.

Om temaet

Utgangspunktet for denne masteroppgaven har vært debatten rundt datalagringsdirektivet med utgangspunkt i høringsuttalelsene. Debatten har vært inn og ut av medias søkelys i Norge helt siden det ble kjent at direktivet kunne være EØS-relevant. Det har vært mange ulike interesser involvert i debatten og denne oppgaven søker å identifisere de *relevante sosiale gruppene* og de *fremtredende diskursene* i høringsuttalelsene.

Direktivets formål har blitt koblet til bekjempelse av terror og alvorlig kriminalitet. PST-sjef Janne Kristiansen har uttalt følgende om direktivet "*Uten datalagringsdirektivet vil Norge bli mer utsatt for terror. Det er et avgjørende verktøy i vårt forebyggende arbeid. Vi bruker lagring av data i alle deler av vår virksomhet. De som vil ramme oss, er avhengige av å bruke datakommunikasjon*" (NOU[3] 2011). Justisminister Knut Storberget har tidligere uttalt at datalagringsdirektivet er viktig for å sikre at politiet fortsatt har et verktøy for å bekjempe alvorlig kriminalitet i en tid der han mener den teknologiske utviklingen går raskt (AP 2010). Andre igjen har påpekt bekymringer for det de mener er faren for økt overvåkning. IKT-Norges Torger Waterhouse har i den sammenheng uttalt følgende "*Dette er et skritt videre i forhold til datalagringen. En aksept for datalagring vil lede til dette og andre systemer som EU nå utvikler*" (Jørgenrud 2010).

Kontroversene rundt datalagringsdirektivet har inneholdt mange ulike hensyn til blant annet økonomi, personvern, etterforskning, overvåkning og kildevern. Den har innholdt motstandere og tilhengere, men også mer usikre aktører som har ønsket mer inngående konsekvensutredninger eller strengere krav. Hvorvidt direktivet har vært EØS-relevant har også blitt trekt frem og mens noen har ønsket at Norge skulle ta i bruk reservasjonsretten har andre igjen bare ytret behovet for en utredning av muligheten for å reservere seg mot direktivet. Det diskursive landskapet er med andre ord vidt og det er mange ulike aktører som har vært involvert i prosessen rundt høringsuttalelsene.

Trafikkdataene vi etterlater oss på nett er dessuten ikke bare interessant for etterretningstjenestene. Private aktører har lenge vist interesse for denne typen data. I første rekke har de ulike teletjenestene brukt dataene for faktureringsformål, noe som har vært utgangspunktet for tilgjengeligheten det offentlige gjennom politi og påtalemyndighetenes har hatt til denne typen data tidligere. Trafikkdata har også hatt betydning for markedsføring på nett. Google som er en av verdens mest brukte søketjenester lagrer for eksempel alle søkene

dine og om du har en Gmail-konto kan denne informasjonen kobles direkte til din brukerkonto. Denne informasjonen kan du selv finne om du sjekker ut webapplikasjonen "Google Web History" (Olsen 2008). Amazon.com som er en av verdens mest populære nettsider for kjøp og salg opplyste så tidlig som i år 2000 at de endret sin praksis i forhold til kundedata og åpnet for å selge disse opplysningene til andre selskaper (Kvistad 2000). Trafikkdata har med andre ord vært verdifulle opplysninger ganske lenge.

Elektronisk kommunikasjon kan på mange måter anses som en frigjøringsteknologi gjennom den innvirkningen den har for kommunikasjon på lokalt, nasjonalt og globalt nivå. Under demonstrasjonene i Iran ble blant annet Twitter trukket frem som en medvirkende årsak til at de som demonstrerte fikk kommunisert med hverandre og resten av verden. "*Well developed Twitter lists showed a constant stream of situation updates and links to photos and videos, all of which painted a portrait of the developing turmoil*" (Washington Times 2009). Internett har potensiale for å spre informasjon, men det etterlates også mye informasjon av brukerne. Dette åpner opp for at den elektroniske kommunikasjonen kan spores og et sentralt spørsmål er om den da kan kontrolleres.

Problemstilling

Denne oppgaven har som formål å se på diskursene som ble satt i spill rundt datalagringsdirektivet og hvilke aktører som har vært involvert i disse diskursene. Oppgaven begrenser seg til de norske høringsuttalelsene og tar utgangspunkt i van Dijks (2009) diskursideologiske tilnærming og Bijkers (1997, 2009) SCOT-analyse. Den diskursideologiske tilnærmingen er valgt med tanke på de ideologiske ulikhetene mellom aktørene, mens Bijkers SCOT-analyse er valgt med tanke på å kartlegge de relevante sosiale gruppene Siden disse analyseverktøyene blir brukt i kombinasjon vil den diskursanalytiske delen bli brukt for å kategorisere aktørene rundt datalagringsdirektivet. Målet med SCOT-analysen er deretter å identifisere de relevante sosiale aktørene og utdype relasjonene mellom dem gjennom diskursene. Debatten har i media virket to-sidig med to klare fronter. Jeg ønsker å se nærmere på argumentene til aktørene som har involvert seg og gå dypere inn i debatten. Hannemyrs (2002) Foucault-inspirerte *virtuelle panoptikon* gir bakgrunn for å diskutere om datalagring kan oppfattes som en overvåkningsteknologi.

Hvilke diskurser er det som har blitt satt i spill rundt datalagringsdirektivet? Hvilke aktører har vært involvert i disse diskursene?

Datalagringsdirektivet bakgrunn og historie

EU vedtok 15.mars 2006 direktiv 2006/24/EF som åpnet for lagring av data fremkommet ved bruk av elektronisk kommunikasjon. Samferdselsdepartementet opprettet samme år en interdepertemental arbeidsgruppe bestående av Justisdepartementet, Fornyings- og administrasjonsdepartementet, Utenriksdepartmentet, Datatilsynet, Post- og teletilsynet og Kripos. Gruppen fikk i oppgave å vurdere direktivet og diskutere spørsmål rundt valgmulighetene knyttet til gjennomføringen. Arbeidet dannet grunnlaget for høringsnotatet som kom ut i 2010. Samferdselsdepartementet søkte ytterligere bistand fra en referansegruppe som ble sammensatt av et representativt utvalg av ekomtilbydere bestående av Telenor, NetCom, Tele2, Telio, TDC, Infonett Røros og Lyse Tele. Post- og teletilsynet og Kripos deltok også i denne referansegruppen. Fokuset her havnet på den potensielle konkurransevridningen og hvem som skulle dekke kostnadene (NOU[1] 2010).

Fristen for implementering av direktivet for EUs medlemsland ble satt til 15. september 2007. Direktivet åpnet videre for en utsatt implementering knyttet til internett, bredbåndstelefoni og e-post til mars 2009. Direktivet ble ikke umiddelbart lagt til i EØS-avtalen på bakgrunn av at Norge ønsket å avvente utfallet av rettsaken Irland førte mot Ministerrådet og EU-parlamentet. Det ble stillt spørsmål til direktivets rettslige grunnlag siden det ble vedtatt med hjemmel i artikkel 95 i EF-traktaten. Irland mente regelverket burde blitt vedtatt som en rammebeslutning med hjemmel i del VI av EU-traktaten (politi- og strafferettssamarbeidet). Utfallet av rettsaken kom 10. februar 2009 og den slo fast at artikkel 95 i EF-traktaten var riktig hjemmel for direktivet. Denne avgjørelsen ble gjort fordi direktivet utelukkende regulerer tilbydernes plikt til å lagre data og ikke inneholder bestemmelser om rettshåndhevendes myndigheters tilgang til eller bruk av opplysningene. Domstolen viste også til at en rekke medlemsstater etter terroristangrepene 11. september 2001 i New York, 11. mars 2004 i Madrid og 7. juli 2005 hadde vedtatt regler om datalagring. Noe flere stater etterhvert hadde planer om å følge opp. På bakgrunn av de økonomiske konsekvensene for tilbyderne ble direktivet direkte knyttet til det indre markedet (NOU[1] 2010).

Norge var tidlig i prosessen avventende til å ta stilling til innlemming av direktivet. I høringsnotatet blir det blant annet trekt frem at tilbydere i Norge allerede lagret data til kommersielle forhold og at politiet hadde tilgang til disse dataene dersom de ønsket å etterforske eller forebygge straffbare handlinger. Det nye med datalagringsdirektivet var en pålagt lagringsplikt gjennom en utvidelse av dataene som skulle lagres og lagringstiden. Noe som kunne beskrives som en vridning fra kommersielle behov og over til behovet for kriminalitetsbekjempelse. Dataene som nå skulle lagres var trafikkdata, lokaliseringsdata og abonnoments/brukerdata som fremkommer av elektronisk kommunikasjon som fasttelefoni, mobiltelefoni og internettaksess, brebåndstelefoni og e-post. Denne endringen reiste i følge høringsnotatet spørsmål rundt personvern, kriminalitetsbekjempelse og rammevilkårene for ekomnett og -tjenester. Departementene la derfor vekt på krav til datasikkerhet, personvern og like regler for tilbyderne for å hindre konkurransevridning (NOU[1] 2010).

Formålet med direktivet var å harmonisere lovgivningen om lagring av data med nærmere definisjoner av hvilke data som skulle lagres. Hensikten i følge høringsnotatet var å gi justismyndighetene et verktøy til å avdekke, etterforske og rettsforfølge alvorlig kriminalitet. Det er imidlertid åpent for nasjonale myndigheter å ta nærmere stilling til flere viktige spørsmål. I hovedsak hvem som skal ha tilgang til utlevering av dataene, lagringstiden (6 til 24 måneder), kostnader, lagringsmetode og hvem som skulle ha tilsynsrollen (NOU[1] 2010).

Teleplans økonomiske analyser

Teleplan utførte tre økonomiske utredninger angående kostnadene rundt datalagringsdirektivet (2006, 2008 og 2010). Den første utredningen omhandlet potensielle kostnader for tilbyder og myndigheter. Det ble anslått at investeringskostnaden for tilbyder ville ligge på rundt 72,9 millioner kroner, men her var utviklingskostnaden medregnet. For myndighetene ville kostnaden variere etter hvor lang lagringstiden ble og i forhold til hvilke kostnader de pålegger seg selv. Det laveste estimatet beregnet kun kostnader forbundet med uthenting av trafikkdata (NOU 2006). Utredningen fra 2008 konkluderte med at kostnadene ville bli høyere og estimerte at kostnader relatert til oppgradring og etablering av sentralutstyr og støttesystemer ville ligge mellom 81 og 94 millioner kroner. Kostnader relatert til selve lagringen ville ligge mellom 28 og 44 millioner kroner og kostnader relatert til uthenting av data mellom 13 og 15 millioner kroner. Dette utgjorde en merkostnad for tilbydere på rundt

20 til 25 millioner kroner per år. Til sammen ble kostnadene regnet til å variere mellom 207 og 261 millioner kroner over en femårs-periode for 6 måneders lagring avhengig av hardwareløsning og hvor mye tilpasninger som ville bli krevd av tilbydernes systemer. Økningen til 12 måneders lagring ville imidlertid bare føre til marginale endringer i kostnadsbilde (NOU 2008). Det korrigerte estimatet for den samlede kostnaden i 2010 var på 257 millioner kroner. Økningen i kostnader forbundet med 12 måneders lagring ble fremdeles regnet som lave (NOU[2] 2010).

Lovforslaget

Datalagringsdirektivet ble godkjent i stortinget 4.mars 2011. I lovforslaget fremgår det at en hver fysisk eller juridisk person som tilbyr andre tilgang til elektronisk kommunikasjonsnett som anvendes til offentlig kommunikasjonstjenester eller tilbyr slike tjenester har lagringsplikt. Lagringsplikten vil gjelde trafikkdata, lokaliseringsdata og abonnements/brukerdata som fremkommer av elektronisk kommunikasjon som fasttelefoni, mobiltelefoni, internettaksess, e-post og brebåndstelefoni. Det foreslårs en lagringsplikt på 12 måneder. I vektleggelsen av personvernsmessige hensyn er det ikke foreslått en sentral lagringsløsning. Sikkerheten oppfattes å kunne lagres best gjennom lokal lagring. Post- og teletilsynet og Datatilsynet vil fortsette som tilsynsførere. Dataene kan kun utleveres gjennom en rettslig kjennelse hvor strafferammen er på 4 år eller mer. Dette anses som en sentral rettsikkerhetsgaranti. Det økonomiske ansvaret for tilrettelegging foreslås delt mellom ekomtilbyder og post- og teletilsynet. Økte utgifter for post- og teletilsynet foreslås dekt av økte gebyrer (NOU[1] 2011).

Lovendringen vil tre i kraft senest 1. april 2012 og skal evalueres etter fire år. Lagringstiden (NOU 2011[2])

Datalagringsdirektivet i media

2009

Stopp Datalagringsdirektivet ble stiftet i 2009 som en protestakasjon mot

datalagringsdirektivet. I følge Unanue-Zahl (2009) hadde den bred politisk støtte. Gjennom kampanjer på Facebook og Twitter prøvde motstandere av direktivet å uttøve politisk press mot Datalagringsdirektivet. Politikere fra Frp til Rødt,organisasjoner fra Ja til Eu til Nei til Eu støttet opp om organisasjonen. Det ble vist til en undersøkelse foretatt av tyske myndigheter som viste at direktivet hadde svært marginale konsekvenser for oppklaringsprosenten av kriminalitet (Unanue-Zahl 2009). Tidligere leder for Unge Venstre Lars-Henrik Michelsen ble valgt til leder for Stopp Datalagringsdirektivet. Michelsen fremla at direktivet var en trussel mot personvernet og mente det var snakk om begynnelsen på et omfattende overvåkningsregime vi ikke hadde sett i nyere norsk historie (Bryne[1] 2009). Omdahl la frem argumenter for at direktivet hadde bakgrunn i den amerikanske forestillingen om at det var mulig å føre en "krig mot terror" gjennom å institusjonalisere et kontroll- og overvåkningsregime (Omdahl[1] 2009). Stortinget var tidlig delt rundt spørsmålet om implementering. Justisminister Knut Storberget var tidlig opptatt av å implementere datalagringsdirektivet, men møtte blant annet motstand hos regjeringspartnerne fra senterpartiet som krevde et grundig notat der både ulemper og fordeler måtte belyses (NTB[1] 2009). Under den muntlige spørretimen 04.11.09 var Norges forhold til EU et dominerende tema og KrF-leder Dagfinn Høybråten ville vite om regjeringen var innstillt på å involvere stortinget sterkere i Europa-politikken og nevnte spesifikt tjenestedirektivet og datalagringsdirektivet som saker der regjeringen hadde vært motvillig til å trekke de folkevalgte inn i prosessen. Jonas Gahr Støre lovte her å fremlegge et høringsnotat i 2010 (NTB[2] 2009). Marie Simonsen dro samme dag frem bekymringer rundt kildevernet og beskrev hvordan en kilde nylig hadde krevd at intervjuet skulle skje over en sikker linje. Justisministeren Knut Storberget ble kritisert for sin støtte av datalagringsdirektivet.

"*Knut Storbergets forsvar av datalagringsdirektivet hopper bukk over det skillet når han viser til at data allerede lagres og tidvis brukes av myndighetene i jakten på kriminelle. Som jurist vet han selvfølgelig at forholdet mellom myndigheter og borgere er mer komplisert. Det bygger på grunnleggende prinsipper som privatlivets fred og rettsikkerhet. Til gjengjeld er myndighetene gitt makt*" (Simonsen 2009).

Tilliten mellom myndighetene og folket ville i følge Simonsen bli satt på prøve dersom direktivet ble innført (Simonsen 2009). Arbeiderpartiets Helga Pedersen mente imidlertid at Norge sto i fare for å bli en frihavn for pedofile og kriminelle dersom datalagringsdirektivet ikke ble gjennomført. Det ble samtidig varslet i Soria Moria II at det trolig ville være dissens om datalagringsdirektivet innad i regjeringen. På stortinget hadde FrP, Venstre, SV og SP

slått fast at de ville gå mot direktivet. Flere høyre-politikere var også motstandere av direktivet på denne tiden (Flydal 2009). Solhjell fra Sosialistisk Venstreparti var tidlig ute med å kritisere det han oppfattet som Pedersens "udokumenterte påstander". Solhjell mente det var snakk om overdrivelser som var ødeleggende for debatten (Glomnes 2009).

IKT-Norge var på samme tid av den oppfatning at Arbeiderpartiet spredde feilinformasjon om datalagringsdirektivet og bidro til usikkerhet rundt datalagringsdirektivet. Arbeiderpartiet ble blant annet kritisert for å fremstille det som om ingen nye data ville bli lagret i forhold til datidens ordning (Eltvik 2009). Omdahl mente på samme tid at det hadde vært stille en stund rundt det han omtalte som det omstridte datalagringsdirektivet. Regjeringen var fremdeles splittet mellom småpartiene Sosialistisk Venstreparti og Senterpartiet som motstandere og Arbeiderparitet som var for. Det ble trekt frem at datalagringsdirektivet kom til å erstatte etterforskningsprinsippet der informasjon om alle borgere ville bli lagret systematisk og forbli det i lengre tid. Datalagringsdirektivet ble derfor igjen sammenlignet med et overvåkningsregime og Omdahl (2009) mente det fremdeles ikke var forsent å si nei (Omdahl[2] 2009).

2010

Filosof og forfatter av boken Terrorindustrien Jon Wessel-Aas kom i 2010 med en kronikk om hvordan alle borgere ville være under mistanke dersom direktivet ble innført. Høyre på dette tidspunktet hadde ikke tatt stilling til direktivet, men åpnet samtidig opp for å si ja etter en intern høringsprosess og et resolusjonsforslag. Wessel-Aas mente debatten hadde skiftet spor fra det prinsipielle og over til nødvendigheten, realpolitikken og Norge som potensiell frihavn for kriminelle (Wessel-Aas 2010). I høringsnotatet til forsvarsdepartementet ble det i følge Egeberg (2010) uttrykt stor skepsis og bekymring rundt datalagringsdirektivet. Det var bekymringer rundt hvordan spioner, terrorister eller andre fremmede aktører ved hjelp av hacking eller utro tjenere kunne få tilgang til de lagrede opplysningene. Det ble reagert på de ulike lagringsmetodene av dataene som ble skissert i direktivet. Forsvarsledelsen stillte spørsmålstegn ved kompetansen norske myndigheter hadde til å stille krav til informasjonssikkerhet og føre tilsyn med at kravene ble opprettholdt (Egeberg 2010). Forsvarsminister Grete Faremo tilbakeviste senere påstanden om at forsvarsdepartementet var mot innføringen av datalagringsdirektivet i en pressemelding hvor hun gav uttrykk for at

forsvaret kun gav uttrykk for at de fryktet at informasjon om norske borgere skulle komme på avveie (NOU[3] 2010). Lars Erik Fjørtoft i revisjonsselskapet KPMG uttalte imidlertid til Nettavisen om at sannsynligheten for at dataer om oss ville komme på avveie var stor og mente en sentral løsning ville føre til et veldig attraktivt mål for hackere og alle andre som ville ha interesse av informasjonen (Blaker 2010)

Både Kristelig Folkeparti og Fremskrittsparitet stillte seg i 2010 positive til Senterpartiets forslag om et nasjonalt kompromiss om personvern. Høyreleder Erna Solberg kritiserte imidlertidig forslaget kraftig og beskyldte Senterpartiet for å lage EU-kamp ut av personvernsdebatten. Denne kritikken ble i etterkant tilbakevist av Fremskrittspartiet (NTB 2010).

2011

Datalagringsdirektivet ble innført i Norge den 04.04.2011 og ble vedtatt med 89 stemmer mot 80 etter en langvarig debatt på stortinget. Det var tidlig klart at direktivet ville få gjennomslag ettersom Høyre og Arbeiderpartiet hadde kommet til enighet om rammene og enkeltelementene i det. Motstanderne på stortinget krevde likevel at behandlingen skulle utsettes i påvente av EUs egen evaluering av direktivet, men siden Høyre og Arbeiderparti hadde flertall ignorerte de resten av stortinget på dette punktet. Venstre-leder Trine Skei Grande uttalte at de som hadde stemt for direktivet ikke hadde skjønnt hva de hadde stemt på. Det var imidlertidig fem høyrerepresentanter som brøt med partileder Erna Solberg. Erna Solberg var imidlertidig fornøyd med å få på plass en regulering av det hun omtalte som et delvis rettsløst område i det norske samfunnet med påfallende strenge lovreguleringer. Solberg mente direktivet hadde fått gjennomslag for både personvernet og kriminalitetsforkjempelse. Sosialistisk Venstrepartis parlamentiske leder Bård Vegar Solhjell mente det burde være rom for litt "slark" og argumenterte for at direktivet ville føre til masseovervåkning av hvert eneste feilgrep. Fremskrittspartiets Bård Hoksrud mente stortinget hadde gitt politiet virkemidler som Stasi og KGB kunne vært misunnelig over. Venstres leder beskyldte arbeiderpartiets Martin Kolberg for å ikke ha forstått rekkevidden av hva han hadde klart å få Høyre med på og mente behandling av direktivet kunne kategoriseres som useriøs (NTB[1] 2011). I etterkant av implementeringen ble flere av politikerene som hadde stemt for direktivet utsatt for hets og trusler. Anette Trettebergstuen fikk følgende meldinger "Vi vet hvor du bor", "din jævel" og "Dette skal dere få svi for" (Færaas 2010).

EU-kommissær Cecilia Malmström la etter litt over en måned frem Kommisjonens evaluering av datalagringsdirektivet som pålegger alle land i EØS-området lagring av trafikkdata i 6-24 måneder. I følge rapporten var det store forskjeller i måten direktivet hadde blitt innført i de ulike EU-landene når det gjaldt hvem som skulle ha tilgang og hvordan politi- og påtalemyndighet skulle gå frem for å få dem utlevert. I mange land var det ikke bare politi- og påtalemyndighet som fikk innblikk i de lagrede trafikkdataene. Det var også land som ikke krevde en domstolsavgjørelse for å gi myndighetene tillatelse til å hente ut opplysninger. Det påpekes imidlertid i den samme artikkelen at dette vil bli strengt regulert i Norge og at det vil være en høy straffeterskel for saker der politiet kan begjære innsyn. Alle forespørsler må dessuten behandles av en domstol. Avslutningsvis nevner artikkelen at Sverige og Østerrike enda ikke har innført direktivet og Sverige har blitt pålagt bøter av EU-domstolen som en konsekvens av denne uthalingen. I Romania, Tyskland og Tsjekkia har grunnlovsdomstolene underkjent den nasjonale lovanvendelsen og selv om DLD er innført mangler implemteringene selve innholdet i direktivet (NTB[2] 2011).

Oppgavens struktur

Oppgaven startet med et kort forord og en introduksjon av temaet og problemstillingen. Den gikk videre til å si litt om datalagringsdirektivets bakgrunn og historie hvor teleplans økonomiske analyser og lovforslaget etter at direktivet ble stemt inn i stortinget ble tatt med. Oppgaven fortsatte med en gjennomgang av datalagringsdirektivets tid i media. Vi skal nå gå videre til metoden hvor jeg vil utdype bakgrunnen for analysen, fremgangsmåten til forarbeidet og til slutt kildebruk og kritikk. Etter metoden går vi gjennom de teoriene som brukes i analysen. Først vil jeg si litt om virtuelle panoptikon før jeg går inn på teorien rundt de to analyseverktøyene jeg har valgt. Den diskursanalytiske tilnærmingen tar for seg teorier rundt van Dijks (2009) diskursive ideologier og Neumann (2000) beskrivelse av diskursens materialitet. Like etter introduseres Bijkers (1997, 2009)SCOT-analyse. Oppgaven begynner deretter på analysen hvor de empiriske funnene blir trekt frem. Hoveddiskursene gjennom overvåkningsdiskursen og etterforskningsdiskursen blir først introdusert. Etter det tar vi for oss nytteverdidiskursene og hvordan de relaterer seg til hoveddiskursene. Når det er gjort går vi videre til personvernsdiskursen som settes opp mot sikkerhetshetsdiskursen som følger like etter. Til slutt trekker denne delen av oppgaven frem den tredje hoveddiskursen som er identifisert som økonomidiskursen. Her går vi igjennom ulike økonomiske hensyn som aktørene innenfor økonomidiskursen har trekt frem. Oppgaven følger deretter opp med en

oppsummering og analyse av hovedfunn før oppgaven konkluderes. Oppgaven inneholder 2 vedlegg (Diskurskart og appendix).

Metode

Bakgrunn

Oppgaven tar utgangspunkt i en diskursanalyse og kombineres med SCOT. Datamateriale baserer seg på høringsuttalelsene som kom i forbindelse med høringsnotatet angående datalagringsdirektivet. På tidspunktet når høringsuttalelsene ble hentet ned var det kommet opp 115 høringsuttalelser (10.05.10). Dokumentene er å finne på regjeringen.no i søkbare PDF-dokumenter. Siden omfanget er såpass stort har det ikke blitt trekt inn andre empirikilder i selve analysen. Omfanget har imidlertid ført til begrensninger i forhold til hva som har kommet i fokus. Mange høringsuttalelser har hatt spesifikke forslag til blant annet lagringstid. I denne oppgaven kommer slike detaljer litt i bakgrunnen til den delen av høringsuttalelsene som har mer ideologisk substans. Det som kan gå tapt i en slik tilnærming er en mer raffinert inndeling av de ulike aktørene. Det er for eksempel forskjell på de som yttrer et ønske om minimum lagringstid på 6 måneder og de som ønsker opp til 2 års lagringstid. Denne oppgaven tar heller til sikte å fordele aktører innenfor ulike diskurser og hvordan disse står i relasjon til hverandre. På denne måten ønsker jeg å få et enklere overblikk over konstillasjonene som oppstår mellom grupper som ikke nødvendigvis har de samme ideologiske interessene.

Fremgangsmåte

Arbeidet med høringsuttalelsene begynte med en inndeling som baserte seg på om uttalelsen kom fra *foreninger og forbund, interesseorganisasjoner, media, myndigheter, næringslivet, politiske partier, privatpersoner, universiteter og høgskoler* eller om de var *uten merknad*. Denne inndelingen ble gjort delvis intuitivt når det gjaldt organisasjoner jeg kjente til fra før og de organisasjonene som var ukjent for meg ble etterhvert søkt opp. Jeg ønsker å utdype hva jeg mener med interesseorganisasjoner siden denne gruppen ikke er like intuitiv som de andre. En interesseorganisasjon er i denne sammenheng brukt om organisasjoner som hadde klare motiver i forhold til datalagringsdirektivet. Elektronisk Forpost Norge og senere Stopp

Datalagringsdirektivet var for eksempel tidlige motstandere av direktivet og gav klart uttrykk for det i media. Hewlett Packard Norge hadde levert lagringssystemer for datalagringsdirektivet i andre land og hadde med den kompetansen en interesse av å få datalagringsdirektivet implementert. En organisasjon som IFPI hadde på sin sidet en interesse av å få gjennom datalagringsdirektivet på bakgrunn av deres ønske om å bekjempe piratkopiering av film og musikk på nett. Jeg regnet også Nei til EU som en interesseorganisasjon med bakgrunn i deres mostand til EU. Denne kategorien var med andre ord en mangfoldig samling av ulike interesser. En erfaring jeg gjorde tidlig i prosessen var at en del aktører passet inn i flere kategorier. Denne utfordringen ble møtt med en intuitiv tolkning av hvor jeg mente de passet best inn.

Den neste delen av forarbeidet gikk ut på å lage oppsummeringer av alle høringsuttalelsene og kategorisere de innenfor fire kategorier. De fire kategoriene som ble brukt var *motstandere*, *tilhengere*, *økonomiske betenkeligheter* og *tvilerne*. *Tvilerne* ble videre delt inn i de som så behovet for dokumentert virkning, de som så behovet for innflytelse og de som var skeptiske til nytteverdien. *Motstanderne* ble delt inn i forhold til hvilket fokus de hadde i kritikken mot datalagringsdirektivet. Denne kategorien ble delt inn i de som fokuserte på personvernet, de som mente datalagringsdirektivet utfordret demokratiske verdier og de som mente yttringsfriheten sto i fare. *Tilhengerne* ble delt inn i de som hadde kommersielle interesser, etterforskningsinteresser, de som hadde forbehold om strenge krav og de som mente politiets sikkerhetsnøkkel beskyttet personvernet. De med *økonomiske betenkeligheter* ble delt inn i forhold til de som fokuserte på administrative ekstrakostnader, de som fokuserte på økte fasiliteringskostnader og de som fokuserte på konkurranseulemper.

Når jeg ble ferdig med forarbeidet begynte jeg å identifisere diskurser og hvordan de relaterte seg til hverandre. Jeg identifiserte to hoveddiskurser gjennom overvåkningsdiskursen og etterforskningsdiskursen. Under *overvåkningsdiskursen* identifiserte jeg relasjoner til personvernsdiskurser, omgåelsesdiskursen, utglidningsdiskursen og i mindre grad økonomiske diskurser fra hovedsakelig ekomtilbydere. Jeg identifiserte at omgåelsesdiskursen og utglidningsdiskursen hengte sammen fordi utglidningsdiskursen blant annet bruker omgåelsesdiskursen for å argumentere for utglidningsfaren. Personverndiskursene tar utgangspunkt i frimodighetsdiskursen og rettsprinsippdiskursen. Jeg identifiserte at disse diskursene hengte sammen fordi det er snakk om forventninger til rettsstaten innenfor rettsprinsippdiskursen mens frimodighetsdiskursen tar for seg potensielle konsekvenser av det

som oppfattes som et brudd med gjeldende rettsprinsipper. Kildevernsdiskursen er bekymringer som hovedsakelig er ytret med hensyn til journalistikk, mens barns beste diskursen tar for seg en interessant vri på barns interesser i forhold til personvernet. Ekomtilbyderne er ikke i utgangspunktet prinsipielle motstandere av direktivet, men er kritisk til nytteverdien i forhold til kostnadene og tar i noen tilfeller i bruk argumenter fra personvernsdiskursene, spesielt med tanke på kundetillit. Under *etterforskningsdiskursen* identifiserte jeg relasjoner til sikkerhetsdiskursen, behovsdiskursen og risikodiskursen. Sikkerhetsdiskursen har fokus på personvernet, men mente personvernet kunne bli bedre ivaretatt ved implementering av direktivet. Behovsdiskursen og risikodiskursen henger sammen fordi risikoen av å ikke implementere direktivet blir trekt frem når det argumenteres for hvorfor datalagringsdirektivet bør implementeres. Jeg identifiserte at de sistnevnte diskursene sto i kontrast til omgåelsesdiskursen og utglidningsdiskursen fordi de representerte motstridende tilnæmringer til forståelsen av nytteverdien til direktivet. Innenfor *nytteverdidiskursene* finner vi også dokumentasjonsdiskursen som på generelt grunnlag gav uttryk for at ytterligere dokumentasjon er nødvendig før meninger kunne gjøres opp og gav spesielt uttrykk for at direktivet burde ha en merkbar positiv effekt i andre land som har implementert direktivet før Norge implementerte det selv. En oversikt over de nevnte relasjonene kan bli funnet i diskurskartet (vedlegg 1). Det er også en oversikt over datamaterialet i appendixen (vedlegg 2).

Kildebruk og kritikk

Kildemateriale for denne oppgaven er omfattende og det er derfor naturlig at en del som kunne vært relevant har fallt utenfor. Jeg har hovedsakelig ekskludert høringsuttalelser fra privatpersoner, politiske partier, høgskoler og universiteter. Private personer representerte ikke en stor nok sosial gruppe til å anses som spesielt relevante, spesielt med tanke på at det var større sosiale grupper som inkluderte store deler av det som kom frem i disse høringsuttalelsene. Uttalelsene kunne nærmere bestemt knyttes til beskrivelsene som kom fra Stopp Datalagringsdirektivet. Politiske partier ville i utgangspunktet vært en vesentlig gruppe å involvere i diskursene, men stortinget var kun representert gjennom venstre, senterpartiet og rødt. Rødt var det partiet som hadde levert flest høringsuttalelser med representasjon fra hovedpartiet og en rekke fylker (Sogn og Fjordane, Høyanger og Sør-Trøndelag). På bakgrunn av manglende representasjon fra større partier som arbeiderpartiet og fremskrittspartiet valgte jeg å kutte ut politiske partier. Politiske partier er derimot ikke

fraværende i oppgaven og blir presentert under historien og bakgrunnen for datalagringsdirektivet og gjennom datalagringsdirektivets tid i media. I forhold til universiteter og høgskoler var NTNU, UiO, UiT og Høgskolen i Gjøvik representert. Det er interessant å merke seg at de uttalte seg kritisk til direktivet med henvisning til menneskerettigheter og kildevernet. Jeg valgte isteden å fokusere på andre aktører med lignende beskrivelser av datalagringsdirektivet.

Fokuset i oppgaven har vært å få frem beskrivelsene av datalagringsdirektivet på en best mulig måte. Omfanget av høringsuttalelser gjorde det derimot vanskelig å få inkludert alle beskrivelsene. I forhold til aktøranalysen har jeg valgt å fokusere på aktører som har uttalt seg overraskende ut i fra det ideologiske utgangspunktet jeg hadde forventet fra dem. Itillegg har jeg sett nærmere på relasjonene mellom de ulike diskursene.

Det er viktig å påpeke at forskning som involverer et preg av tolkning fort kan medføre en viss innflytelse over de diskursene eller artifaktene man finner. Forskerrollen baserer seg i utgangspunktet på å være så nøytral som mulig, men forskerens egne tolkninger kan likevel bære preg av forutinntatte holdninger. Hva slags teori som brukes, hvilke innfallsvinkler som velges og hva som fremheves er alle potensielle fallgruver for forskeren. Sosiologien har dessuten en lang historie med samfunnskritikk. Teorier og tidligere funn bærer ofte preg av denne tilnærmingen. En ideologisk tilnærming til diskursanalysen kan fort bli mindre nøytral enn hva forskerrollen krever, men gjennom å være fokusert på at det som presenteres ikke skal formidles som sannheter eller usannheter, men isteden som diskurser eller artifakter som representerer ulike måter å beskrive datalagringsdirektivt kan disse fallgruvene i stor grad unngås.

Teori

Virtuelle panoptikon

Overvåkningens pedagogiske funksjon har i følge Hannemyr (2002) en særlig plass i Foucaults maktanalyse. Det klareste eksemplet på denne pedagogiske ideen kommer i følge Hannemyr (2002) frem i begrepet om panoptikon.

Den sentrale standarden for kommunikasjon mellom datamaskiner på internett betegnes med initialene TCP/IP som står for *Transmission Control Protocol* og *Internet Protocol*. Disse loggene gjør det mulig å knytte forbindelser mellom en bestemt dataoverføring på nettet og et bestemt individ. Denne forbindelsen kan imidlertid brytes ved hjelp av en anonymiserende stedfortreder (på engelsk kjent som en anonymizing proxy). Slike muligheter har i følge Hannemyr (2002) ført til at myndigheter i flere land har gjort inngrep i kyberrommets arkitektur. I USA har de blant annet et system som er kjent som *Carnivore* som eksisterer ved siden av TCP/IP og gir FBI muligheten til å overvåke all netttrafkk (Smith et al. 2000 i Hannemyr 2002). Slike systemer kan i følge Hannemyr (2002) sidestilles med konstruksjonen av et virtuelt panoptikon. Konturene av et slikt panoptikon kan i følge Hannemyr (2002) også registreres i statsadvokat Inger Marie Sundes artikkel om endringer i tele- og personvernslovgivningen. I denne artikkelen fremhever Hannemyr (2002) statsadvokatens ønske om å fjerne tilbud for anonyme kommunikasjonstjenester hvor brukeren ikke er identifiserbar for politiet. Det blir også ytret et behov for et register som kan spore bruken tilbake til abonnent og et ønske om minst ett års lagringstid etter at bruken tok sted. Opplysningen må deretter i følge Sunde (2000) kunne utleveres direkte til politiet i forbindelse med etterforskning (Sunde 2000 i Hannemyr 2002). Hannemyr (2002) legger i sin artikkel vekt på at Sunde ikke skiller mellom ordinære borgere og personer som politiet har skjellig grunn til å mistenke for kriminalitet. Tilsvarende ønsker om overvåkning mener Hannemyr (2002) å finne igjen hos politimyndigheter i hele EØS-området og nevner eksempler fra Storbritannia der lovforslag ønsker å gjøre registrering og avlytting av trafikken enklere (*Regulation of Investigatory Powers Bill*). Hannemyr (2002) påpeker en forståelse for hvordan denne typen overvåkningssystemer vil gjøre politiets arbeid enklere, men legger vekt på Foucaults begrep om panoptikon og hvordan denne typen datainnsamling kan ha en disiplinerende funksjon. Denne typen teknologier er i følge Hannemyr (2002) ikke bare

kriminalitetsbekjempende og -forebyggende, men også et apparat for observasjon , informasjonsinnsamling og opplæring av de som blir overvåket (Foucault 1977 i Hannemyr 2002). Hannemyr (2002) referer til lovlig pornografi, informasjon knyttet til seksuelle legninger, sykdommer, alternative livvsyn og radikale politiske bevegelser som sosiale grupper som kan føle seg spesielt utsatt for denne typen datainnsamling.

Den diskursanalytiske tilnærmingen

Å definere en diskursanalyse har tidligere blitt påpekt av blant annet Tayler (2001 i Devereux 2007) som en vanskelige oppgave, men det finnes likevel mange ulike definisjoner. Begrepet har derfor blitt beskrevet som for omfattende og derfor lite stødig (Taylor 2001 i Devereux 2007). Bell og Smith (2007 i Devereux 2007) utdyper i sin definisjon av diskursanalysen at den bør inneholde en nærgående utforskning av tekst som inkluderer visuelle bilder, lyd, tale og skriftspråk. Den bør ta innover seg både formen på teksten, den sosiale konteksten, konstruksjonen, distribusjonen og mottagelsen. Målet er da å forstå og utdype meningene og den sosiale signifikansen til teksten (Smith and Allan 2007 i Devereux 2007) I følge Smith og Bell har Devereux (2003) valgt en mer abstrakt tolkning i sin definisjon av diskursanalysen hvor det blir beskrevet som en form for kunnskap (Devereux 2007). Noe de påpeker bidrar til at diskursanalysen kan gå utover ordene og bildene som konstituerer selve teksten. Isteden for å søke etter svar kan diskursanalysen åpne for å stille spørsmål, analysere og tolke utover det som kanskje kan oppfattes som den foretrukne måten å forstå teksten(Devereux 2007). Det kan med bakgrunn i denne tilnærmingen være bedre å forstå diskursanalysen som en lang rekke med ulike tilnærminger isteden for en enkelt tilnærming (Taylor 2001 i Devereux 2007). Likheten mellom de ulike praksisene er fokuset på språket og tilnærmingen er som regel kvalitativ fremfor kvantitativ (Devereux 2007).

I forhold til reabilitet og validitet har forskere tradisjonelt sett prøvd å trekke frem sin upartiskhet og prøvd å holde seg utenfor diskursene. I følge Bell og Smith (2007 i Devereux 2007) er det likevel vanskelig å komme utenom en slik involvering når diskursanalyser går ut på å utforske og tolke tekster. For å unngå de største fellene det representerer er det viktig for forskeren å støtte opp om funnene sine gjennom teori og beviser fra andre studier. Det er likevel viktig for Bell og Smith (2007 i Devereux 2007) å påpeke at det er opp til publikum/leseren å være klar over sin mulighet til å akseptere, avvise eller forhandle med den akademiske diskursen på den måten de måtte ønske.

Diskursive ideologier

Den intellektuelle bakgrunnen for tilnærminger som involverer ideologi finner vi i strukturalismen. Foucault (1994 i Devereux 2007) påpeker i sin tilnærming at diskurser har en sosial makt som påvirker hva som blir ansett som virkelig og dermed mulig. Slike konstruksjoner avgjør hvordan verden blir sett og hva som kan gjøres i den. Diskurser er på denne måten essensielle for å forstå hvordan det sosiale subjektet er posisjonert og begrenset. Fairclough (2003 i Devereux 2007) mener de enkelte diskursene inluderer antagelser om hva som er, hva som er saken, hva som er mulig, hva som er nødvendig og hva som vil skje. Det argumenteres deretter for at det i noen tilfeller er slik at antagelsene og diskursene de er assosiert med er ideologiske. Fairclough (2003) i Devereux 2007) påpeker videre at dette kan fremstilles som uungåelige prosesser.

Ideologier kan i følge van Dijk (2009) anses å være enkle rammer for en sosial oppfatning som deles av medlemmer i en sosial gruppe. Denne oppfatningen konstitueres gjennom relevante utvelgelser av sosiokulturelle verdier og organiseres gjennom et ideologisk skjema som representerer hvordan en gitt gruppe definerer seg selv. I følge van Dijk (2009) vil det foruten om den sosiale funksjonen det innebærer for opprettholdelse av gruppens interesser, inneholde en kogniktiv funksjon gjennom organiseringen av den sosiale representasjonen av gruppen, noe som indirekte kan overvåke grupperelaterte sosiale praksiser og dermed også tekst og tale som kommer fra gruppemedlemmene (van Dijk 2009).

I motsetning til kunnskap kan ideologier definers som systemer for sosiale oppfatninger som er evaluerende og utgjør grunnlaget for avgjørelser rundt hva som er bra og dårlig, rett og galt, noe som igjen kan tilby de grunnlegende retningslinjene for sosial persepsjon og interaksjon. van Dijk (2009) tar derfor utgangspunkt i at de grunnleggende byggesteinene i ideologier er sosiokulturelle verdier som for eksempel likhet, rettferdighet, sannhet eller effektivitet. Slike verdier behøver ikke i følge van Dijk (2009) å være avgrenset til spesifikke grupper, men kan også ha en bredere kulturell relevans. De kan med andre ord være kulturelt spesifikke eller inneholde kulturell variasjon selv om noen verdier også kan være universielle (Hofstede 1980, Rokeach 1973, 1979 i van Dijk 2009). van Dijk (2009) antar at de sosiale gruppene gjør valgene sine basert på egeninteresse og etablerer et hiearki for deres relevans som en funksjon for dets sosiale posisjon og mål. For hver gruppe kan det derfor i følge van

Dijk (2009) antas at disse verdiene konstituerer de grunnleggende evalueringskriteriene for meningene som definerer det ideologiske systemet (van Dijk 2009).

I likhet med kogniktive systemer er ideologier sannsynligvis ikke uorganiserte forslag for evaluering, men basert på gruppeskjemaer som gruppemdlemmene bruker på seg selv. Et slikt skjema kan ta for seg spørsmål som kan brukes i analysen; Hvem tilhører gruppen og hvem gjør det ikke? Hva er gruppens typiske gjøremål? Hvilke målsetninger har den? Hvilke normer og verdier brukes for gruppens evalueringer? Hva slags posisjon har gruppen? Hvilke ressurser ønsker gruppen å beskytte?

En slik kategorisering må ikke forveksles med en beskrivelse av den sosiale virkeligheten, men heller anses som en konstruksjon av ideologisk egeninteresse i forhold til gruppens selvbilde i relasjon til andre grupper (Abrams og Hogg 1990 Turner og Giles 1981 i van Dijk 2009).

I en hver kontinuerlig periode vil det i følge Bell og Smith (2007 i Devereux 2007) finnes konkurrerende former for å beskrive hendelser og dens historie. Ideer kan linkes til interesser og disse konkurrerende interessene vil gjerne søke mot en forklaring av verden som legitimerer deres egen posisjon. Ideologi definert som et interesseperspektiv og dens kamp for å legitimitere seg selv vil dermed kunne gå hånd i hånd. Språket og definisjonene kan i utgangspunktet anses som en kamparena for de ulike gruppene. Her kan vi ikke bare se spesifikt på teksten, men vi må også undersøke de sosiale relasjonene som genererer de ulike beskrivelsene. Et viktig teoretisk poeng kan være det samme uten at det samsvarer med innholdet. De ulike partene i en konflikt kan for eksempel bruke ulike argumenter som tilpasser seg nye omstendigheter. For å forstå denne prosessen kan det være nødvendig å gå utover selve teksten (Devereux 2007). Vi kan i følge Bell og Smith (2007 i Devereux 2007) begynne vår tilnærming med antagelsen om at ulike forklaringer vil komme frem fra en konflikt gjennom for eksempel subgrupper eller konkurrerende institusjoner.

Diskursens materialitet

Neumann (2000) påpeker i sin artikkel om diskursens materialitet at hovedpoenget med en diskursanalyse er å studere mening og de sosiale institusjoner som bærer mening ved hjelp av en og samme metode. Det legges vekt på at begge disse fenomenene kan forstås som en helhet. Meningsdannelser anses å være en intergrert del av det sosiale og det påpekes derfor at samfunnsvitere i senere tid har valgt å fokusere på språket for å fange opp det sosiale aspektet.

Neumann (2000) mener hovedutfordringen i en diskursanalyse er å fange inn både det språklige og det materielle i et helhetsperspektiv gjennom å se på begge fenomenene. Han argumenterer for at det er viktig å finne handlingsbetingelsene for det som blir sagt og gjort, om utsagnet for eksempel aktiverer eller setter i spill en serie med sosiale praksiser, og til slutt hvordan utsagnet i sin tur kan bidra til å bekrefte eller avkrefte de ulike praksisene. Neumann (2000) trekker i sin tolkning av diskursens materialitet inn Foucaults forarbeid med *vitenskapsarkeologien* og hvordan vi kan tolke handlingsbetingelser ut fra begrepet om "arkivet". Arkivet er ikke dokumentene selv, men en forståelse for tilgjengeligheten av diskursen. Dette innebærer en forståelse av de grensene som kan ligge i for eksempel språklig kompetanse og hvilke medium diskursen er tilgjengelig gjennom (Neumann 2000). I forhold til en slik forståelse kan en avhengig av forskningsbehovet spesifisere tekstens materialitet i det uendelige i følge Neumann (2000). Når vi begynner å spørre om hvilke deler av arkivet som har hvilke sosiale bånd til hvilke grupper og institusjoner så påpeker Neumann (2000) at det kommer frem en materialitet utover selve teksten. For Neumann (2000) er det viktig å identifisere diskursens overgang fra språket og over til den materialiteten som ikke er språklig. Gjennom en slik distinksjon er det i følge Neumann (2000) mulig å stille spesifikke spørsmål om diskursens materalitet. Hvilke materielle handlingsbetingelser av språklig og ikke-språklig art stiller det relevante arkivet opp for et utsagn og hvilke formelle og uformelle institusjoner (forstått som regulære handlingsmønstre) setter det i spill? Analytiske grep som kan spesifisere diskursens materialitet vil i følge Neumann alltid ha en pris gjennom at noe må ofres fordi det tingliggjør et utgangspunkt for analysen. Det er for eksempel mulig å ta utgangspunkt i en tekst, en gjenstand eller en hendelse og spore dets ringvirkninger (Neumann 2000).

Den sosiale konstruksjonen av teknologi

Den sosiale konstruksjonen av teknologi (SCOT) er en av mange vitenskapelige konstruktivistiske tilnærminger til teknologi som oppsto på 80-tallet. Meningen bak konstruktivistbegrepet handler i følge Bijker om sannheten rundt vitenskapelige fakta og hvorden artifaktene kan studeres som en konstruksjon isteden for iboende egenskaper rundt disse faktaene og maskinene. Det er først og fremst en måte å studere teknisk forandring i samfunnet, både historisk og i samtidsstudier. Samtidig er det en teori rundt utviklingen av teknologi og dets forhold til samfunnet (Bijker 2009). Konstruktivistiske studier av vitenskap og teknologi fyller et vidt spekter fra milde til radikale tilnærminger (Sismondo 1993 i Bijker

2009). De milde versjonene ønsker å inkludere den sosiale konteksten når utviklingen av teknologi skal beskrives mens de mer radikale versjonene argumenterer for at innholdet i vitenskap og teknologi er sosialt konstruert. Vitenskapelige uttalelser og de tekniske egenskapene til maskiner kan med andre ord ikke forklares gjennom naturen, men må isteden anses som konstituert av en sosial prosess (Bijker 2009). Utgangspunktet for SCOT var som en kritikk av teknologisk determinisme hvor teknologi ble ansett å utvikle seg under autonome forhold og på en teknologisk måte påvirket den sosiale utviklingen (Bijker 2009).

SCOT er i følge Bijker (2009) en heuristisk tilnærming til studien av teknologi i et samfunn og den sosiale konstruksjonen kan fremlegges i tre etterfølgende forskningssteg. Viktige konsepter i det første steget er "relevante sosiale grupper" og "tolkningsmessig fleksibilitet". I det andre steget følger forskeren opp med hvordan den "tolkningsmessige fleksibiliteten" minsker fordi noen artifakter skaffer seg dominans over andre og meningene konvergeres. Til slutt vil en artifakt resultere fra den sosiale konstruksjonen. Viktige konsepterer i det andre steget er "avslutning" og "stabilisering" som begge beskriver resultatet av prosessen rundt sosial konstruksjon. I det tredje steget analyseres og tolkes stabiliseringen ut i fra et bredere konsept om hvorfor den sosiale konstruksjonen resulterer i noe fremfor noe annet. Det sentrale konseptet i det tredje steget er en "teknologisk ramme" som kan brukes på alle de relevante sosiale gruppene. Denne tre-stegs prosessen handler kort sagt om: (1) Sosiologisk dekonstruksjon av en artifakt for å demonstrere dets tolkningsmessige fleksibilitet; (2) beskrivelse av artifaktens sosiale konstruksjon; og (3) forklaringen rundt denne konstruksjonsprosessen i de teknologiske rammene for de relevante sosiale gruppene (Bijker 2009).

Den deskriptive modellen

For å fange inn de relevante sosiale gruppene rundt datalagringsdirektivet har jeg tatt utgangspunkt i høringsuttalelsene gjennom å spore hva de ulike gruppene gav uttrykk for. Bijker (1997) mener at slike sosiale grupper er relevante for å forstå hvordan teknologi utvikles. I følge Bijker (1997) er de relevante sosiale gruppene like viktig for utviklingen av artifakter som den tekniske historien. Når de er identifisert og beskrevet er det i følge Bijker (1997) viktig å finne avgrensningene mellom de relevante sosiale gruppene og etterhvert klargjøre disse avgrensningene mer presist. Grensene kan i utgangspunktet virke åpenbare, men samtidig kan det være distinksjoner mellom dem som kan skape nye grupper. Aktører

kan på denne måten simplifisere og omorganisere deres verden gjennom å fjerne tidligere grenser eller ved å omjustere seg til nye grenser (Bijker 1997).

Bijker (1997) legger vekt på at relevante sosiale grupper kan kategoriseres som aktører og at det er en viktig kategori å analysere. Den teknologiske utviklingen bør i følge Bijker (1997) bli sett på som en sosial prosess og ikke bare en autonom begivenhet. De relevante sosiale gruppene blir derfor beskrevet som en prosessdrivende faktor. Bijker (1997) mener også at en relevant sosial gruppe må være tilstedeværende i prosessen for å være relevant for analysen. Det påpekes at denne tilnærmingen har to potensielle problemer i forhold de politiske og epistemologiske aspektene. Gjennom det politiske aspektet må vi i følge Bijker (1997) annerkjenne avmakten til sosiale grupper som ikke har evnen eller muligheten til å uttale seg på egne vegner. Disse vil gjerne mangle gjennom en slik analyse. Det epistomologiske aspektet handler om den påståtte identiteten mellom aktører og hvordan de kategoriseres. Den som analyserer må derfor ta innover seg at andre forskere vil kunne ta andre avgjørelser og kan velge å inkludere andre sosiale grupper (Bijker 1997). Det er ifølge Bijker (1997) ingen mekanisk måte å avgjøre hvilke av tilnærmingene som er best. En analyse av aktører vil derfor som regel dra på forskerens egne tolkninger.

Utvikling forstått som en sosial prosess

Hvis vi ønsker å forstå utviklingen av teknologi som en sosial prosess må vi i følge Bijker (1997) forstå artifaktene slik de blir ansett av de relevante sosiale gruppene. For å unngå at teknologien tar på seg en anonym tilværelse kan vi derfor forsøke å identifisere de ulike meningene de relevante sosiale gruppene gir til artifaktet vi analyserer og hvordan det produserer ulike artifakter. Dette kan gjøres gjennom å fokusere på hvilke problemer og løsninger som de relevante sosiale gruppene gir uttrykk for (Bijker 1997). Bijker (1997) mener fokus på de ulike relevante sosiale gruppene kan bidra effektivt til å gardere seg mot implisitte antagelser rundt en linær forståelse av utviklingen.

Hvorfor unngå en evolusjonistisk deskriptiv modell?

Deler av den deskriptive modellen kan forstås som en evolusjonistisk prosess. En slik presentasjon vil i følge Bijker (1997) måtte fokusere på tre lag i prosessen gjennom variasjonen og utvelgelsen av (1) problemer, (2) løsninger og (3) de nye artifaktene. Det er

imidlertid to relaterte problemer til en slik tilnærming i følge Bijker. Praktisk sett vil en slik beskrivelse være ekstremt kompleks og selv om den skulle være omfattende påpeker Bijker (1997) problemet med at artifaktet nesten uungåelig vil ende opp å bli forstått som en konstant og forhåndsbestemt entitet generert av variasjoner i prosessen og deretter dyttet gjennom en utvelgningsprosess. Bijker (1997) legger vekt på at et hvert problem og enhver løsning sånn som de blir oppfattet av de relevante sosiale gruppene vil kunne endre artifaktets mening uavhengig om løsningen blir implementert eller ikke (Bijker 1997).

Den fleksible tolkningen

"*To analyze true and false claims symmetrically, they must apply the same conceptual apparatus to each*" (Bijker 1997:270)

Etter å ha beskrevet de ulike artifaktene gjennom de relevante sosiale aktørene kan vi i følge Bijker (1997) diskutere mer eksplisitt konsekvensene av de ulike oppfatningene rundt artifaktet. Hva som fungerer og hva som ikke fungerer med et artifakt må i følge Bijker (1997) behandles som sosialt konstruerte oppfatninger og ikke som iboende egenskaper hos selve artifaktet. Bijker (1997) mener det åpner for en symmetrisk analyse av teknologi. I forhold til en slik tilnærming er det viktig at forskeren ikke gjør vurderinger rundt hva som er sant eller usant, men heller beskriver sannheter og falsifiseringer symmetrisk gjennom like konseptuelle rammer (Bijker 1997).

De ulike tolkningene av artifaktet kan basere seg på skjulte oppfatninger rundt artifaktet. Bijker (1997) trekker frem i sin analyse av den teknologiske utviklingen til sykkelen at de ulike oppfatningen rundt sykkelen, hvor noen anså den som utrygg og andre igjen oppfattet den som macho ikke kunne konkluderes som en sann oppfatning og en usann oppfatning. Begge perspektivene bidro på hver sine måte til utviklingen av sykkelen i følge Bijker (1997).

Dersom vi kan demonstrere at det finnes fleksibelilitet rundt tolkningen av en artifakt har vi i følge Bijker (1997) de riktige rammene for en sosial analyse. Når vi på denne måten har dekonstruert artfifaktet inn i flere artifakter kan vi lettere forklare hvordan en av artifaktene etterhvert blir dominerende. De relevante sosiale gruppene ser i følge Bijker (1997) ikke bare ulike aspekter med et artifakt, men konstituerer artifaktet gjennom sine tolkninger. Bijker (1997) mener det er like mange artifakter som det er relevante sosiale grupper du kan knytte til det.

Konsepter rundt avslutning og stabilisering

På bakgrunn av den sosiologiske dekonstruksjonen av artifakter gjennom den fleksible tolkningen kan vi i følge Bijker spore den sosiale konstruksjonen. Den sosiale konstruksjonen er i følge Bijker (1997) resultatet av to kombinerte prosesser. Gjennom avslutning og stabilisering av en artifakt. Bijker (1997) mener denne prosessen må forstås som en sammenhengende prosess. Konseptet rundt avslutning kan i følge Bijker (1997) relateres til forståelsen av den fleksible tolkningen mens konseptet rundt stabilisering handler om en allmen aksept av en dominerende artifakt. Hvordan noe avsluttes befinner seg på et interaksjonistisk nivå mens stabilisering handler om semantistisk endring. Stabilisering kan observeres gjennom at ulike tolkninger faller bort og en tolkning aksepteres av alle. Avslutningsmekanismer kan innebære en retorisk avslutningsmekanisme der et essensielt eksperiment eller et viktig argument avslutter en kontrovers uten å være fullstendig overbevisende for kjernen av forskere, men likevel er lettere å akseptere eller har større appell for et publikum som ikke selv er eksperter. Avslutning betyr med andre ord at mulighetene for en fleksibel tolkning innskrenkes og mangfoldet av artifakter synker. Prinsipielt sett mener Bijker (1997) at graden av stabilisering vil variere i de ulike sosiale gruppene. Når prosessen rundt avslutning er i gang vil det i følge Bijker (1997) være veldig vanskelig å reversere prosessen, men ikke fullstendig. Det understrekes likevel at denne prosessen er kontinuerlig selv om den ikke er like aktiv hele tiden. Fokuset på relevante sosiale grupper og konseptet rundt tolkningsmessig fleksibilitet sikrer at modellen møter kravet om symmetri mens konsepter rundt avslutning og stabilisering sørger for at vi møter kravene om forståelse av forandring og kontinuitet (Bijker 1997).

Analysen og empiriske funn

I høringsuttalelsene rundt datalagringsdirektivet identifiserer jeg tre hoveddiskurser gjennom *overvåkningsdiskursen, etterforskningsdiskursen* og *økonomidiskursen*. I forhold til de to første som ble nevnt er *nytteverdidiskursene, personvernsdiskursen* og *sikkerhetsdiskursen* satt opp slik at de går frem og tilbake mellom beskrivelser av datalagringsdirektivet fra aktører innenfor overvåkningsdiskursen og etterforskningsdiskursen. Nytteverdidiskursen inneholder flere perspektiver enn personvernsdiskursen og sikkerhetsdiskursen som begge omhandler ulike tilnærminger til personvernet og sikkerheten rundt det. *Økonomidiskursen* fokuserer hovedsakelig på økonomiske betenkelighetene rundt direktivet, men *samfunnsansvarsdiskursen*, *opphavsrettdiskursen* og *kundetillitsdiskursen* samsvarer delvis med henholdvis etterforskningsdiskursen og overvåkningsdiskursen. Underveis trekker jeg frem aktørene ulike bekymringer, meninger og beskrivelser rundt datalagringsdirektivet.

Overvåkningsdiskursen

Overvåkningsdiskursen er en beskrivelse av datalagringsdirektivet som gjerne fremheves av motstandere av direktivet. Aktørene som befinner seg innenfor denne diskursen deler et syn om at datalagring er en form for overvåkning. Overvåkningsdiskursen kan anses som den overordnede diskursen for motstandere av datalagring fordi beskrivelsene som kommer frem under kildevernsdiskursen, persovernsdiskursen (herunder også omgåelsesdiskursen og utglidningsdiskursen) gjerne tar utgangspunkt i at datalagring er overvåkning. Under økonomiske diskurser finner vi også en kundetillitsdiskurs hvor ekomtilbydere frykter at kundene skal føle seg overvåket og miste tilliten til tilbyderen.

Aktører innenfor overvåkningsdiskursen legger i stor grad vekt på ulike potensialer rundt datalagringsdirektivet. Det rettes først og fremst kritikk mot den vide tilnærmingen direktivet har til datainnsamling. *Nei til EU* mener datalagringsdirektivet åpner for å gjøre alle som registreres til gjenstand for etterforskning og *nei til EU* oppfatter det som svært inngripende i forhold til personvernet fordi det kan kartlegge sensitiv informasjon om enkeltindividers sosiale nettverk. (Heming & Hobøl 2010). *Advokatforeningen* beskriver direktivet som en formålsløs lagring av telekommunikasjonsdata som egner seg til å gi en truende følelse av å være overvåket. Lagring av data i det omfanget som direktivet pålegger innebærer i følge

Advokatforeningen en systematisk og vedvarende 'screening' av befolkningens daglige bruk av kommunikasjonsmidler. Noe som oppfattes som en prinsipiell ny måte å bekjempe kriminalitet. Datalagringsdirektivet vil i følge *advokatforeningen* være et betydelig inngrep i befolkningens private forhold og *advokatforeningen* frykter fremtidig misbruk dersom direktivet først etableres (Reiss-Andersen & Smith 2010).

Advokatforeningen mener datalagringsdirektivet ikke kan sammenlignes med dagens system fordi det i følge *advokatforeningen* åpner for utstrakt bruk av den innsamlede informasjonen gjennom de gitte vilkårene med en strafferamme på 3 år eller dersom det kan antas å ha betydning som bevis (Reiss-Andersen & Smith 2010). Høringsnotatet legger imidlertid vekt på en strafferamme på 3 år eller mer og åpner i utgangspunktet bare opp for at visse forbrytelser som er vanskelig å oppklare uten trafikkdata med lavere strafferamme kan få unntak og vurderes som "særlige saker". Kritikken kan imidlertid kobles til politiets tilgang gjennom straffeprosessloven § 214 som gjelder pålegg om sikring av elektronisk lagrede data. Sikringspålegget gir imidlertid ikke en automatisk rett for påtalemyndigheten til å få de sikrede dataene utlevert. Påtalemyndigheten har imidlertid etter en begjæring om tilgang, rett til opplysninger som kan avdekke hvor de aktuelle dataene kom fra og hvor de eventuelt ble sendt jf. § 215. En slik begjæring vil imidlertid begrense seg til et kortere tidsrom på 90 dager (NOU[1] 2010).

Datatilsynet mener datalagring kan brukes som kommunikasjonskontroll og oppfatter det som uheldig at direktivet i høringsnotatet fremstilles som mindre inngripende enn telefonavlytting. *Datatilsynet* argumenterer samtidig for at kommunikasjonskontroll i motsetning til datalagringsdirektivet var en målrettet metode som bare kunne tas i bruk mot en begrenset krets med personer der det forelå en kvalifisert mistanke om særlige grove lovbrudd. Datalagringdirektivet oppfattes på den andre siden som et tiltak som iverksettes uten konkret mistanke mot noen og det trekkes frem at direktivet retter seg mot hele befolkningen (Apenes 2010). I følge høringsnotatet vil imidlertid ikke datalagringsdirektivet være åpent for innsyn uten en rettslig begjæring av opplysningene (NOU[1] 2010). Det virker imidlertid ikke som datatilsynet skiller mellom når politiet har direkte og indirekte tilgang til dataene. Denne tilnærmingen kan kobles til Hannemyrs (2002) begrep om et virtuelt panoptikon fordi den baserer seg på et usikkerhetsmoment rundt når noen blir eller ikke blir etterforsket. Det virtuelle panoptikon handler i første rekke om den disiplinerende funksjonen indirekte overvåkning kan ha på befolkningen. Hvor individer kan ende opp med å ta utgangspunkt i at

de blir overvåket uten å egentlig være det og dermed disiplinerer sin egen aktivitet basert på en potensiell overvåkning.

Datatilsynet mener grunnholdningen bak direktivet kan karakteriseres som en diffus lengsel etter en tilstand der individet er underornet statens behov for kunnskap om og kontroll med individene. *Datatilsynet* mener den bygger på en ubegrunnet forestlling om at alle politiske, sosiale og kulturelle problemer kan løses gjennom innhenting, lagring, bearbeiding og analyse av personopplysninger. Dagens teknologi setter i følge *datatilsynet* ikke lengre grenser for en slik holdning og de mener det derfor blir viktigere at staten selv begrenser seg på bakgrunn av gjeldende menneskerettsprinsipper. *Datatilsynet* legger vekt på at det ikke er snakk om registrering av enkelte øyeblikk i våre liv og mener derfor at det heller er snakk om en kontinuerlig overvåkning (Apenes 2010). *Elektronisk forpost Norge* mener argumentene som blir fremstilt i høringsnotatet med tanke på dagens situasjon fungerer like godt for å argumentere for at lovverket ikke trenger ytterligere styrking. *Elektronisk forpost Norge* mener direktivet legger opp til å lete etter et nåløye i en høystakk. *Elektronisk forpost Norge* foretrekker større fokus på målrettet etterforskning fremor innføring av datalagringsdirektivet (Østmoen & Gramstad 2010).

Det digitale samfunn tilrettelagt for overvåkning

Elektronisk Forbund Norge betrakter de teknologiske mulighetene som eksisterer i dag som nærmest tilrettelagt for kartlegging av samtlige bevegelser mennesker gjør i løpet av en dag. Faren for stadig eskalerende kontroll anses derfor som større enn problemet med for lite kontroll (Østmoen & Gramstad 2010). Opplysningene direktivet ønsker å lagre vil i følge *advokatforeningen* kunne gi betydelig innsikt i den enkeltes bevegelser, nettverk og interesser (Reiss-Andersen & Smith 2010). Denne tolkningen utdypes av *Norweigan Unix User Group* som legger vekt på hvordan dagens raske utvikling av elektronisk kommunikasjon gjennom for eksempel smarttelefoner med GPS vil føre til en kontinuerlig overvåkning over hvor individer befinner seg når disse dataene etterhvert kan knyttes til datalagringsdirektivet (NUUG 2010). For å realisere et slikt potensial kan det være viktig å påpeke at direktivet må åpnes opp for videre bruk enn høringsnotatet foreslår, men dersom vi forholder oss til usikkerheten rundt hvem som eventuelt kan havne under etterforskning kan kritikken kobles til begrepet om et virtuelt panoptikon.

Yrkes og sentralforbundet mener datalagringsdirektivet kommer i tillegg til en rekke andre overvåkningsmuligheter som allerede er på plass (Kvalheim & Kastet 2010).. *EL & IT Forbundet* trekker i sin høringsuttalelse frem hvordan dagens digitaliserte samfunn allerede lagrer for store mengder med personlige opplysninger. *El & IT forbundet* mener direktivet vil bidra til ytterligere press på utviklingen av nye lagringssystemer (Gundersen 2010). *Elektronisk Forpost Norge* nevner blant annet kunde, konto- og transaksjonsopplysninger som skatteetaten, NAV og politiet allerede har tilgang til via hjemler for innsyn (Østmoen & Gramstad 2010). *Den internasjonale juristkommisjon* påpeker i sin høringsuttalelse at datalagringsdirektivet utvikles samtidig som mer generelle og avanserte overvåkningsystemer. *Den internasjonale juristkommisjon* mener hensikten med disse systemene i lengden er å skape sosial kontroll (Lund & Wessel-Aas 2010). Systemene som spesifikt nevnes er EU-prosjektene INDECT (Intelligent information system supporting observation) og ADABTS (Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces). *Den internasjonale Juristkommisjon* trekker også frem Schengen-, Prüm- og Europol-samarbeidet og påpeker at disse avtalene bidrar til at de ulike systemene og registrene vil kobles sammen og utveksles mellom politi og hemmelige tjenester over landegrensene (Lund & Wessel-Aas 2010). *Yrkes og sentralforbundet* mener derfor at datalagringsdirektivet er enda et steg mot et samfunn der alt vi gjør blir registrert (Kvalheim & Kastet 2010). LO i Trondheim mener det finnes stor tillit til myndighetene i Norge og i de fleste EU-land og dermed liten frykt for misbruk, men påpeker at det også i demokratiske land har vært en lang historie med overvåkning. De legger vekt på at fagforeningsaktivister oppfattes som opprørsk i mange land og at direktivet kan bidra til å overvåke slike nettverk (Byrkjeflot 2010).

Data på avveier

Risikoen for at dataene kommer på avveie vil i følge *nei til EU* alltid være tilstede. Det trekkes frem to eksempler. TELE2-saken der kredittopplysninger til et seksifret antall personer fant sin vei til uvedkommende. Det andre eksempelet referer til en større skandale som skjedde i Storbritannia i 2007 hvor to ukrypterte disker med personopplysninger vedrørende alle familier i Storbritannia med barn under 16 år kom på avveie. *Nei til EU* legger til i sin høringsuttalelse at ved en eventuell implementering må sikring av dataene ha høy prioritet og noe av denne sikkerheten må i følge *nei til EU* baseres på begrenset tilgang. Her støttes forslaget i høringsnotatet om kravet til en rettslig kjennelse (Heming & Hobøl 2010).

Elektronisk forpost Norge går lengre i sin kritikk av muligheten for at de lagrede data havner på avveie og mener det vil kunne skape uttrygghet. Det legges vekt på at opplysningene også vil være verdifulle hos de direktivet er ment å forsvare oss mot (Østmoen & Gramstad 2010). I følge *elektronisk forpost Norge* legger datalagringsdirektivet opp til privatisering av politioppgaver fordi bevisinnsamlingen ikke blir gjort direkte av politiet. En slik løsning anses derfor å øke risikoen for tukling med dataene. *Elektronisk forpost Norge* mener det også er en fare for at dataene kan falle i gale hender eller misbrukes av myndighetene og private selskaper (Østmoen & Gramstad 2010).

En sentral verdi for aktørene under overvåkningsdiskursen er tillit til de som ikke er under konkret mistanke for noe kriminelt. Aktørene innenfor overvåkningsdiskursen mener datalagringsdirektivet representerer et brudd på tillitsforholdet mellom befolkningen og myndighetene til fordel for kontroll. Aktørene innenfor overvåkningsdiskursen vurderer samtidig ikke datalagringsdirektivet kun ut i fra hva det måtte innebære alene, men mener det supplerer et større nettverk av eksisterende og potensielle overvåkningssystemer. Kritikken baserer seg heller ikke bare på direktivet i sin nåværende form og det spekuleres i stor grad rundt hvordan direktivet vil utvikle seg over tid. Aktørene innenfor overvåkningsdiskursen har heller ikke tro på de mekanismene som skal forhindre misbruk og utglidning av formålet over tid.

Kildeverndiskursen

Nei til EU mener direktivet utfordrer kildevernet. I følge *nei til EU* vil denne retten uthules fullstendig ved en eventuell implementering av datalagringsdirektivet. De mener derfor at kildevernet må styrkes mot beslag og utlevering av trafikkdata mellom journalister og avisredaksjoner (Heming & Hobøl 2010).

Norsk Journalistlag mener massemediens kjennskap til og bruk av anonyme kilder kan få etterspill når kildevernet blir satt på prøve i domstolsapparatet. *Norsk journalistlag* påpeker at kildens informasjon kan være av interesse for oppklaring i et mulig straffbart forhold eller for saksforholdet i en sivil sak, og retten vil derfor kunne ønske å vite kildens identitet. Det refereres til EMK artikkel 10 som verner ytringsfriheten og nødvendighetskravet i artikkelens annet ledd innebærer at formålet med det aktuelle inngrepet i ytringsfriheten må være nødvendig i et demokratisk samfunn for å være lovlig. *Norsk journalist* påpeker at det i dag

må foretas en konkret avveining av de ulike interessene i den enkelte sak. *Norsk jouranlistlag* mener derfor at en bevisplikt må tolkes innskrenkende for å være i tråd med EMK artikkel 10, jf. Rt 2004 s.1400 (avsnitt 46).

Norsk journalistlag mener det ved anledninger det finnes grunnlag for alvorlig tvil i forhold til en inngripen skal tvilen falle til fordel for at bevisplikt ikke pålegges. Konsekvensene med en eventuell implementering av datalagringsdirektivet vil i følge *norsk journalistlag* være at myndighetene kan fange opp kommunikasjon mellom journalister og deres anonyme kilder. *Norsk journalistlag* mener det vanskeliggjør muligheten for å kommunisere sporfritt og at det på den måten truer den frie journalistikken. *Norsk journalistlag* krever at direktivet ikke brukes direkte mot journalisters virksomhet og ikke kan brukes til å avdekke kildens identitet, fange opp kommunikasjon mellom journalist og kilde som en utilsiktet konsekvens eller bruke materiale som er fremkommet som bevis (Floberghagen & Lindahl 2010).

Norsk redaktørforening mener direktivet gir grunnlag for berettiget frykt for konsekvensene dersom kildevernet ikke tas på alvor. *Norsk redaktørforening* utdyper at en av grunntankene i selve ytringsfriheten er ideen om borgernes adgang til den anonyme ytring. *Norsk redaktørforening* anser kildevernet for å være anonymitetsretten som skal beskytte kildene som kan bidra med viktig informasjon som ellers ikke ville kommet frem. *Norsk redaktørforening* mener denne tilnærmingen bidrar til å beskytte demokratiet. *Norsk redaktørforening* frykter at direktivet kan bidra til å fjerne tillitsforholdet mellom journalister og kilder. *Norsk redaktørforening* påpeker at den indre justisen hos journalister (Vær Varsom-plakaten) tilsier at en hver journalist med respekt for seg selv ikke oppgir sine kilder selv i situasjoner hvor det er mulig. Kilder skal i følge *norsk redaktørforening* ikke være nødt til å gjøre kompliserte juridiske vurderinger på egenhånd, men kunne hvile på den tilliten de har til journalister (Jensen 2010).

Norsk rikskringkasting mener direktivet åpner for at statlig eller private arbeidsgivere går til sivilt søksmål mot en ansatt som mistenkes for å ha lekket taushetsbelagt informasjon til pressen. *Norsk rikskrinkasting* påpeker at de synes kildevernet allerede er under stekrt press og referer til en rapport kallt 'Silencing Sources' som ble utgitt i 2007 av Privacy International hvor det ble rapportert at kildevernet allerede i dag blir utfordret og krenket i økende grad i Europa og verden forøvrig (Wessel-Aas 2010).

Den internasjonale juristkommisjon trekker i sin høringsuttalelse frem et eksempel på det de oppfattet som en krenkelse av kildevernet når den daværende forsvarsminister Anne-Grete

Strøm-Erichsen ba PST om å etterforske VGs anonyme kilder etter avsløring av de reelle kostnadene forbundet med flytting av Fellesoperativt hovedkvarter fra Stavanger til Bodø (Lund & Wessel-Aas 2010). VG hadde en egen artikkel som het "Hysjen beordret på kildejakt etter VG-avsløring" hvor forsvarsministeren uttalte at hennes vurdering var å anmelde et hvert forhold der graderte dokumenter hadde blitt lekket (Johansen, Johnsen & Hopperstad 2008) . Muligheten til å kunne avsløre kilder kan i følge *den internasjonale juristkommisjon* føre med seg en 'chilling effect' rundt potensielle kildeners motivasjon til å bidra med informasjon. Gjennom å hacke systemet for å avsløre kilder mener Den internasjonale juristkommisjon tror også hacking av systemet kan brukes til å avsløre identiteten til varslere og mener også det kan skremme vekk potensielle (Lund & Wessel-Aas 2010).

Aktørene innenfor kildevernsdiskursen mener datalagringsdirektivet er en trussel mot kildevernet. Diskursen kan på mange måter kobles til overvåkningsdiskursen fordi aktørene mener potensialet for at myndighetene og private aktører vil avsløre identiteten til informanter er stor ved en innføring av direktivet. Kjerneverdien blant aktørene er ytringsfrihet og diskursen kan derfor også kobles til frimodighetsdiskursen som blir trekt frem senere under personvernsdiskursen.

Etterforskningsdiskursen

Etterforskningsdiskursen er en beskrivelse av datalagringsdirektivet som gjerne fremheves av tilhengere av direktivet. Aktørene som befinner seg innenfor denne diskursen er kritisk til forståelsen av datalagring som overvåkning og fremhever politiets behov for effektive virkemidler i bekjempelse av moderne kriminalitet. Et av de tydeligste skillene mellom overvåkningsdiskursen og etterforskningsdiskursen er hvordan hensynet til allmenheten sidestilles med hensynet til ofrene. Etterforskningsdiskursen kan anses som den overordnede diskursen for tilhengere av datalagring fordi beskrivelsene som kommer frem under sikkerhetsdiskursen, utsatt sletteplikts-diskursen, behovsdiskursen og risikodiskursen tar utgangspunkt i at datalagring er viktig for etterforskning av alvorlig kriminalitet. Under økonomiske diskurser finner vi også en opphavsrettdiskurs hvor tilbydere av media trekker frem de økonomiske tapene muligheten for anonymitet på internett skaper.

Enkelte kriminalitetstyper har i følge *økokrim* særtrekk som gjør trafikkdata særlig relevante og betydningsfulle. *Økokrim* mener det i første rekke gjelder kriminalitet som begås av flere personer i felleskap der kommunikasjon mellom aktørene står sentralt. Kommunikasjonen kan i følge *økokrim* i noen tilfeller være det eneste elementet som knytter vedkommende til det straffbare forholdet og her trekkes bakmenn spesielt frem. *Økokrim* trekker også frem at kommunikasjon kan være den eneste komponenten som skiller en straffbar handling fra en lovlig handling. Her nevnes blant annet ulike former for verdipapirkriminalitet deriblant ulovlig innsidehandel og misbruk av innsideinformasjon. Videre nevnes tradisjonelle former for krimanilitet som identitetstyveri. Itillegg har internett i følge *økokrim* åpnet for nye former for kriminalitet. En rekke sentrale samfunnsstrukturer er flyttet over på nett og *økokrim* trekker spesielt frem banker. Disse vil i følge *økokrim* bli svært sårbare for kriminelle handlinger dersom ikke data om bruken kan registreres. For å ha mulighet til å følge utviklingen på dette omårdet mener *økokrim* politiet må ha mulighet til teknologisk etterforsking og tilgang til opplysninger om internettbruk (Schea 2010).

Norsk narkotikapolitforening mener de viktigste elementene i narkotikabekjempelsen er forebygging av narkotikamisbruk blant ungdom og reduksjon av tilgjengelighet av narkotika i samfunnet. For å redusere tilgjengeligheten mener de det er behov for å ha nødvendige etterforskningsmetoder til rådighet slik at personer som innfører og distribueer narkotika blir pågrepet og stilt til ansvar for dette. I denne sammenheng mener de datalagringsdirektivet vil være sentralt. Det handler i følge *norsk narkotikapolitiforening* blant annet om muligheten til å kunne rekonstruere et hendelsesforløp og kartlegging av de involverte. I denne sammenheng anses trafikkdata ofte som de eneste objektive bevisene politiet har fordi de mistenkte i liten grad samarbeider med politiet eller fordi det ikke finnes vitner (Gultvedt 2010).

Utsatt sletteplikt diskursen

Politiets fellesforbund mener ideen om at datalagringsdirektivet vil føre til et ”overvåkningssamfunn” der hele befolkningen kriminaliseres er en misvisende tolkning av direktivet. *Politiets fellesforbund* påpeker at det handler om å utsette sletting av data som allerede lagres og benyttes av politet ved behov (Johannessen & Gustafson 2010).

Politijuristene påpeker i sin høringsuttalelse at de mener begrepet datalagring er en misvisende beskrivelse av de oppfatter som en tidsbegrenset utsatt sletting av spesifiserte typer data fra telefoni og internettbruk, slik at opplysningene kan bli tilgjengelige som bevis i straffesaker. De mener det ikke er snakk om nye data som ikke allerede eksisterer i systemene hos teletilbyderne. De mener dette skiller fra overvåkning fordi overvåkning forutsetter aktiv innhenting av informasjon som ikke allerede eksisterte i systemene. Opplysningene som skal lagres er i følge *politijuristene* kun tilgjengelige ut fra lovregulerte retningslinjer og inneholder regler om sletting og datasikkerhet, herunder dokumentasjon og statistikk rundt informasjonen som hentes ut (Frantsvold 2010). I motsetning til overvåkningsdiskursen er tilnærmingen her smal og konkret. Det legges vekt på hvordan direktivet har et spesifikt virkningsområdet og hvordan det tar i bruk eksisterende data i motsetning til å produsere nye gjennom aktiv overvåkning.

Politidirektoratet mener frykten for et 'overvåkningssamfunn' og behovet for et sterkt personvern er svært overdrevet. Ubehaget borgerne kan føle ved å vite at noen sitter med denne informasjonen må i følge *politidirektoratet* anses som en mer 'teoretisk trussel' enn de reelle konsekvensene av alvorlig kriminalitet. *Politidirektoratet* mener samtidig at innføringen av lagringsplikt for trafikkdata ikke er uforholdsmessig med tanke på de rettsgoder som lagringen medfører for samfunnet gjennom den enkeltes beskyttelse mot overgrep fra kriminelle (Gjengedal 2010).

Aktørene innenfor utsatt sletteplikt-diskursen er først og fremst kritisk til koblingen mellom datalagringsdirektivet og overvåkning. Datalagringsdirektivet beskrives isteden som en utsettelse av sletteplikten ekomtilbydere forholder seg til i dag. Overvåkning assosieres gjerne med et inngrep i den private sfæren, men aktørene innenfor utsatt sletteplikt-diskursen mener datalagringsdirektivet isteden kan bidra til å beskytte den private sfæren mot kriminelle.

Nytteverdidiskursene

Nytteverdidiskursene er ikke en enhetlig kategori i denne oppgaven. Det er en samling av diskurser og hvordan de tilnærmer seg nytteverdien til direktivet på ulike måter. Behovsdiskursen og risikodiskursen henger i stor grad sammen med etterforskningsdiskursen. Behovsdiskursen fokuserer på utfordringene politi- og påtalemyndighetene har i forhold til

etterforskning av alvorlig kriminalitet og hvorfor datalagringsdirektivet anses som nødvendig i den sammenheng. Risikodiskursen fokuserer mer på den risikoen vi utsetter oss for dersom direktivet ikke blir implementert. Omgåelsesdiskursen henger på en lignende måte sammen med overvåkningsdiskursen. Omgåelsesdiskursen fremhever hvordan kriminelle kan unngå å bli fanget opp av datalagringen og hvordan det forminsker nytteverdien til direktivet. Det er også gjort rom for dokumentasjonsdiskursem hvor aktørene ikke nødvendigvis er for eller mot datalagringsdirektivet, men formidler et ønske om å avvente en avgjørelse rundt implementering til erfaringer fra land som har innført direktivet blir bedre dokumentert.

Behovsdiskursen

Økokrim legger vekt på at personvernsdebatten er viktig. Retten til en personlig sfære og kontroll over opplysninger som angår en selv er i følge *økokrim* helt sentralt i en rettsstat, men personvernshensynet må i følge *økokrim* ikke være et altoverskyggende utgangspunkt og på den måten fullstendig avgjørende i vurderingen om hvorvidt det skal innføres en lagringsplikt for trafikkdata. *Økokrim* utdyper at det handler om en avveining mellom to likestillte hensyn. Retten til personvern og retten til å ikke bli utsatt for krenkelser av sin fysiske og psykiske integritet. *Økokrims* mener det sistnevnte gjerne får mindre oppmerksomhet i samfunnsdebatten (Schea 2010).

Kripos synes høringsnotatet manglet en tilstrekkelig kartleggingen av politi- og påtalemyndighets behov for trafikkdata og synes det er en åpenbar svakhet i høringen (Ingerø 2010). Det er i følge Kripos behov for både elektroniske og fysiske bevis for å oppklare straffesaker. Hvis ikke begge bevistypene er tilgjengelig mener Kripos det skaper et ufullstendige bevisbilde. De mener behovet kommer spesielt frem i etterforskning av internettreleaterte seksuelle overgrep og spredning av overgrepsmateriale mot barn hvor de legger vekt på at internett er et sentralt kommunikasjonsmedium (Ingerø 2010).

Det nasjonale statsadvokatembetet ønsker å slå fast at datalagringsdirektivet er avgjørende for å kunne motvirke organisert kriminalitet og terror på en effektiv måte. *Det nasjonale statsadvokatembetet* mener det ikke er muligheter for en effektiv bekjempelse av terror og organisert kriminalitet med moderate virkemidler og samtidig være mot gjennomføringen av datalagringsdirektivet. Å være for bekjempelse av organisert kriminalitet og samtidig mot implementering av datalagringsdirektivet blir omtalt som en selvmotsigelse. *Det nasjonale*

statsadvokatembetet mener det vil representere en reell nedprioritering av kampen mot organisert og alvorlig kriminalitet**.** *Det nasjonale statsadvokatembetet* er av den oppfatning at det ikke bare er politiets oppgave å bekjempe denne typen kriminalitet, men noe alle borgere, institusjoner og organer må bidra med i en rettsat. Politiets behov oppfattes derfor som større enn borgernes behov for persovern fordi borgernes rett til vern mot alvorlig kriminalitet og beskyttelse av sentrale samfunnsfunksjoner veie tyngre (Frigaard & Glent 2010).

Trafikkdata er i følge *kripos* av den typen bevis som normalt vil veie tungt i bevisvuderingen fordi de oppfattes som objektive og konstaterbare. I saker som har utspilt seg på internett vil det derfor i følge *kripos* være umulig med en domfellelse uten slike bevis. *Kripos* mener det kom frem i deres egen undersøkelse at trafikkdata hadde betydning for flere ulike formål hvor trafikkdata ble innhetet og spesielt nyttig i forhold til kontroll over mistenkte/siktedes bevegelser, kontrollering av opplysninger fremkommet i politiavhør eller andre undersøkelser og til å kontrollere opplysninger om mistenktes/siktedes kontaktmønster. Undersøkelsen viste også i følge Kripos at det var variasjoner i hvilke formål trafikkdata ble benyttet til innenfor de ulike sakstypene (Ingerø 2010).

Det nasjonale statsadvokatembetet nevner i sin høringsuttalelse at det krever mye ressurser å innhente og bearbeide trafikkdata, men legger vekt på at det likevel må gjøres fordi nytten overstiger kostnaden. Det refereres til kripos undersøkelse som tilsa at trafikkdata innhentes i ca. 50% av de alvorlige straffesaken**e**. *Det nasjonale statsadvokatembetet* som er overordnet påtalemyndighet for Kripos og PST har siden opprettelsen i 2005 ikke hatt noen saker vedrørende organisert kriminalitet eller terrorbestemmelsene der trafikkdata ikke har utgjort en viktig del av bevisbildet). Siden disse bevisene oppfattes som objektive beviser påpeker *Det nasjonale statsadvokatsembetet* at disse bevisene også kan bidra til å frifinne uskyldige som er mistenkte i en sak (Frigaard & Glent 2010).

Økokrim utdyper videre at det er ingen andre etterforskningsmetoder som kan erstatte trafikkdata. *Økokrim* mener dette kommer spesielt tydelig frem i de tilfeller der etterforskningen kommer inn etter den aktuelle straffbare handlingen er begått (reaktiv etterforskning) og generelt der opplysninger rundt handlingsforløpet skal samles inn. Manglende tilgang til trafikkdata kan samtidig svekke politiets muligheter til å bruke andre etterforskningsmetoder på en effektiv måte i følge *økokrim*. *Økokrim* utdyper denne uttalelsen ved å påpeke at enkelte typer trafikkdata vil være nødvendig for at politiet skal kunne sette i

gang kommunikasjonskontroll etter straffeprosessloven §§216a og 216b. *Økokrim* påpeker at tap av tilgang til trafikkdata vil kunne føre til at bruken av andre og mer inngripende etterforskningsmetoder må økes i både antall og omfang (Schea 2010).

Dataene vil i følge *norsk narkotikaforening* etterhvert få mindre betydning for tilbyder ettersom de går over til en prismodell der prisene ikke varierer mellom abonnoment. Dataene vil i følge *norsk narkotikaforening* fremdeles vil være viktig i politiets etterforskning (Gulvedt 2010). *Politiets fellesforbund* er bekymret over en situasjon der datalagringsdirektivet ikke gjennomføres og mener det vil kunne få store konsekvenser for politet og samfunnets muligheter til å bekjempe kriminalitet. *Politiets fellesforbund* påpeker i sin høringsuttalelse at det bare er et spørsmål om tid før tilbyderne ikke lengre selv vil ha behov for å ta vare på trafikkdata i faktureringsøyemed og i en slik situasjon risikerer politiet å miste et av sine viktigste verktøy, noe politiets fellesforbund mener vil ha alvorlig konsekvenser og gå på bekostning av både demokratiet og rettsikkerheten (Johannessen & Gustafson 2010).

Aktørene innenfor behovsdiskursen beskriver datalagringsdirektivet som et viktig etterforskningsverktøy. Datalagringsdirektivet oppfattes som en ressurs politi- og påtalmynidgheter ikke kan klare seg uten. Aktørene frykter samtidig at ekomtilbyderne ikke lengre vil ha interesse av å lagre disse dataene selv i fremtiden fordi behovet kan forsvinne gjennom overgangen til faste prismodeller. Trafikkdata verdsettes høyt fordi det anses som objektive beviser i mange saker.

Risikodiskursen

Politijuristene problematiserer forslaget om å innskjerpe mistankekravet, slik at en bestemt person må kunne identifiseres før trafikkdata utleveres. Politijuristene utdyper at politiets formål med lagring av trafikkdata er å identifisere ukjente gjerningsmenn og innskjerpingen fremstår for *politijuristene* som lite gjennomtenkt. Dette anses ikke som en styrking av tilliten til prossessen eller som egnet til å styrke rettsikkerheten (Frantsvold 2010). Dagens ordning krever i følge *riksadvokaten* ikke skjellig grunn til mistanke mot en bestemt person. Det er tilstrekkelig at det foreligger skjellig grunn til mistanke om en straffbar handling og at materialet kan ha betydning som bevis (§210). Denne ordningen bør i følge *riksadvoakten*

videreføres, siden innhenting av trafikkdata ofte har som formål å identifisere en antatt gjerningsmann (Busch 2010).

Det vil i følge *det nasjonale statsadvokatembetet* være flere tilfeller hvor behovet for hastekompetanse vil være tilstede, for eksempel under en aksjon, hvor en må innhete data for å pågripe en person. *Det nasjonale statsadvokatembetet* mener det vil være uheldig å måtte vente til neste kontordag i slike tilfeller. De legger til at hastekompetansen også er viktig på grunn av plutselige rettsanmodninger fra utlandet og mener det er viktig for å vedlikeholde samarbeid mellom internasjonale politi- og påtalemyndigheter (Frigaard & Glent 2010).

Kripos mener en manglende evne til å bidra vil ramme samarbeidspartnerene, men mest av alt oss selv. På samme måte som de kriminelle søker anonymitet i det offentlige rom vil de i følge *kripos* også søke anonymitet i kyberrommet. *Kripos* fremhever at når et kriminelt nettverk velger sted for neste anslag så vurderer de ikke bare muligheten for utbytte, men også risikoen for å bli avslørt. Dersom datalagringsdirektivet ikke innføres i Norge frykter *kripos* at organiserte kriminelle grupperinger i enda større grad vil etablere seg her fordi sjansen for å bli tatt vil være mindre enn i nabolandene som har implementert direktivet (Ingerø 2010). *Det norske Statsadvokatembetet* tror Norge uten implementering kan ende opp som en frihavn for kriminelle på bakgrunn av klart dårligere metodemuligheter enn ellers i Europa (Frigaard & Glent 2010).

De kriminelle vil i følge *kripos* alltid ta hensyn til politiets kapasitet og metodebruk, men *kripos* mener det likevel ikke gjør saker umulig å oppklare og refererer til NOKAS-saken som et eksempel på hvordan kriminelle tidligere har prøvd å unngå politiets sporingsmuligheter gjennom nøye planlegging. Videre viser de tilbake til en historisk skepsis rundt effektiviteten av politiets metoder og referer blant annet til kritikken mot avlytting av telefon og hvordan det ville få mindre konsekvenser ettersom kriminelle gikk over til Skype-lignende løsninger. *Kripos* mener telefonavlytting har vist seg å være et viktig verktøy for politiet. *Kripos* mener motstrategiene gjør sakene mer kompliserte og de mener denne problemstillingen støtter opp om lengre lagringstid. Samtidig ønsker kripos å fremheve at en rekke typer kriminalitet ofte skjer i affekt der gjerningspersonen ikke har tatt spesielle forhåndsregler (Ingerø 2010). *Riksadvokaten* mener mange som i dag begår alvorlig kriminalitet benytter kommunikasjon som fanges opp og de synes derfor at omgåelsesmomentet ikke kan vektlegges ved en vurdering av dagens situasjon (Busch 2010).

Politidirektoratet mener vi uten lagring av trafikkdata vil gjøre internett til et sted der politiet ikke har tilgang uavhengig om det skulle foreligge mistanke rundt ulike kriminelle handlinger. *Politidirektoratet* mener det ofte fremheves som et argument at forbrytere vil finne nye veier og at politiet derfor alltid vil henge etter i utviklingen, men *politidirektoratet* legger til at politiet ikke kan la være å forsøke av den grunn (Gjengedahl 2010).

Aktørene innenfor risikodiskursen er opptatt av hvordan Norge vil se ut dersom datalagringsdirektivet ikke innføres. Dersom vi ikke innfører direktivet ser aktørene innenfor denne diskursen for seg at Norge vil bli en frihavn for terrorister og andre kriminelle. Aktørene er samtidig kritisk til tiltak som begrenser de rettighetene politi- og påtalemyndighetene har i dag og mener det bidrar til å vanskeliggjøre etterforskningen.

Mangfoldet av bevis

Oslo statsadvokatembeter mener mange i og utenfor politiet har bastante og unyanserte oppfatninger når det gjelder nytteverdien av datalagring. *Oslos statsadvokatembeter* fremhever at effektivitetsgevinster for politi og påtalemyndighet må veies opp mot tunge personvernshensyn. *Oslo statsadvokatembeter* påpeker at det vil være vanskelig å fremskaffe en kvantifiserbar nytteeffekt, men uten lagringsplikt kan politiets arbeid reelt svekkes og det kan være et argument for lagringsplikt uavhengig av selve direktivet (Øvigstad, Busch, Kvande & Aase 2010). *Oslo statsadvokatembeter* mener et avgjørende moment vil være hvilke andre bevismidler som er tilgjengelige i den aktuelle saken. Det kan være alt fra banktransaksjonsopplysninger som har lang lagringstid, vitneforklaringer, tingelige bevis, innhold av eventuelle avlyttede samtaler, mistenkelige feil i mistenkte/siktedes forklaring. *Oslo statsadvokatembeter* advares derfor mot det de mener er påstander om at manglende tilgang til lagrede trafikkdata vil være avgjørende i svært mange saker. *Oslo statsadvokatembeter* mener det heller inngår i en mer omfattende beviskjede. Betydningen vil også variere etter hvilken fase den aktuelle saken befinner seg i. *Oslos statsadvokatembeter* påpeker at trafikkdata utvilsomt vil være nyttig informasjon for kartlegging av for eksempel kontaktnett i en del tilfeller. *Oslo statsadvokatembeter* mener verdien av eldre informasjon (lengre lagringstid) ikke kan verifiseres utover gjetninger og antagelser. På generelt grunnlag vil *Oslo statsadvokatembeter* si at etterforskning er informasjonssamling og at mer informasjon derfor alltid vil ha verdi, men det blir problematisert av hensynet til blant annet

personvernet (Øvigstad, Busch, Kvande & Aase 2010). Oslo statsadvokatembeter skiller seg her fra de andre aktører innenfor politi- og påtalemyndighetene som har uttalt seg om behovet for datalagringsdirektivet. Trafikkdataene avskrives ikke fullstendig som en ressurs for politiet, men Oslo statsadvokatembeter legger seg heller ikke helt på linje med aktørene som står dem nærmest ideologisk.

Omgåelsesdiskursen

EL & IT Forbundet legger seg på linje med *Norweigan Unix User Group* om måten direktivet i første rekke rammer lovlydige borgere og ikke nødvendigvis vil være like effektivt ovenfor kriminelle og terrorister (Gundersen 2010). *TDC* mener erfaringer fra Danmark har vist at bruken av dataene ikke oppnår tilsiktede formål og har kostet mye. Det er samtidig i følge *TDC* et løpende ønske om å benytte de lagrede data til etteforskning generelt (Johansen 2010). *Telenor* mener den teknologiske utviklingen på mange måter har løpt fra direktivet gjennom webbaserte tjenester som ikke lagres hos tilbyder. Tjenester som nevnes er webbasert e-post, ventrilo, skype og muligheten for at uvedkommende tar i bruk usikrede trådløse nettverk (Krogh 2010).

Gjennom anonyme proxyservere eller programvare som er designet for å hindre sporbarhet og sikre anonymitet kan direktivet i følge *Norges juristforbund* enkelt omgås av de som ønsker det. *Norges juristforbund* trekker videre frem 'The Ring' (www.torproject.org) og 'Dold' (www.dold.se) som eksempler på slike tjenester. *Norges jursistforbund* nevner også muligheten for å kryptere sin trafikk eller ta i bruk webbaserte e-posttjenester. Gjennom slike tiltak kan forbrukere i følge *Norges juristforbund* kommunisere uten å legge igjen den informasjonen direktivet ønsker å fange opp. *Norges juristforbund* påpeker at det allerede finnes en rekke selskaper som tilbyr anonyme VPN-tjenester med krypterte linjer utenfor datalagringdirektivets virkeområde. Et eksempel på det sistnevnte som blir trekt frem er det Panama-baserte selskapet 'ShadowVPN' (www.shadowvpn.com). Teknologiutviklingen går i følge *Norges juristforbund* mot økte muligheter for å være anonym uavhengig av kommunikasjonsform og dette kan resultere i at direktivet ikke vil virke mot kriminelle som tar i bruk slike tjenester (Tengelsen 2010).

Datatilsynet nevner videre muligheter for unndragelse gjennom bruk av internettkafeer, usikrede trådløse nettverk, stjålne mobiler og fremtidig teknologi. I følge *datatilsynet* har det blitt hevdet at trafikkdata har vært nyttig i ca. 45% av alle saker hvor opplysninger har blitt innhentet av politiet, men *datatilsynet* er av den oppfatning at slik statistikk er meningsløs fordi politiet alltid vil ha nytte av mer informasjon. *Datatilsynet* mener også det er grunn til å tro at erfaringer gjort før datalagringsdirektivet eventuelt ble implementert ikke tar høyde for endringer i kriminell atferd (Apenes 2010).

Nei til EU retter en kritikk mot høringsnotatets manglende opplysninger rundt elektroniske kommunikasjonsformer som ikke omfattes av direktivet av praktiske årsaker. Nei til EU trekker frem sosiale nettsteder som Facebook, Biip og Orkut frem. Brebåndstelefoni og chattetjenester som IRC og MSN. *Nei til EU* mener det er sannsynlig at kriminelle raskt vil tilpasse seg den nye tilværelsen. *Nei til EU* ser for seg at effekten av direktivet muligens vil kunne irritere kriminelle og terrorister som tvinges til å omgå det, men effekten for selve etterforskningen anser de som minimal (Olaussen & Hobøl 2010). *Nav* mener det er åpenbart at grove og organiserte kriminelle miljøer vil tiplasse seg datalagringsdirektivet og nasjonale lovbestemmelser og dermed benytte seg av alternative kommunikasjonskanaler som ikke er sporbare (Saglie & Aulie 2010)

Aktørene innenfor omgåelsesdiskursen fremhever kommunikasjonsformer som ikke fanges inn av datalagringsdirektivet og muligheter for å kryptere sine egne data. Lovlydige borgere fremstilles som taperne ved en eventuell implementering siden de i utgangspunktet ikke vil ha behov for å aktivt skjule sine spor. Kriminelle og terrorister vil på den andre siden ha gode grunner for å aktivt gå inn for å omgå det datalagringsdirektivet har muligheten til å fange inn. Aktørene innenfor omgåelsesdiskursen mener derfor den potensielle nytteverdien til direktivet faller bort.

Dokumentasjonsdiskursen

Nødvendighetskravet er i følge *den internasjonale juristkommisjonen* presisert i den europeiske menneskerettsdomstolen slik at det fra statens sidet må godtgjøres at det foreligger et pressende samfunnsmessig behov for eventuelle inngrep overfor det enkelte individ som rammes. *Den internasjonale juristkommisjon* påpeker derfor at det ikke er tilstrekkelig at

direktivet er nyttig eller hensiktsmessig. Det skal i følge *den internasjonale juristkommisjonen* også være nødvendig. *Den internasjonale juristkommisjonen* mener det må påvises at inngrepet er egnet til å ivareta de hensyn som begrunner det, men også at de samme hensynene ikke kan ivaretas på alternative og mindre inngrepende måter. *Den internasjonale juristkommisjon* mener det må være proposjonalitet mellom mål og middel" (Lund & Wessel-Aas 2010).

Nei til EU viser til personvernskommisjonens sluttrapport og etterlyser en grundigere klargjøring i form av dokumentasjon av behovet for lagring. Det vises deretter til kravet i EMK artikkel 8 om skjellig grunn til mistanke (Olaussen & Hobøl 2010).

Landsorganisasjonen i Norge er bekymret for en økende kriminalitet som skjer via elektronisk overførte datatjenester og telefoni. *Landsorganisasjonen* mener denne formen for kriminalitet bidrar til å undergrave den legale økonomien som elektroniske medier potensielt utgjør. Landsorganisasjonen påpeker også at andre former for kriminalitet kan utvikles og kommuniseres gjennom digitale metoder. *Landsorganisasjonen i Norge* oppfatter den digitale verden som hersket av de kriminelle og anser myndighetene for å være på etterskudd i kampen mot kriminelle miljøer og enkeltpersoner. *Landsorganisasjonen i Norge* påpeker samtidig at direktivets klare svakhetspunkter er omgåelsesproblemet. *Landsorganisasjonen i Norge* mener direktivets effektivitetsgevinst må sannsynliggjøres og dokumenteres før en eventuell implementering. *Landsorganisasjonen* synes høringsnotatet er mangelfullt når det kommer til hvor effektivt direktivet vil være ovenfor kriminalitetsbekjempelse. *Landsorganisasjonen i Norge* fremhever også bekymringene til datatilsynet og personvernskommisjonen ovenfor personvernet tillegges stor vekt i det videre arbeidet med datalagringsdirektivet (Solbakken 2010). *Nav* synes hensikten med direktivet er god, men ser ikke at behovet for en utvidet og omfattende lagring av personopplysninger gir en så stor vinning for kriminalitetsbekjempelse at et slikt direktivet bør innføres på bekostning av personvernet. *Nav* ønsker derfor at nytteverdien av direktivet dokumenteres og konkretiseres ytterligere (Saglie & Aulie 2010).

Norsk senter for informasjonssikring mener en viktig faktor for om Norge bør innføre direktivet er avhengig av om andre land også gjør det. *Norsk senter for informasjonssikring* påpeker at trafikkdata er grenseoverskridende data og trafikken kan derfor være lagret i et annet land enn der tilbyder har tilhold. *Norsk senter for informasjonssikring* mener Norge bør

vurdere erfaringer fra land som allerede har tatt i bruk datalagringsdirektivet. Slike erfaringer er ikke beskrevet i høringsnotatet (Orderløkken 2010).

Abelia mener direktivet gir rom for store friheter og synes ikke det er klargjort hvor effektivt det vil være i forhold til de oppgavene det er ment å ta seg av. *Abelias* anbefaling er å avvente EU-kommisjonens evaluering av direktivets effekt i de landene som allerede har implementert det (Chaffey 2010).

Aktørene innenfor dokumentasjonsdiskursen er usikre rundt datalagringsdirektivets nytteverdi og ønsker at direktivet først skal testes ut i EU før Norge vurderer å implementere det. Behovet for å bekjempe alvorlig kriminalitet og personvernshensyn likestilles på en slik måte at direktivets effekt i andre EU-land kan vippe aktørene den ene eller den andre veien i forhold til å støtte eller være mot implementering.

Barns beste-diskursen

Barneombudet ser ikke bort fra at trafikkdata er viktig for politiets etterforskning og oppklaring av kriminelle handlinger. En pliktmessig lagring kan godtgjøre mange gode formål, men samlet kan disse dataene også utgjøre en stor trussel mot personvernet til barn. Det kan ikke være datalagringsdirektivet alene som trygger barn mot seksuelle overgrep og farene for en glidning i retning av et overvåkningssamfunn, uavhengig av de positive sidene må i følge *barneombudet* vektlegges. Det oppfattes derfor som problematisk å konkludere noe rundt datalagringsdirektivet gjennom et barneperspektiv (Haanes & Olsen 2010).

I lys av forpliktelsene Norge har gjennom barnekonvensjonen artikkel 34 til å beskytte barn mot seksuelle overgrep gjennom ny teknologi kan lagring av data for etterforskningsformål være formålstjenelig og nødvendig i følge *barneombudet*. Myndighetene har plikt til å beskytte barn. Denne plikten gjelder også i situasjoner der det vil gripe inn i barnets og familiens privatliv. *Barneombudet* mener samtidig at det er et alvorlig inngrep i barn og voksnes rett til personvern (Haanes & Olsen 2010).

Redd Barna ettersøker bedre dokumentasjon på hvor formålstjenelig et slikt inngrep vil være i beskyttelsen av barn. Internett brukes i dag til å utvekse og produsere bilder og filmer av overgrep og mishandling av barn både lokalt og globalt. Kripos har i debatten om datalagringsdirektivet påpekt at lagringen av trafikkdata er en sentral forutsetning for å

etterforske seksuelle overgrep som foregår på nett. Det etterlyses dokumentasjon for en slik påstand. *Redd barna* mener samtidig det er avgjørende at politiet har effektive verktøy til å etterforske nettovergrep, men savner alternativer til datalagring. Rapporteringsfunksjoner til politiet nevnes deretter som et alternativ som allerede er i bruk (Borgen & Hegg 2010).

Aktørene innenfor barns beste-diskursen har koblinger til både personvernsdiskursen og dokumentasjonsdiskursen. Datalagringsdirektivet blir ikke beskrevet som noe utelukkende positivt for barns sikkerhet, men aktørene er samtidig åpne for å endre oppfatning dersom effektiviteten til direktivet kan dokumenteres i andre land som har innført direktivet. Det interessante er likevel at barns personvern blir fremhevet isteden for barns sikkerhet fordi aktørenene innenfor denne diskursen som regel behandler barn som har vært utsatt for ulike former for overgrep. Det ville i utgangspunktet vært naturlig å anta at aktørene innenfor barns beste-diskursen ville koble seg til offerdiskursen som blir trekt frem under sikkerhetsdiskursen.

Personvernsdiskursen

Aktørene innenfor personvernsdiskursen er gjennom måten oppgaven er satt opp på, representativt for prinsipielle motstandere av direktivet. Det kan derfor være viktig å påpeke at sikkerhetsdiskursen som blir introdusert like etter også fokuserer på personvernet, men med større vekt på sikkerheten rundt datalagringsdirektivet og ofrenes personvernsrettigheter. Denne inndelingen er gjort for å enklere kunne skille aktørenes ideologiske beskrivelse av datalagringsdirektivet med tanke på personvernet.

Utglidningsdiskursen

FriBit påpeker at politiet allerede har tilgang til enorme mengder data som allerede finnes hos teletilbydere og som lagres der til praktiske formål. *FriBit* mener politiet har muligheten til å hente ut eller fryse ned disse dataene ved behov. *FriBit* påpeker videre at det er politiets oppgave å oppklare lovbrudd og i den sammenheng vil det i følge *FriBit* alltid være behov for mer informasjon. *FriBit* mener det er viktig å være kritisk til dette behovet og legger i sin høringsuttalelse vekt på at det må være proporsjonalitet mellom gevinsten for politiet og konsekvensene ulike tiltak kan ha for borgerne (Dragly 2010). *Norsk forening for*

kriminalitetsreform trekker frem i sin høringsuttalelse at politiets søken etter nye etterforskningsmidler er et umettelig behov fordi det uavhengig av suksess vil bli ansett som et stort fremskritt og avvikling som et stort tilbakeskritt. *Norsk forening for kriminalitetsreform* referer videre til politiets egne uttalelser der politiet har ytret misnøye med det de mener er vesentlige rettsikkerhetsmomenter som 'skjellig grunn til mistanke' for å kunne hente ut data og fraværet av hastekompetanse (Haraldseid & Renland 2010). En hver kritikk av direktivet vil i følge *Norsk forening for kriminalitetsreform* møtes med argumentet om at det svekker politiets evner til å forfølge alvorlig kriminalitet. *Norsk forening for kriminalitetsreform* tror derfor det vil bli vanskelig å argumentere mot fremtidig styrking og ekspandering av direktivet dersom politiets behov får presedens. Det vil i følge *norsk forening for kriminalitetsreform* alltid være en svekkelse for politiet når ytterligere overvåkning ikke aksepteres (Dragly 2010).

Norges juristforbund mener høringsnotatet legger opp til at direktivet garantert vil øke oppklaringsprosenten for politiet og at ny teknologi vil kunne gi avgjørende bevis i mange saker. En slik tilnærming til direktivet anses derimot som problematisk fordi det i følge *norges juristforbund* ikke angir noen kjerneverdi for hvor de eventuelle grensene for innsamling av bevis skulle befinne seg. *Norges Juristforbund* trekker videre frem i sin høringsuttalelse hvordan tilgangen til de lagrede dataene etterhvert kan bli aktuelle for andre aktører enn politi- og påtalemyndighet. Faren for lekkasjer og utglidning trekkes frem som potensielle problemer ved en implementering, hvor misbruk etterhvert forventes å finne sted. *Norges Juristforbund* argumenterer for at dette er uungåelig gjennom å beskrive det som en naturlov at informasjon som eksisterer vil bli brukt og legger derfor til at de frykter politikerenes vilje til å finne stadig nye måter å bruke opplysningene på slik at personvernet i deres øyne minimaliseres (Tengelsen 2010). *Datatilsynet* utdyper denne kritikken og mener det etterhvert vil fremtvinges et behov for å lagre innholdsdata for blant annet internettsurfing, for å kunne registrere e-poster som blir sendt og motatt gjennom webbaserte tjenester og innholdsdata fra telefonsamtaler for å verifisere hvem som faktisk har benyttet en påstått stjålet telefon (Apenes 2010).

FriBit legger i sin høringsuttalelse vekt på at implementering av datalagringsdirektivet kan føre med seg en snøballeffekt og nevner spesifikt strategisk informasjonsanalyse som et eksempel på noe som vil kunne være et nyttig verktøy for politiet for å identifisere potensielle kriminelle. Slike analyser kan bidra til å oppdage generelle mønstre, men det påpekes

samtidig at slike data kan gi falske positiver (Dragly 2010). *Elektronisk forpost Norge* mener grunnen til dette er kompleksiteten rundt slike databeregninger (Østmoen & Gramstad 2010). Høringsnotatet legger ikke i utgangspunktet opp til en slik bruk av de lagrede dataene, men aktører innenfor utglidningsdiskursen legger likevel vekt på slike potensialer for å fremheve sin kritkk av datalagringsdirektivet.

Stopp datalagringsdirektivet henviser til tidligere erfaringer med større tilgjengelighet for informasjon som kan hentes ut fra lagrede trafikk- og lokasjonsdata og mener med bakgrunn i disse erfaringenene at det vil føre til at flere vil gjøre krav om å få tilgang. Det refereres til England hvor direktivet på dette tidspunktet allerede var implementert og til sammen 600 forskjellige myndighetsinstitusjoner hadde tilgang til dataene som direktivet pålegger tilbydere å lagre. *Stopp datalagringsdirektivet* mener derfor at selv om direktivet fastslår at kun politiet skal ha tilgang er det ingen garanti mot en formålsglidning (Michelsen m. fl 2010). Interesseorganisasjoner innenfor intellektuell eiendom nevnes også som potensielle aktører som etterhvert vil være interessert i å få tilgang på de lagrede dataene. *FriBit* nevner spesielt et tilfelle der Post- og teletilsynet fikk pålagt brudd på taushetsplikten i forbindelse med den sivile opphavsrettstvisten rundt ”Max Manus-saken”. *FriBit* mener presedensen som ble lagt ned i denne rettsaken viser at sterke interesser fremdeles kan få gjennom krav om legitim utlevering av data selv med lovpålagte krav om taushetsplikt (Dragly 2010).

Aktørene som faller inn under utglidningsdiskursen fremhever i stor grad de potensielle konsekvensene av datalagringsdirektivet med referanser til eksisterende og potensialet til fremtidige 'overvåkningssystemer'. Aktørene innenfor denne diskursen stoler ikke på begrensningene som er fremhevet i høringsnotatet og oppfatter direktivet som en del av et større sosialt prosjekt for å skape sosial kontroll.

Frimodighetsdiskursen

Elektronisk Forpost Norge mener videre at utvidelser av datalagring, selv om det er blitt mer vanlig, utfordrer viktige verdier for et fritt samfunn. *Elektronisk Forpost Norge* legger samtidig vekt på at det vil være de svakeste i samfunnet som vil lide først under det de oppfatter som en overdreven kontrollvilje (Østmoen & Gramstad 2010). *Nei til EU* mener nytteverdien må veies opp mot effekter på frimodighet. Det legges i høringsnotatet opp til en regulering av tilgangen politiet vil ha til dataene, men *nei til EU* mener dette må vurderes

uavhengig av denne reguleringen fordi de tror vissheten om at all trafikkdata lagres og muligheten for sporing kan medføre en begrensning i individuell frihet. Det trekkes frem at direktivet er i strid med EMK og *nei til EU* er derfor av den oppfatning at direktivet svekker rettsnytelsen rundt privatliv og privat kommunikasjon og dermed vil være et ufroholdsmessig inngrep i ytringsfriheten (Heming & Hobøl 2010).

Å holde informasjon privat handler i følge *samfunnsorganisasjonen demos* om respekt for individets selvstendighet og integritet. Samfunnsgruppen demos påpeker at hemmelig informasjon ofte handler om den fordel eller makt som kan oppnås ved å skjule noe for andre. *Samfunnsorganisasjonen demos* legger vekt på at persovern i motsetning handler om informasjonsvern. *Samfunnsorganisasjonen demos* tror tilliten til samfunnsinstitusjoner vil svekkes hvis befolkningen mottar løfter som enkeltindivider umulig kan vite for sikkert blir opprettholdt. Det vil i følge *samfunnsorganisasjonen demos* være en tillit som kun baserer seg på etiske og moralske normer, noe *samfunnsorganisasjonen demos* mener kan føre til ubevisste begrensninger i egen atferd og uttalelser. Når store mengder sensitiv informasjon lagres for fremtidig bruk tror *samfunnsorganisasjonen demos* det vil spille inn i enkeltindividers vurderinger av tillit og risiko i forhold til samfunnet og myndighetene (Finneid 2010). *Elektronisk forpost Norge* mener tillitsforholdet mellom borgere og myndigheter og mellom samtidlige medlemmer i samfunnet vil uungåelig lide og bli preget av større mistro dersom datalagringsdirektivet innføres (Østmoen & Gramstad 2010).

EL & IT Forbundet legger i sin høringsuttalelse vekt på at direktivet på prinsipielt grunnlag ikke kan repareres gjennom mer eller mindre strenge regler rundt når og til hva opplysningene kan brukes til av myndighetene. *EL & IT Forbundet* mener det ikke handler om vi har noe å skjule, men i større grad om beskyttelse av den private sfæren som et fellesgode i det de oppfatter som et fungerende demokrati gjennom en informasjons- og kontrollbalanse (Gundersen 2010).

EL & IT Forbundet legger til at direktivet kan bidra til å frata samfunnsgrupper muligheten til å utvikle og utveksle tanker, meninger og strategier i fortrolighet (Gundersen 2010). Det er et viktig rettsprinsipp for EL & IT Forbundet at ingen som ikke er under etterforskning skal overvåkes på noen måte (Gundersen 2010). *Datatilsynet* mener datalagringsdirektivet vil medføre en rekke utfordringer i forhold til ytringsfriheten, forsamlings- og foreningsfriheten

og muligheten til å gjennomføre anonym varsling og kildevern, noe de mener kan være hemmende for atferd som er både lovlig og samfunnstjenelig (Apenes 2010).

FriBit mener direktivet kan føre til en endring i folks atferdsmønster og henviser til potensialet for en 'chilling effect'. *FriBit* beskriver effekten som selvsensurering pågrunn av overvåkning av privat kommunikasjon der balansen eller grensen mellom det offentlige og private forskyves. Hvor nasjoner baserer seg på mistillit fremfor tillit og uskyld må bevises til en hver tid (Dragly 2010). Både *den internasjonale jursitkommisjon* og *stopp datalagringsdirektivet* trekker i sine høringsuttalelser frem en undersøkelse som ble utført i Tyskland i 2008. Undersøkelsen viste tegn til at datalagringsdirektivet hadde endret tyske borgerers atferd. (Michelsen m. fl 2010, Lund & Wessel-Aas 2010). Så lenge direktivet er implementert mener *elektronisk forpost No*rge at lovgivningen alltid vil være flytende rundt populistiske ideer, politiske flertall og stemningsgivninger. Når dataene først er lagret mener elektronisk forpost Norge at borgerne ikke har noen sikkerhet mot fremtidig misbruk (Østmoen & Gramstad 2010).

Aktørene som befinner seg innenfor frimodighetsdiskursen er spesielt opptatt av individuell frihet. Datalagringsdirektivet blir i den sammenheng fremstillt som en trussel mot denne friheten. Det er en trussel mot aktørenes ideologi rundt hvordan et fritt samfunn skal fungere. Frykten innebærer at muligheter for å være anonym vil forsvinne dersom direktivet implementeres. Uten muligheten for å være sikker på sin anonymitet i den private sfæren tror aktørene innenfor denne diskursen at det vil føre til selvsensurering. En slik tolkning av datalagringsdirektivet ligger nært opp til begrepet om det virtuelle panoptikon (Hannemyr 2002) der usikkerheten for om en blir sett fører til en form selvdisiplinering.

Rettsprinsippdiskursen

Elektronisk forpost Norge mener at det i en rettsat ikke kan være akseptabelt at myndighetene i lang tid skal kunne tillegne seg kunnskap om lovlydige borgeres bruk av telefon, e-post, sms/mms-meldinger og eventuelt nettbruk, ved å kreve at det skal lagres detaljerte opplysninger om hvem og med hva borgerne kommuniserte og om når disse kommunikasjonshandlingene fant sted (Østmoen & Gramstad 2010). *Elektronisk forpost Norge* påpeker samtidig at EMK artikkel 15 åpner opp for unntakssituasjoner der krig eller annen nødsituasjon truer nasjonens liv hvor staten kan komme med innskrenkinger i

ytringsfriheten og privatlivet som normalt ikke vil være i harmoni med menneskerettigheter (Østmoen & Gramstad 2010). *Den internasjonale juristkommoisjon* sammenligner vi nærmer oss en kronisk unntakstilstand der forholdet mellom stat og borger endrer karakter og målet om et fritt samfunn blir forlatt og friheten i den private sfæren permanent må vike plass for statlig kontroll og overvåkning (Lund & Wessel-Aas 2010). *EL & IT Forbundet* legger til at retten til å ikke være overvåket når det ikke foreligger en konkret mistanke er et viktig rettsprinsipp i demokratiet (Gundersen 2010). *Stopp datalagringsdirektivet* mener demokratiet er avhengig av et gjensidig tillitsforhold mellom borger og stat. Stopp Datalagringsdirektivet mener borgernes friheter innskrenkes for mye til fordel for økt statlig kontroll og at det vil svekke tilliten, og med det også demokratiet (Michelsen m.fl 2010).

Samfunnsorganisasjonen demos mener det er urovekkende at det i senere tid har skjedd en økt sentralisering av verdifull og personsensitiv informarsjon om individers aktiviteter. Samtidig ser *samfunnsorganisasjonen demos* for seg en konstant utvikling av slike systemer som alltid vil ha rom for forbedringer og utvidelser. *Samfunnsorganisasjonen demos* ønsker ikke at slike løsninger skal gå på bekostning av det de oppfatter som grunnleggende menneskerettigheter og demokratiske rettsprinsipper (Finneid 2010).

Elektronisk forpost Norge mener kjernen til balansen mellom borgere og myndigheter som en ufravikelig forutsetning for rettstaten og for demokratiet. Uten en slik balanse er *elektronisk forpost Norge* av den oppfattning at forutsetningene for et samfunn der innbyggerne har medbestemmelsesrett og trygghet mot overgrep fjernes (Østmoen & Gramstad 2010).

Direktivet reiser samtidig i følge *advokatforeningen* spørsmål rundt grunnleggende menneskerettigheter, deriblant retten til privatliv som de mener er beskyttet av EMK artikkel 8 (Reiss-Andersen & Smith 2010). Stopp datalagringsdirektivet finner det underlig at norske myndigheter legger til grunn for at høringsnotatet er i tråd med menneskerettighetene når omfanget av direktivets personvernsutfordringer underkjent på prinsipielt grunnlag i begge landene som prøvde direktivet for domstolene. Stopp datalagringsdirektivet referer til domstolene i Romania og Tyskland der direktivet ble dømt grunnlovsstridig og i strid med EMK (Michelsen 2010). *Datatilsynet* legger vekt på at det er en fare for at fremtidige regjeringer ikke vil ha den samme demokratiske forankringen som vi har i dag. Høringsnotatet mangler i følge *datatilsynet* en ansvarlig utredning hvor det reflekteres over mulighetene for myndighetsmisbruk (Apenes 2010).

Nei til EU mener reguleringen vil gripe inn i livet til hver enkelt borger gjennom å redusere verdien av privatliv og integritetsvern, noe de oppfatter som en svekkelse av demokratiet som et gode. Det strider derfor i følge *nei til EU* mot norske tradisjoner og eksisterende lover (Olaussen & Hobøl 2010). *Elektronisk forpost Norge* mener hensynet til premisset om at borgerne skal kontrollere staten, og ikke omvendt tilsier at regjeringen må snu i denne saken og mener rettstatens prinsipper gir et imperativ om at personvernbegrepet skal tolkes og defineres i lys av befolkningens rettsikkerhet og trygghet mot maktmisbruk (Østmoen & Gramstad 2010).

Datatilsynet reagerer på at departementene begrunner behovet for datalagring med muligheten opplysningene potensielt vil ha for å frikjenne noen som er urettmessig mistenkt for alvorlig kriminalitet og mener det er i strid med uskyldispresumpsjonen som er stadfestet i EMK artikkel 6 (Apenes 2010). *Stopp Datalagringsdirektivet* legger til i sin høringsuttalelse at en slik tilnærming snur uskyldspresumpsjonen på hodet og mener det rettferdiggjør enhver inngripen fordi det kan anses som et gode (Michelsen 2010). *Norsk forening for kriminalitetsreform* mener direktivet ikke skiller mellom mistenkte og uskyldige borgere, men tar utgangspunkt i at all trafikkdata skal lagres uavhengig om det finnes en rettslig påkjennelse (Haraldseid & Renland 2010).

Den internasjonale juristkommisjon mener det er snakk om utvikling av en mer preaktiv strafferett og innføring av sterkere kontroll- og tvangsmidler for staten i kriminalitetsbekjempelsens navn, noe de mener er et steg i retning av politistaten (Lund & Wessel-Aas 2010).

Aktørene innenfor rettsprinsippdiskursen mener direktivet utfordrer sentrale rettsprinsipper og menneskerettigheter i et demokrati. Denne tolkningen baserer seg på at direktivet vil føre til overvåkning av befolkningen eller en følelse av å være overvåket. Det sistnevnte kan igjen kobles til Hannemyrs (2002) begrep om et virtuelt panoptikon. Aktørene mener uskyldspresumpsjonen blir snudd på hodet fordi direktivet lagrer trafikkdataene til alle og ikke baserer seg på konkrete mistanker. Aktørene mener derfor at tilliten mellom befolkningen og myndighetene svekkes fordi befolkningen ikke kan være sikre på at de lagrede dataene ikke kommer til å bli misbrukt. Aktørene er samtidig skeptisk til ordleggingen rundt datalagringsdirektivets potensial for å frikjenne mistenkte individer.

Sikkerhetsdiskursen

Aktørene innenfor sikkerhetsdiskursen er kritisk til sammenligningen mellom datalagring og overvåkning. Det fremheves at dataene allerede er i systemet og at politi- og påtalemyndigheten kun ønsker å utsette slettingen av disse dataene for å kunne sikre spor i etterkant av et lovbrudd. Datalagringsdirektivet blir dermed ikke fremhevet for sin potensielle prevantive effekt, men isteden fremhevet for sin rolle i etterforskningsprosessen. Sikkerheten rundt dataene blir også fremhevet i forhold til de strenge reglene som vil være tilstede for å kunne hente ut dataene og hvordan dataene vil være krypterte så lenge de ikke er begjært. I forhold til personvernet er det et større fokus på offeret og hvordan politiets oppgave er å beskytte befolkningen mot kriminalitet.

Krypteringsdiskursen

Politiets fellesforbund mener kravene til sikkerhet rundt dataene vil ivareta samfunnet og enkeltindividets behov for sikkerhet og personvern. I følge *politiets fellesforbund* vil personvernet styrkes gjennom implementering av datalagringsdirektivet fordi slike opplysninger ofte benyttes i etterforskningen og fremstår som avgjørende for å bevise både skyld og uskyld (Johannessen & Gustafson 2010). *Kripos* påpeker at det er sikkerheten rundt de lagrede data og graden av tilgjengelighet som er de sentrale faktorene i sammenheng med personvernet (Ingerø 2010). *Politiets fellesforbund* mener straffeprosessloven vil ivareta personvernet og rettsikkerheten til den eller de som er mistenkt eller siktet i en straffesak i tillegg til lover som regulerer og sanksjonerer urettmessig innsyn (Johannessen & Gustafson 2010). *Svein Willassen AS* påpeker at risikofaktorer for personvern ved datalagring henger sammen med hvem som har tilgang til dataene. Kryptering av data på en slik måte at datainnholdet ikke kan leses av noen medfører i følge *Svein Willassen AS* til at risikofaktorene for personvernet fjernes. *Svein Willassen AS* påpeker likevel at publisering av data vil kunne medføre en betydelig risikofaktor for personvernet for de dataene omhandler. *Svein Willassen AS* oppfatter derfor risikoen som avhengig av den praktiske tilnærmingen i motsetning til en prinsipiell tilnærming der enhver lagring av data anses som skadelig for personvernet uavhengig om dataene kan leses av noen eller ikke (Willassen 2010). *Kripos* legger vekt på at det finnes lagringsløsninger som krypterer alle dataene som genereres og på denne måten gjør de uleselig for alle parter, teletilbyder og politiet inkludert. Slik kan de i følge kripos forbli til

det foreligger en rettslig kjennelse for at politiet skal ha tilgang til dataene. *Kripos* legger seg på linje med Svein Willassens utredning som påpeker at uleselige data vil redusere misbrukspotensialet og øvrige personvernsmessige betenkeligheter til et minimum (Ingerø 2010).

Aktørene innenfor krypteringsdiskursen mener datalagringsdirektivets potensielle trussel mot personvernet avverges gjennom sikkerheten rundt lagringen. Om dataene sikres godt nok oppleves farene forbundet med potensielt misbruk og trusselen mot personvernet som minimal. Denne sikkerheten mener aktørene innenfor krypteringsdiskursen kan oppnås ved å kryptere dataene og sørge for at bare de relevante instansene har tilgang til en sikkerhetsnøkkel som kan åpne opp for å lese dataene.

Offerdiskursen

Riksadvokaten har merket seg at både Politidirektoratet, Kripos, Sjefen for PST, og en rekke politimestre har dokumentert behovet for tilgang til trafikkdata gjennom politiets virksomhet, både for ulike sakstyper og konkrete saker. Konklusjonen til Riksadvokaten ut fra dagens situasjon er derfor at materiale som i dag lagres i en periode har vist seg å være meget nyttig ved politiets etterforskning og om ikke DLD innføres, vil politi og påtalemyndigheten, og domstolene ikke få tilgang til denne informasjonen i fremtiden. (Busch 2010).
Det norske statsadvokatembetet mener direktivet er forenelig med EMK artikkel 8. fordi personvernet gjelder like mye for offerets fundamentale rettigheter (Frigaard & Glent 2010).

Riksadvokaten tror ikke direktivet vil medføre vesentlige endringer for borgerne sammenlignet med situasjonen i dag utover lagringstid og formålet med lagringen. Riksadvokaten utdyper at direktivet i seg selv er i strid med EMK artikkel 8 nr.1, men om implementering skjer med de foreslåtte lovendringer vil innføringen være i tråd med EMK art. 8 nr.2. *Riksadvokaten* påpeker at direktivet oppfyller nødvendighetskriterier i EMK art. 8 nr.2 fordi trafikkdata anses som viktig for å oppklare og iretteføre en lang rekke kriminalitetstyper (Busch 2010).

Kripos mener en annen måte å se på EMD Artikkel 8 nr.1 er å anse direktivet som en forutsetning for at Norge skal kunne ivareta forpliktelser med utgangspunkt i personvernet til

ofrene for kriminelle handlinger. Norge har i følge *kripos* forpliktelser til blant annet FNs barnekonvensjon. *Kripos* mener derfor at direktivet er nødvendig for at Norge skal være i stand til å verne privatlivet til den enkelte borger. *Kripos* påpeker at myndighetene har en forpliktelse i forhold til å identifisere og straffeforfølge personer som krenker andres liv, helbred og rett til privatliv. *Kripos* oppfatter det som vanskelig å ivareta en slik forpliktelse uten implementering av datalagringsdirektivet (Ingerø 2010). *Politiets fellesforbund* påpeker samtidig at Norge gjennom menneskerettskonvensjonen også har forpliktet seg til å sikre politiet effektive etterforskningsverktøy for å kunne bekjempe kriminalitet (Johannessen & Gustafson 2010).

Aktørene innenfor offerdiskursen utfordrer personvernsdiskursen gjennom å fremheve at offerets integritet kan bli krenket av å bli utsatt for kriminelle handlinger. EMK artikkel 8 blir derfor tolket som et argument for isteden for mot innføring av datalagringsdirektivet fordi Norge plikter seg også til å bekjempe kriminalitet.

Anonymitetsdiskursen

Økokrim mener datalagringsdirektivet vil utgjøre en relativt liten andel av den samlede mengden personlige data som lagres i dag. *Økokrim* trekker frem at vi legger igjen elektroniske spor i personregistre, kunderegistre, pasientregistre og hos finansinstitusjoner, til og med når vi kjører gjennom en bomring. *Økokrim* mener det gir grunnlag for å si at befolkningen ikke anser slike data som veldig personlige eller sensitive. Det vil derfor i følge *Økokrim* være grunn til å tro at lagring av trafikkdata ikke vil virke særlig hemmende på folks personlige utfoldelse og frimodighet. Økokrim trekker også frem at de mener trafikkdata er mindre sensitivt enn innholdsdata (Schea 2010). *Kripos* stiller seg tvilende til at direktivet vil ha en 'chilling effect' og mener et slikt hensyn eventuelt må være basert på at det faktisk kan påvises en klar effekt og årsakssammenheng i de europeiske landene som har innført direktivet (Ingerø 2010). Det Norske Statsadvokatembetet kaller faren for en kjølende effekt for en udokumentert påstand og mener den tyske undersøkelsen ikke kan dokumentere en slik effekt. Det argumenteres for at Norge har hatt datalagring helt siden telefonen ble introdusert og at det har blitt brukt som bevis i minst 16 år. De mener frimodigheten heller har økt med de gode mulighetene for nettanonymitet (Frigaard & Glent 2010).

Aktørene innenfor anonymitetsdiskursen mener kritikken av datalagringsdirektivets potensielle 'chilling effect' er sterkt overdrevet. Datalagring anses ikke som et nytt fenomen, men noe norske borgere har levd med i lang tid uten å bli merkbart påvirket. Det fremheves at vi allerede legger igjen mange spor og at det til nå ikke har virket å begrense individers utfoldelse på nett. I forhold til omgåelsesdiskursen påpeker aktørenene innenfor anonymitetsdiskursen at mulighetene for å være anonym fremdeles er store.

Tilhengere med forbehold om strenge krav

Tekna oppfatter det som et verdispørsmål hvor langt teknologien skal kunne benyttes til et omforent godt formål når det går på bekostning av enkeltindividets integritet. *Tekna* mener det er grunnleggende personvernshensyn som må vike for at politiet, og eventuelt andre skal få muligheten til å kontrollere den enkelte borgers opptreden og kontakt med andre. *Tekna* påpeker at datalagringsdirektivet inneholder enorme muligheter og mener det bringer med seg en fare for misbruk. *Tekna* tror samtidig det er lite sannsynlig at direktivet noen gang vil reverseres om det eventuelt blir implementert. *Tekna* mener det uansett er viktig at politiet har mulighet til å bekjempe den typen kriminalitet som ny teknologi bringer med seg. Tekna utdyper at forutsetningen må være at lagringen skjer innenfor en fast og tidsavgrenset ramme med et kontrollorgan som har tillit i folket. Hensyn til personvernet bør i følge *Tekna* basere seg på at uvedkommende ikke får mulighet til å misbruke opplysningene. *Tekna* mener det under forutsetningen om at myndighetene styrker kontroll- og sikkerhetsrutiner rundt bruk, lagring og oppbevaring av data, ikke er noe som står i veien for at *Tekna* støtter implementering (Johnsen 2010).

Internett og telebransjens anti-kriminalitets tiltak mener en innføring av datalagringsdirektivet vil kreve en balansegang. *Internett og telebransjens anti-kriminalitets tiltak* mener at det på den ene siden finnes et hensyn til effektiv etterforskning og på den andre siden finnes et hensyn til individets integritet og personvern. *Internett og telebransjens anti-kriminalitets tiltak* mener det derfor må legges opp til gode og tydelige saksbehandlingsregler for uthenting av slike data (Seip & Johansen 2010).

Unio mener elektroniske spor som 'tause vitner' har blitt stadig viktigere for politiets bekjempelse av organisert og alvorlig kriminalitet. Det er samtidig viktig for *Unio* at borgerne er forsikret om at lagring og bruk av trafikkdata skjer i henhold til intensjonen med direktivet

og at dataene kun kan hentes ut når det er rettslig grunnlag for det (Hovdesnakk & Solgaard 2010).

Post- og Teletilsynet mener på generelt grunnlag at tilgangen til trafikkdata bør begrenses til de tilfeller hvor fordelene med å få tilgang til trafikkdata for mottakende etat klart overstiger de personvernsmessige konsekvensene. Denne vurderingen bør gjøres konkret og individuelt. De mener det derfor bør skrives en eksklusiv lovhjemmel dersom en etat skal få tilgang til trafikkdata. For sivile parter foreslår *post- og teletilsynet* at deres rolle i dag når det gjelder fritakelse fra taushetsplikten skal opprettholdes (tvisteloven §22-3) (Jensen & Storm 2010).

Politiets sikkerhetstjeneste stiller seg bak direktivet, men har forbehold om at en implementeringen tar i bruk strenge omstendigheter for tilgang. *Politiets sikkerhetstjeneste* støtter forslaget om at all form for tilgang og bruk må godkjennes av en domstol. *Politiets sikkerhetstjeneste* legger også til at det bør være straffesanksjoner for teletilbydere og deres ansatte dersom taushetsplikten brytes under andre omstendigheter. Det foreslås samtidig at politiet kan få hjemmel for hastekompetanse (Kristiansen 2010).

Norsk senter for informasjonssikring mener det er viktig å fokusere på sikring av dataene fremfor å stille seg negativ til direktivets overvåkningspotensial. *Norsk senter for informasjonssikring* utdyper samtidig at det er viktig å sikre trafikkdata på en sånn måte at personvernet ikke blir krenket. Det er snakk om store mengder trafikkdata og med en innføring av datalagringsplikt vil det i følge *Norsk senter for informasjonssikring* være behov for strenge sikringstiltak (Orderløkken 2010).

Aktørene som krever strenge tiltak rundt implementering av datalagringsdirektivet avviser ikke i like stor grad de hensyn som trekkes frem under personvernsdiskursen. Sikkerheten rundt de lagrede dataene står her sentralt samtidig som aktørene uttrykker bekymringer rundt de personvernsmessige konsekvensene direktivet kan innebære dersom sikkerheten ikke er optimal.

Økonomidiskursen

Aktørene innenfor de økonomidiskursen tar hovedsakelig for seg de økonomiske konsekvensene direktivet innebærer for de ulike instansene som faller inn under direktivets domene. Kostnadsdiskursen fremhever kostnadene forbundet med ekomtilbydernes behov for

en utvidet lagringskapasitet og sikkerhet. Samfunnsansvarsdiskursen vektlegger at disse kostnadene bør anses som et samfunnsansvar for ekomtilbyderne. Realiseringsdiskursen påpeker utfordringene rundt implementeringen fra en av aktørene som har stått bak innføringen av direktivet i andre land. Konkurransevridningsdiskursen stiller seg kritisk til tolkningsaspektet rundt hvorden hvert enkelt land ønsker å implementere direktivet og de konkurransevridningene det kan medføre. Kundetillitsdiskursen samsvarer delvis med kritikken vi finner i overvåkningsdiskursen med fokus på tillitsforholdet mellom ekomtilbyder og kundene. Opphavsrettdiskursen er på sin sidet klar på at datalagringsdirektivet er nødvendig for å beskytte deres økonomiske interesser. Itillegg har vi en EØS-diskurs som tar opp relevansen direktivet har til EØS-avtalen.

Kostnadsdiskursen

Stiftelsen Elektronikkbransjen er grunnleggende positiv til intensjonen med datalagringsdirektivet om forebygging av kriminalitet, men kritisk til at bransjen pålegges å innhente ytterligere informasjon enn det aktørene selv har behov for i forbindelse med sin virksomhet. De mener politet og påtalemyndighetene allerede har tilgang til den informasjonen de ønsker. De økonomiske kalkyliene til teleplan anses som usikre og det er en frykt for store usikre kostnader. Slike kostnader vil i følge Stiftelsen Elektronikkbransjen bli overført til forbrukerne gjennom dyrere tjenester. Bransjen er på generelt grunnlag svært kritiske til at aktørene pålegges å samle inn informasjon om kundenes bruk av deres tjenester utover det de har behov for (Bjørke 2010). Direktivet vil i følge *Get AS* føre til betydelig arbeid og kostnader for tilbyderne i forbindelse med etablering og håndheving av nye systemer og rutiner. Tilbyder har i følge *Get AS* ikke behov for dataene siden de ikke kan benytte dem til eget formål og tjenesten utføres derfor på statens vegne for å bidra til bekjempelsen av kriminalitet. Det er derfor viktig for *Get AS* at kostnadene dekkes av staten og de er sterkt i mot at tilbydere skal dekke deler av kostnadene (Myksvoll 2010). *Nei til EU* mener samfunnskostnaden ikke vil være proporsjonal i forhold til direktivets effekt (Olaussen & Hobøl 2010). De største vinnerene ved implementering av datalagringsdirektivet vil i følge *Norges Juristforbund* være konsulentselskapene som skal utvikle systemene som må til for å ivareta reglene (Tengelsen 2010).

Aktørene innenfor kostnadsdiskursen mener datalagringsdirektivet er en vesentlig utvidelse av

dataene som allerede lagres hos tilbyderne. Det er samtidig stor usikkerhet forbundet med de potensielle kostnadene for lagring og sikring av dataene mot inntrengere. Datalagringsdirektivet anses samtidig som en utgiftspost som aktørene ikke vil få noe igjen for siden de selv ikke vil ha tilgang til dataene.

Samfunnsansvarsdiskursen

Politidirektoratet setter spørsmål til om staten gjennom politiet skal bære betydelige kostnader for hver enkelt tilbyder, i et marked som er i sterk vekst. *Politidirektoratet* mener det vil medføre en kostnadseksplosjon som ikke har noen som helst sammenheng med en eventuell økning i antall henvendelser fra politiet. Dagens ordning som innebærer forhandlinger med hver enkelt tilbyder oppleves dessuten som svært ressurskrevende for begge parter. *Politidirektoratet* vil bemerke at også tilbyderne av ekomnett- og tjenester har et samfunnsansvar på lik linje med finansnæringen som er rapporteringspliktige gjennom hvitvaskingsregelverket, og bærer alle kostnadene for dette selv (Gjengedal 2010). Fremfor å diskutere hvilken nytte ekomtilbyderne selv har av datalagringen fremhever aktørene innenfor samfunnsansvarsdiskursen isteden et iboende samfunnsansvar rundt datalagring. Aktørene innenfor denne diskursen mener det derfor ligger et betydelig økonomisk ansvar på ekomtilbyderne på lik linje med hvordan finansnæringen er rapporteringspliktige.

Realiseringsdiskursen

I følge *Hewlett-packard* er de det ledende selskapet i EU på implementering og realisering av datalagringsdirektivet. Hewlett Packard betrakter dette som et strategisk satsningsområde og har levert løsninger til over 50% av markedet i EU der direktivet er innført. Innføring av direktivet kan i følge *Hewlett-Packard* medføre flere skjevheter med hensyn til konkurranse i et åpent marked. *Hewlett-Packard* mener det blir viktig å ta hensyn til små og mellomstore aktører som må forholde seg til regelverket for lagring og uthenting av data fordi kravene som stilles til sikkerhet vil bli en finansiell utfordring for disse bedriftene. *Hewlett-Packard* legger derfor til en rekke forslag i sin høringsuttalelse for hvordan problemet kan løses gjennom blant annet et felles datautvekslingspunkt eller en organisasjon. Videre mener *Hewlett-Packard* en felles søkerportal for politiet mellom de ulike teleaktørene bør legges inn som et krav fra myndighetene. Små og mellomstore bedrifter bør i følge Hewlett Packard gå for

standardiserte løsninger gjennom for eksempel felles lagringsløsninger eller at de får en Turn-Key pakke som innfrir alle kravene som myndighetene stiller.

Hewlett-Packards vurderinger i forhold til markedsposisjon på telemarkedet er at omtrent 80% av lagrede data vil bli administrert av to teleoperatører. I prinsippet gir dette i følge Hewlett Packard en tilnærmet sentral løsning. *Hewlett-Packard* legger til at i EU-landene hvor direktivet er innført er det ingen av teleoperatørene som har tatt ansvar for å lagre data for sine MVNOs(virtuelle nettverksoperatører). Dette vil i følge *Hewlett-Packard* sannsynligvis være tilfellet i Norge også, noe som vil gi en klar kostnadsvridning i favør av de store aktørene. Myndighetene bør i følge *Hewlett-Packard* komme frem til løsninger som er basert på å levere datalagring som en tjeneste og dermed unngå invisteringskostnader for Ekom-tilbyderne (Roald 2010).

Realiseringsdiskursen fremhever potensielle skjevheter som kan forekomme med hensyn til konkurransen i det åpne markedet. Hewlett-packard fremhever at en felles løsning er viktig for å forminske kostnadsvridninger som favoriserer de store aktørene.

Konkurransevridningsdiskursen

Telenor mener det vil være uheldig dersom direktivet vil skape usikkerhet i markedet om hvilke tilbydere som omfattes av lagringsplikten. Om IP-baserte tjenester som Skype ikke nødvendigvis er inkludert mener *Telenor* at direktivet ikke er konkurransenøytralt. *Telenor* nevner at konkurransen i økende grad foregår på et internasjonalt marked (peer-to-peer tjenester, webbaserte epost-tjenester, brebåndstelefoni og andre tjenester som vedlikeholdes i utlandet). Det er derfor viktig for *Telenor* at Norge ikke velger en svært streng og detaljert implementering av direktivet fordi omfanget uansett vil være veldig stort. Om norske myndigheter samtidig går inn for en løsning som gjør at enkelte tjenestetilbydere ikke blir inkludert påpeker *telenor* at det vil føre til en konkurransevridning. *Telenor* ønsker at deres ressurser i størst mulig grad er forretningsmessig begrunnet (Krogh 2010).

Altibox AS mener direktivet må spesifiseres for å unngå konkurransevridninger som hemmer innovasjon og næringsutvikling i IKT-bransjen (Ims 2010). *Get AS* er på sin sidet opptatt av at direktivet ikke implementeres med store omgåelsesmuligheter som fører til en

konkurransevridning mellom tilbydere som omfattes av direktivet og de som faller utenfor. De påpeker også at direktivet vil slå ulikt ut for de som allerede har adekvate systemer på plass og de som må gjøre mer for å tilpasse seg (Myksvoll 2010). *TDC* mener direktivet kan medføre en etableringsbarriere for mindre selskaper (Johansen 2010). Om kostnadene blir pålagt tilbyderne vil mindre tilbydere i følge *Tele2* ønske å begrense kostnaden og *Tele2* påpeker derfor at sikkerhet og kvalitet må prioriteres for å sikre like konkurransevilkår mellom de store og små tilbyderne. *Tele2* mener også det ved en eventuell implementering er behov for en europeisk harmonisering. *Tele2* påpeker at medlemstater stilles fritt med hensyn til lagringstid, økonomisk kompensasjon og hva som skal anses som alvorlig kriminalitet (Jensen 2010). *NetCom* kan ikke se at EU har lyktes med en harmonisering og likhet over landegrensene i forbindelse med datalagringsdirektivet (Punsvik 2010).

Aktørene innenfor konkurransevridningsdiskursen frykter en rekke ulike konkurransevridninger dersom ikke alle aktørene innenfor markedet (nasjonalt og internasjonalt) har like betingelser for sin virksomhet på grunn av ulike tolkninger rundt hvordan datalagringen skal gjennomføres og hvem som plikter seg til å lagre dataene.

Kundetillitsdiskursen

Telenor ønsker ikke å lagre mer informasjon om kundenes data- og telefonbruk enn det som er nødvendig av det de mener er en nødvendig og grunnlegende respekt for en kontraktspart. De mener det er en forutsetning for tilbyder å ha tillit hos kundene sine. *Telenor* mener det går et skarpt skille mellom å lagre informasjon for å kunne levere og fakturere de tjenestene kundene benytter og det å bli pålagt å samle inn og lagre informasjon som utelukkende skal benyttes til andre formål. Det bør derfor i følge telenor heller sees etter alternativer innenfor dagens regelverk (Krogh 2010).

Get AS er også opptatt av å ivareta kundenes personvernsinteresser og å gi kundene trygghet om at et kundeforhold med Get AS ikke medfører inngrep i kundenes individuelle integritet (Myksvoll 2010). Det må i følge *Netcom* være en overordnet samfunnsinteresse å ikke motvirke effektiv kommunikasjon (Punsvik 2010).

Aktørene innenfor kundetillitsdiskursen kobler seg i noen grad til overvåkningsdiskursen. Datalagringsdirektivet oppfattes som et forstyrrende element i tillitsforholdet mellom

ekomtilbyder og kundene fordi det ikke lar seg kombinere med å beskytte kundens personvern. Det er viktig for disse aktørene at kundene føler seg trygge på at deres personvern blir ivaretatt.

Opphavsrettdiskursen

Norsk Videogramforening legger seg på linje med rettighetsinnehavere innenfor musikk og mener deres medlemmeer itillegg til andre rettighetshavere innen film blir rammet av omfattende distribusjon av spillefilm og TV-serier på internett uten deres samtykke. *Norsk videogramforening* og deres medlemmer forteller derfor i sin høringsuttalelse at de har brukt betydelige ressurser de senere årene for å stanse den omfattende ulovlige distribusjonen av deres verker og arbeider, og har i den forbindelse samarbeidet med IFPI Norge (Dye 2010).

"*Selv om krenkeren har handlet i god tro, kan rettighetshaver uansett skadens størrelse kreve utbetalt nettofortjenesten ved den ulovlige handling*" (Dye 2010:3).

Norsk videogramforening referer til denne konsesjonen fra datatilsynet og mener den gir grunnlag for å kunne dokumentere konkrete rettighetskrenkelser i den grad det er nødvendig for å kunne rette en henvendelse til og et krav mot krenkeren, eventuelt politianmelde forholdet eller gå til sivilrettslige skritt. *Norsk videogramforening* mener alt arbeidet for å stanse de omfattende rettighetskrenkelsene har til felles at de er avhengig av at sluttbruker kan identifiseres. Dersom sluttbruker og den ansvarlige for krenkelsen ikke kan identifiseres vil dokumentasjon av konkrete rettighetskrenkelser i henhold til konsesjonen fra datatilsynet i følge *norsk videogramforening* være nær formålsløst. *Norsk videogramforening* mener også at en politianmeldelse vil være formålsløs om politiet og påtalemyndighetene er uten mulighet til å identifisere den ansvarlige. Manglende muligheter for å samle inn informasjon om sluttbrukeren gir i følge *norsk videogramforening* en følelse av rettsløshet og et amnesti for alle straffbare forhold og sivilrettslige krenkelser som faller utenfor den foreslåtte implementeringen av datalagringsdirektivet. I følge *norsk videogramforening* er det behov for lagring av og tilgang til koblingen mellom sluttbrukernes identitet og IP-adressenes sluttbrukeren har fått tildelt og mener risikofaktorene for personvern knyttet til slik lagring og tilgang, tilsier at det, uavhengig av en eventuell implementering av datalagringsdirektivet bør innføres en plikt for internetttilbyderne til å lagre denne koblingen. *Norsk videogramforening*

legger seg på linje med Svein Willassen om at loggen over ip-adresser sier svært lite om bruksmønstret til abonnentent (Dye 2010).

Aktørene innenfor opphavsrettsdiskursen fremhever at datalagring er det eneste virkemidlet politiet har til å etterforske og opprettholde deres interesser. Lagring av trafikkdata oppfattes som essensielt for å få en stopp på krenkelser av opphavsretten.

EØS diskursen

Samfunnsgruppen demos mener direktivet kun er formulert mot det indre markedet for å kunne innlemmes i EØS-avtalen. De argumenterer for at løsningen som velges og kostnadene som følger med vil være opp til hvert enkelt land og operatør. Det vil derfor i følge *samfunnsgruppen demos* uansett bli ujevne konkurranseforhold uavhengig av om direktivet innføres eller ikke. Demos legger videre vekt på at direktivets formål om å bekjempe kriminalitet ikke har noe med det indre markedet å gjøre og anser det derfor som legitimt å ta i bruk reservasjonsretten. *Samfunnsgruppen demos* mener Norge som en suveren stat ikke må la seg presse av EU og være redd for å stå utenfor på bakgrunn av skremselspropaganda som tilsier at vi vil bli en frihavn for kriminelle. I forhold til internasjonale konsekvenser mener *Samfunnsgruppen demos* at Norge må gjøre en utredning for argumenter og alternative løsninger. Noe de finner mangelfullt i høringsnotatet (Finneid 2010). LO referer også til påpekningene til Finn Arnesen og Fredrik Sejerstad om direktivets EØS-relevans som peker mot at det ikke er det og mener det mangler en grundigere drøfting av muligheten for å reservere seg mot direktivet i høringsnotatet (Solbakken 2010).

Forpliktelser vi har til EF-traktatens artikkel 95

Næringslivets hovedorganisasjon referer til EU-domstolen i februar 2009 der det ble slått fast at hjemmelsgrunnlaget for datalagringsdirektivet er EF-traktatens artikkel 95. *Næringslivets handelsorganisasjon* mener denne artikkelen gjør datalagringsdirektivet til et markedsdirektiv og som et indre markedsinstrument er direktivet EØS-relevant og implementeringspliktig for Norge. *Næringslivets hovedorganisasjon* legger seg på en linje der forholdene legges til rette for en balanse mellom effektiv bekjempelse av kriminalitet og personvernsinteressen, samtidig som næringslivets interesser i et effektivt indre marked med like konkurransevilkår

ivaretas. Det betyr blant annet for *næringslivets hovedorganisasjon* at staten dekker kostnadene og at det blir strenge krav for hvem som skal ha tilgang til dataene (Bernander 2010).

Oppsummering og analyse av hovedfunn

Diskursene rundt datalagringsdirektivet har involvert mange aktører med ulike ideologiske bakgrunner og tilnærminger. Jeg har identifisert tre hoveddiskurser som skiller aktørenes ideologiske utgangspunkt. Under disse har jeg videre identifisert underdiskurser og hvilke relasjoner de har til de andre diskursene.

Overvåkningsdiskursen er en av hoveddiskursene hvor ideologiske motstandere av direktivet befinner seg. Aktørene innenfor overvåkningsdiskursen anser datalagring som en form for overvåkning som truer personvernet. Datalagringsdirektivet blir ikke vurdert som et enkeltstående tiltak, men anses å være en del av et større nettverk av nye og gamle overvåkningssystemer som er ment å skape sosial kontroll. Samfunnet oppleves som tilrettelagt for slike systemer på grunn av tilliten befolkningen har til myndighetene og mangfoldet av informasjon vi etterlater oss i form av elektroniske spor. Denne tilliten blir ikke avvist som grunnløs, men det fremheves heller en frykt for at demokratiet ikke vil stå like sterkt i fremtiden. Store deler av kritikken mot datalagringsdirektivet baserer seg på potensialet det har for å akkumelere informasjon om alle borgerne og hvordan denne informasjonen kan misbrukes. Når informasjonen først er samlet inn frykter aktørene innenfor overvåkningsdiskursen at misbruk er uunngåelig i det lange løp. Idealet for aktørene innenfor overvåkningsdiskursen er et samfunn som baserer seg på tillit til befolkningen der politi- og påtalemyndighet må ha konkrete mistanker rundt kriminelle handlinger før informasjon kan samles inn om individet.

Kildevernsdiskursen er en av underdiskursene til overvåkningsdiskursen. Aktørnene innenfor denne diskursen opplever direktivet som en trussel mot en sentral verdi for journalistisk etikk. Muligheten til å holde identiteten til informantene skjult fremheves som sentralt for at journalister skal ha muligheten til å utføre kritisk journalistikk. Aktørene mener direktivet vil gjøre det vanskeligere for potensielle informanter å stå frem. Det er en frykt for at myndighetene vil misbruke databasen for å spore opp informanter som uttaler seg kritisk til

myndighetene, men også en frykt for at andre aktører som er under lupen vil hacke seg inn i direktivet for å avsløre hvem som lekker informasjon om for eksempel bedriften.

Personvernsdiskursen samsvarer i stor grad med overvåkningsdiskursen. Personvernet til allmenheten oppfattes som truet av datalagringsdirektivet gjennom hemningene det kan ha for frimodighet og faren for en formålsutglidning. Hemningene rundt frimodigheten henger sammen med overvåkningspotensialet. Aktørene tror direktivet kan medføre en 'chilling effect' på befolkningen fordi de føler seg sett og registrert. Denne tolkningen av datalagringsdirektivet er sammenlignbar med konsekvensen av virtuelle panoptikon som Hannemyr (2002) beskriver som selvdisiplinerende. Frykten for å være overvåket overskygger her muligheten for at du ikke er det. *Utglidningsdiskursen* fokuserer på det som oppfattes som et umettelig informasjonsbehov for politi- og påtalemyndighetene og hvordan flere aktører etterhvert vil søke om retten til innsyn. Gjennom *rettsprinsippdiskursen* gir aktørene uttrykk for at datalagringsdirektivet representerer et brudd med gjeldende rettsprinsipper og menneskerettigheter. Fra å være en reaksjonær strafferett oppleves datalagringsdirektivet som en endring over til en preaktiv strafferett. Uskyldspresumpsjonen som tilsier at du er uskyldig inntil det motsatte er bevist oppfattes som snudd på hodet til fordel for at alle er under konstant oppsyn.

Nytteverdien til direktivet blir dessuten sådd tvil om fordi direktivet oppleves som enkelt å omgå for de som går inn for det. Omgåelsesdiskursen påpeker flere svakheter rundt direktivets innsamlingsmetode. Mulighetene for å være anonym selv med et implementert direktiv anses imidlertid som en midlertidlig glede. Aktørene frykter hullene i datalagringsdirektivet vil gjøre det mer omfattende etterhvert og stiller seg derfor i utgangspunktet skeptisk til å la politi- og påtalemyndighetens behov overskygge de potensielle farene de ser for seg direktivet vil plante i samfunnet.

Det oppstår to interessante aktørkonstillasjoner under nytteverdidiskursene. Den første av de to er barns beste-diskursen hvor blant annet *redd barna* og *barneombudet* fremhever at barns personvern også er truet av direktivet. Et av hovedformålene med datalagringsdirektivet er å bekjempe overgrep mot barn som skjer over internett. Aktørene innenfor barns beste-diskursen er imidlertid ikke overbevist om at datalagringsdirektivet er det riktige verktøyet for politiets arbeid med å stoppe denne formen for overgrep. Barns beste-diskursen stiller seg likevel åpen for at en dokumentert effektivitet i andre land som har innført direktivet kan endre deres oppfatning rundt direktivets nytteverdi. Dokumentasjonsdiskursen inneholder for

øvrig samsvarende oppfatninger rundt direktivet. En av de mest interessante aktørene innenfor denne diskursen er Nav. Nav innehar et omfattende register av klienter, men stiller seg likevel kritisk til at politiet kan få tilgang til trafikkdata som kan spore seg frem til hvem de kommuniserer med. Det påpekes at mye av den informasjonen Nav besitter er taushetsbelagt og det oppleves som uheldig viss politi- og påtalemyndigheter kan skaffe seg tilgang til disse opplysningene.

Den andre hoveddiskursen jeg identifiserer i denne oppgaven er ***etterforskningsdiskursen***. Aktørene innenfor denne diskursen kan anses som ideologiske tilhengere av direktivet. Den største skillelinjen mellom etterforskningsdiskursen og overvåkningsdiskursen er den smale tilnærmingen til datalagringsdirektivet. Der hvor overvåkningsdiskursen tenderer mot vide tolkninger av potensialet rundt direktivet er aktørene innenfor etterforskningsdiskursen mer konkrete rundt hva direktivet innebærer for dem. Siden de største advokatene for implementering av datalagringsdirektivet befinner seg innenfor politi- og påtalemyndighetene er ikke denne tilnærmingen uforventet. Trafikkdata har blitt brukt i etterforskning i lengre tid og dette blir i stor grad fremhevet av aktørene innenfor etterforskningsdiskursen. Trafikkdata blir gjerne omdøpt til 'tause vitner' og beskrives som et objektivt bevismateriale som er essensielt for etterforskningen av moderne kriminalitet som tar i bruk ulike former for elektronisk kommunikasjon. Aktørene innenfor etterforskningsdiskursen er uenig i fremstillingen av datalagring som overvåkning og mener det heller er snakk om en utsatt slette-plikt. *Utsatt sletteplikts*diskursen er en av underdiskursene til overvåkningsdiskursen og fremhever at ubehaget borgere måtte føle ved å vite at noen besitter informasjon om deres aktivitet er en teoretisk trussel som må vike for den reelle trusselen kriminelle aktører poserer mot samfunnet.

Sikkerhetsdiskursen svarer på mye av den kritikken som kommer under personvernsdiskursen, men fremhever også en beskrivelse av et robust datalagringsdirektivet. *Krypteringsdiskursen* fremhever hvordan trafikkdataene som lagres kan beskyttes mot uvelkommende inntrengere. Så lenge politiet er de eneste med den rette sikkerhetsnøkkelen for å gjøre dataene lesbare mener aktørene innenfor denne diskursen at dataene er trygge. Risikoen som kobles direkte til direktivet videreføres dermed til tilnærmingen for implementering. Så lenge fokuset er på å finne sikre løsninger anses trusselen mot personvernet som minimal. *Offerdiskursen* tar fokuset vekk fra personvernet til allmenheten og fokuserer på personvernet til ofrene. Alle kan bli et offer for kriminelle handlinger og det er politi- og påtalemyndighetens oppgave å forhindre at dette skjer. Datalagringsdirektivet fremheves som en vesentlig faktor for å kunne

beskytte individers integritet mot overgrep. *Anonymitetsdiskursen* gir en ny vri på det som problematiseres under omgåelsesdiskursen samtidig som frimodighetsdiskursen kritiseres. Først og fremst fremhever aktørene innenfor anonymitetsdiskursen at datalagringsdirektivet representerer et vesentlig liten andel av de personlige dataene vi etterlater oss i dag. Noe som gir aktørene innenfor denne diskursen grunnlag for å mene at befolkningen ikke anser slike opplysninger som veldige personlige og sensitive. Potensialet for frimodighet regnes heller som økt med tanke på de gode mulighetene for nettanonymitet.

Tilhengere med forbehold om strenge krav til sikkerheten rundt datalagringsdirektivet er en spesielt interessant gruppe aktører innenfor sikkerhetsdiskursen. Aktørene innenfor denne gruppen vektlegger det som problematiseres under personvernsdiskursen i mye større grad enn de andre tilhengerne for datalagringsdirektivet. En av de mer interessante aktørene som befinner seg innenfor denne gruppen er politiets sikkerhetstjeneste. I motsetning til mange av de som kan regnes å stå politiets sikkerhetstjeneste nærmest ideologisk stiller de seg fullt bak høringsnotatets forslag om at all form for tilgang og bruk av de lagrede dataene må godkjennes av en domstol. Det er verdt å påpeke at de i samme høringsnotat argumenter for politiets behov for hastekompetanse. Så skillet er ikke stort mellom politiets sikkerhetstjeneste og de andre aktørene innenfor politi- og påtalemyndighetene. Det er likevel verdt å merke seg at de stiller seg i mye større grad bak en strengere tilgang enn de andre aktørene innenfor etterforskningsdiskursen. Innenfor *behovsdiskursen* fremheves datalagrinsdirektivets nytteverdi i forhold til etterforskningsdiskursen. Datalagringsdirektivet påpekes som den eneste muligheten politi- og påtalemyndighetene vil ha i fremtiden for å kunne bekjempe organisert kriminalitet og terrorisme. Aktørene innenfor denne diskursen mener det ikke finnes alternative etterforskningsmetoder som kan erstatte trafikkdata. Aktørene ser for seg at kostnadsmodellen til ekomtilbyderne etterhvert vil endre seg til faste priser og mener det vil medføre at behovet for å lagre trafikkdata for faktureringsformål forsvinner. Implementering av datalagringsdirektivet vil imidlertid sikre tilgangen til disse opplysningene også i fremtiden. Risikodiskursen er kanskje den videste diskursen som kan kobles til etterforskningsdiskursen. Først og fremst problematiserer den innskjerpingene høringsnotatet legger opp til i forhold til politi- og påtalemyndighetens rett til innsyn i dag. Det fremstår som ulogisk at gjerningsmenn må identifiseres på forskudd før trafikkdataene kan innhentes fremfor dagens ordning som tilsier at det bare må være en konkret mistanke. Aktørene påpeker at bristen her oppstår når politiet har behov for å identifisere ukjente gjerningsmenn og ikke kan ta i bruk et søk i de mistenktes trafikkdata for å finne ut hvor de for eksempel

befant seg når lovbruddet tok sted. Aktørene mener politiet her risikerer å miste et viktig hjelpemiddel for å spore opp kriminelle. For det andre problematiseres aktørene en tilværelse der de ikke har fått implementert datalagringsdirektivet gjennom å påpeke at Norge risikerer å bli et fristed for kriminelle og uten mulighet til å effektivt samarbeide med politi- og påtalemyndighetene innenfor EU.

En aktør som stikker seg ut blant politi- og påtalemyndighetene er Oslo statsadvokatembeter som stiller seg kritisk til behovsdiskursen. Det påpekes at trafikkdata ikke er politi- og påtalemyndighetenes eneste ressurs for å fange inn kriminelle, men heller inngår som en del av en langt mer omfattende beviskjede.

Den tredje hoveddiskursen som identifiseres rundt datalagringsdirektivet er ***økonomidiskursen***. Her endres fokuset i stor grad vekk fra de oppfatningene vi finner under overvåkningsdiskursen og etterforskningsdiskursen og over til de økonomiske aspektene rundt datalagringsdirektivet. *Kostnadsdiskursen* er en av underdiskursene som problematiserer kostnadene forbundet med direktivet. Aktørene (i all hovedsak ekomtilbyderne) fremhever her de store kostnadene som henger sammen med etablering og vedlikehold av et omfattende lagringssystem som datalagringsdirektivet vil kreve. Datalagringsdirektivet innebærer for disse aktørene en unødvendig utgiftspost for å lage informasjon de ikke kan eller har behov for å benytte seg av. *Samfunnsansvarsdiskursen* svarer på denne kritikken med å fremheve at ekomtilbydere bærer et samfunnsansvar på lik linje med finansnæringen og bør ta store deler av kostnadene selv. Aktørene under denne diskursen utviser samtidig en usikkerhet rundt hvem som egentlig er ment å finansiere direktivet og fremhever at kostnadene for politi- og påtalemyndighetene kan bli for store dersom ikke ekomtilbyderne selv tar på seg en del av kostnadene. *Realiseringsdiskursen* er imidlertid klar på at staten er nødt til å bidra for å unngå kostnadsvridninger som blir særdeles ufordelaktige for minde aktører. Aktørene innefor *konkurransevridningsdiskursen* tilføyer flere bekymringer rundt potensielle vridninger som datalagringsdirektivet kan bringe med seg. Usikkerheten rundt hvilke tilbydere som har lagringsplikt skaper bekymringer angående om noen kommer til å slippe unna. Samtidig trekker aktørene innenfor denne diskursen frem en rekke eksempler på alternativer som allerede eksisterer som foreløpig ikke er inkludert i planene rundt datalagringsdirektivet. Aktørene påpeker at konkurransen er blitt internasjonal og nevner brebåndstelefoni, peer-to-peer tjenester, webbaserte epost-tjenester og lignende tjenester som vedlikeholdes i andre land. Aktørene mener konkurransen i markedet vil bli ufordelaktig for dem dersom lovverket ikke legger opp til slike tjenester også er lagringspliktige. Aktørene frykter samtidig at de kan

komme til å miste kunder basert på krenkelsen av tilliten mellom kunde og tilbyder datalagringen innebærer. Aktørene innenfor *kundetillitsdiskursen* kan til en viss grad kobles til overvåkningsdiskursen på dette punktet, men det er de økonomiske problemene som står i fokus.

Opphavsrettdiskursen legger seg på linje med etterforskningsdiskursen og påpeker at datalagringsdirektivet er essensielt for å beskytte deres økonomiske invisteringer fra å bli stjelt og delt gjennom elektronisk kommunikasjon. Aktørene innenfor denne diskursen ønsker lagring av trafikkdata for sporing av de som krenker opphavsretten uavhengig av om direktivet blir innført eller ikke. Aktørene mener det er umulig å opprettholde dagens lovverk uten muligheter for å spore opp de som krenker opphavsretten.

EØS-diskursen er en samling av aktører med ulike perspektiver på Norges forhold til datalagringsdirektivet og EØS-avtalen. Aktører innenfor overvåkningsdiskursen mener vi burde bruke reservasjonsretten på datalagringsdirektivet eller ihvertfall undersøke mulighetene for det siden det oppfattes som urelevant for det indre marked. Aktører innenfor etterforskningsdiskursen er imidlertid klar på at datalagringsdirektivet er EØS-relevant gjennom EF-traktatens artikkel 95 som tilsier at datalagringsdirektivet er et markedsdirektiv. På bakgrunn av de konkurransevridningene det kan ha for andre EØS- og EU land blir direktivet ansett som relevant for det indre markedet.

Konklusjon

Det er flere diskurser som settes i spill rundt datalagringsdirektivet. I diskurskartet (vedlegg 1) har jeg prøvd å lage en oversikt over hvordan disse diskursene samsvarer eller delvis samsvarer med hverandre. Hvordan andre diskurser er i direkte konflikt. Jeg har delt hoveddiskursene opp i flere underdiskurser for å kunne gå dypere inn i diskursene. Som forventet fant jeg både ideologiske motstandere og tilhengere av direktivet, men det var også en del diskurser som ikke fulgte denne oppskriften. Økonomidiskursen handlet i liten grad om overvåkning og etterforskning, men rettet store deler av fokuset mot kostnader og konkurransevridninger. Det var underdiskurser rundt økonomidiskursen som delvis samsvarte med både overvåkningsdiskursen og etterforskningsdiskursen, men det ideologiske grunnlaget for å være for eller i mot implementering var ikke det samme. Det diskursive landskapet var

ikke bare preget av klarhet heller. På begge sider var det aktører som uttrykte at det var vanskelig å vurdere personvernet opp mot etterforskningsbehovet. Innenfor dokumentasjonsdiskursen var det for eksempel mer åpenhet for å støtte datalagringsdirektivet dersom det kunne dokumenteres en positiv effekt i andre land som hadde innført direktivet før oss.

Aktører som overrasket meg spesielt var Oslo statsadvokatembeter, redd barna og barneombudet. Til dels også politiets sikkerhetstjeneste for sin uforventede støtte til strenge krav rundt datalagringsdirektivet, der flertallet av politi- og påtalmyndighetene hadde uttalt seg kritisk til innskrenking av dagens rettigheter. Kritikken Oslo statsadvokatembeter uttrykte mot behovsdiskursen var likevel det som overrasket meg mest.

Direktivet ble godkjent i stortinget 4. mars 2011. I forhold til konseptet rundt avslutning og stabilisering er det nok for tidlig å si noe om direktivets fremtid. Det vil muligens være interessant i forhold til fremtidig forskning å undersøke hvilke artifakter/diskurser som fremdeles eksisterer rundt direktivet når det eventuelt har stabilisert seg.

Litteraturliste

Bijker, Wiebe E. (1997) "*King of the road: The Social Construction of the Safety Bicycle*" The MIT Press

Bijker, Wiebe E. (2009) "*A Companion to the Philosophy of Technology: Chapter 15. Social Construction of Technology*" Blackwell Publishing LTD

Devereux, Eoin (2007) "*Media studies: Key issues & debates*" SAGE publications Ltd

Neumann, Iver B. (2000) "*Diskursens Materialitet*" Dansk Sociologi

NOU (2006) "*Økonomisk utredning av konsekvensene knyttet til innføring av EUs Datalagringsdirektiv*" hentet fra http://www.regjeringen.no/pages/2281081/oekonomisk_analyse_2006.pdf den 17.05.11

NOU (2008) "*Økonomisk utredning av konsekvensene knyttet til innføring av EUs Datalagringsdirektiv*" hentet fra http://www.regjeringen.no/pages/2281081/SD_Datalagring_oekonomisk_analyse_v1.0.pdf den 17.05.11

NOU[1] (2010) "*Høringsnotat: Datalagringsdirektivet*" hentet fra http://www.regjeringen.no/pages/2281081/hnotat_datalagring.pdf den 17.05.11

NOU[2] (2010) "*Utdypning av økonomisk analyse knyttet til konsekvensene ved innføring av EUs Datalagringsdirektiv*" hentet fra http://www.regjeringen.no/Upload/SD/Vedlegg/Telekommunikasjon/teleplan_utdyping.pdf den 17.05.11

NOU[3] (2010) "*Feil om datalagringsdirektivet*" hentet fra http://www.regjeringen.no/nb/dep/fd/aktuelt/nyheter/2010/upresist-om-datalagringshoring.html?id=627744 den 17.05.11

NOU[1] (2011) "*Endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett)*" hentet fra http://www.regjeringen.no/nb/dep/jd/dok/regpubl/prop/2010-2011/prop-49-l-20102011/1/2.html?id=627830 den 17.05.11

NOU[2] (2011) "*Viktig verktøy for å bekjempe alvorlig kriminalitet*" hentet fra http://www.regjeringen.no/nb/dep/jd/pressesenter/pressemeldinger/2011/viktig-verktoy-for-a-bekjempe-alvorlig-k.html?id=641018 den 17.05.11

van Dijk, Teun A. (1995) "*Discourse & Society vol.6(2) 243-289: "Discourse semantics and ideology*" SAGE

Artikler

AP (2010) "*DLD: Viktig for å bekjempe kriminalitet*" hentet fra http://arbeiderpartiet.no/Aktuelt/Nyhetsarkiv/Kriminalitet/DLD-Viktig-for-aa-bekjempe-kriminalitet den 16.06.11

Blaker, Magnus (2010) "*Data om deg vil komme på avveie*" hentet fra http://www.nettavisen.no/it/article2939199.ece den 10.07.10

Bryne, Snorre (2009) "*Dette er den mest spennende politiske saken de neste fire årene*" hentet fra http://www.dagbladet.no/2009/11/03/kultur/tekno/datalagringsdirektivet/personvern/data_og_teknologi/8863965/ den 03.11.09

Egeberg, Kristoffer (2010) "*Forsvaret frykter at spioner og terrorister kan utnytte datalagringsdirektivet*" hentet fra http://www.dagbladet.no/2010/04/15/nyheter/dld/datalagringsdirektivet/personvern/tekno/11295851/ den 15.04.10

Eltvik, Anders (2009) "*Ap feilinformerer om datalagring*" hentet fra http://www.nationen.no/eu_wto/article4695176.ece den 10.11.09

Flydal, Eiliv Frich (2009) "*Frykter Norge blir frihavn for pedofile og kriminelle*" hentet fra http://www.dagbladet.no/2009/11/04/kultur/datalagringsdirektivet/personvern/tekno/data_og_teknologi/8876163/ den 04.11.09

Færaas, Arild (2011) "*Politikere hetses og trues etter datalagrings-ja*" hentet fra http://www.vg.no/nyheter/innenriks/norsk-politikk/artikkel.php?artid=10091764 den 06.04.11

Glomnes, Lars Moltenberg (2009) "*Kritiserer Helgas udokumenterte påstander*" hentet fra http://www.dagbladet.no/2009/11/05/nyheter/datalagringsdirektivet/arbeiderpartiet/innenriks/politikk/8893531/ den 05.11.09

Johansen, Marianne, Alf Bjarne Johnsen & Morten Hopperstad (2010) "*Hysjen beordret på kildejakt etter VG-avsløring*" hentet fra http://www.vg.no/nyheter/innenriks/artikkel.php?artid=501063 den 12.04.10

Jørgensen, Marius (2010) " - *Neste skritt etter datalagring*" hentet fra http://www.digi.no/834169/neste-skritt-etter-datalagring den 16.06.11

Kvistad, Øystein (2000) "*Amazon.com vil selge kundedata*" hentet fra http://www.digi.no/45795/amazoncom-vil-selge-kundedata den 17.05.11

NTB[1] (2009) "*Utsetter datalagringsdiretkivet i ett år*" hentet fra http://www.vg.no/teknologi/artikkel.php?artid=582591 den 04.11.09

NTB[2] (2009) "*Støre lover høringsforslag om datalagring før jul*" hentet fra http://www.vg.no/teknologi/artikkel.php?artid=582634. den 04.11.09

NTB (2010) "*Krf og Frp positive til personvernskompromiss*" hentet fra http://www.dagbladet.no/2010/06/18/nyheter/personvern/innenriks/politikk/12187803/ den 18.06.2010

NTB[1] (2011) "*Stortinget sa ja til datalagring*" hentet fra http://www.dagbladet.no/2011/04/04/kultur/datalagringsdirektivet/personvern/data_og_teknologi/politikk/16072501/ den 04.04.2011

NTB[2] (2011) "*EU-kommisjonen foreslår endringer i DLD*" hentet fra http://www.dagbladet.no/2011/04/18/nyheter/politikk/dld/datalagringsdirektivet/data_og_teknologi/16238256/ den 17.05.11

NTB[3] (2011) "*Norge mer utsatt for terror uten lagring*" hentet fra http://www.nrk.no/nyheter/norge/1.7496478 den 16.06.11

Olsen, Pål Joakim (2008) "Se hva google har lagret om deg" hentet fra http://m.dinside.no/php/art.php?id=798306 den 17.05.11

Omdahl, Jan[1] (2009) "*Høyre kan stanse datalagringsdirektivet*" hentet fra http://www.dagbladet.no/2009/11/03/kultur/tekno/data_og_teknologi/datalagringsdirektivet/personvern/8854795/ den 03.11.2009

Omdahl, Jan[2] (2009) "*Europeisk overvåkningskode*" hentet fra http://www.dagbladet.no/2009/10/19/kultur/teknologi/datalagring/8641638/ den 19.10.09

Simonsen, Marie (2009) "*Storberget leter etter nål i din høystakk*" hentet fra http://www.dagbladet.no/2009/11/04/kultur/meninger/tekno/datalagringsdirektivet/8874922/ den 04.11.09

Unanue-Zahl, Pål (2009) "*Protestaksjon mot datalagringsdirektivet*" hentet fra http://www.vg.no/teknologi/artikkel.php?artid=582526 den 03.11.09

Washington Times (2009) "Iran's Twitter revolution" hentet fra http://www.washingtontimes.com/news/2009/jun/16/irans-twitter-revolution/ den 20.06.11

Wessel-Aas, Jon (2010) "Alle borgere under mistanke" hentet fra http://www.dagbladet.no/2010/05/15/kultur/debatt/kronikk/datalagringsdirektivet/personvern/11698938/ den 15.05.10

Høringsuttalelser

Aarbakke, Knut (2010) "*Akademikernes høringssvar til implementering av datalagringsdirektivet*" Akademikerne

Aasen, Olav (2010) "*Høring om datalagring*" Domstoladministrasjonen

Ada Sofie Austegard & Jensen, Mari (2010) "*Høring - datalagring*" Stine Sofies Stiftelse

Andreassen, Camilla Forgaard & Sissel Monsvold (2010) "*Høring om datalagring*" HSH - 5 Hovedorganisasjonen for handel og tjenester i Norge

Apenes, Georg (2010) "*Høringsuttalelse - implementering av datalagringsdirektivet (2006/24/EC)*" Datatilsynet

Augland, Anne Karin (2010) "*Høringsuttalelse: Implementering av datalagringsdirektivet*" Norges Televisjon

Aulie, Nina & Tor Saglie (2010) "*NAV svar på høringsnotat for Datalagringsdirektivet*" NAV - Arbeids- og Inkluderingsdepartementet

Aust-Agder Nei til EU (2010) "*EU's datalagringsdirektiv - Høringsuttalelse*" Aust-Agder Nei til EU

Bernander, John G. (2010) "*Høringsuttalelse - datalagringsdirektivet*" NHO - Næringslivets Hovedorganisasjon

Bingen, Unni & Christian Nordbye (2010) "*Høringsuttalelse på datalagringsdirektivet*" Nei til EU Akershus

Bjerke, Hallstein & Torgeir Waterhouse (2010) "*Høring - datalagring*" IKT Norge

Bjørke, Synnøve (2010) "*Vedrørende høring Datalagringsdirektivet*" Stiftelsen elektronikkbransjen

Borgen, Marianne, Marianne Hagen & Kaja Hegg (2010) "*Høring om EUs datalagringsdirektiv*" Redd Barna

Brodal, Marit (2010) "*Høring - Datalagring*" Ventelo AS

Brenna, Anders (2010) "*Høringsuttalelse om datalagringsdirektivet*" Anders Brenna

Bucholdt, karl M. (2010) "*Høring om datalagring - Høringsuttalelse fra Levanger Venstre*" Levanger Venstre

Bunæs, Eirik & Tore Lindstad (2010) "*Høring om datalagring*" Det kongelige Finansdepartement

Bunæs, Eirik & Geir Holen (2010) "*Finanstilsynets høringsuttalelse om datalagring*" Finanstilsynet

Busch, Tor-Aksel (2010) "*Datalagringsdirektivet - Høringsuttalelse*" Riksadvokaten

Byrkjeflot, Arne (2010) "*Høringsuttalelse EUs datalagringsdirektiv*" LO i Trondheim

Byrkjeflot, Arne (2010) "*Høringsuttalelse fra Nei til EU i Sør-Trøndelag om EUs datalagringsdirektiv*" Nei til EU i Sør-Trøndelag

Byrkjeflot, Arne (2010) "*Høringsuttalelse EUs datalagringsdirektiv. Veto mot datalagringsdirektivet*" Rødt Sør-Trøndelag

Bømer, Knut (2010) "*Høring: Implementering av datalagringsdirektivet*" Kabel Norge

Chaffey, Paul (2010) "Høringsinnspill om datalagring" Abelia - Drivkraft for kunnskapssamfunnet

Digernes, Torbjørn (2010) "*Høring om datalagring*" NTNU

Dragly, Svenn-Arne (2010) "*Høring om datalagring*" FriBit

Dye, Rald (2010) "*Høring om datalagring*" Norsk Videogramforening

Dæhlen, Morten & Gisle Hannemyr (2010) "*Høringsuttalelse om datalagringsdirektivet*" UiO Det matematisk-naturvitenskapelige Fakultet - Universitetet i Oslo

Egge, Kjell Kristian & Maren Edvarsen (2010) "*Høring om datalagring*" UD - Det kongelige Utenriksdepartement

Elgesem, Dag (2010) "*Høring om datalagring*" UiB Insitutt for informasjons- og medievitenskap - Universitetet i Bergen

Fewang, Per. A & Fredrik Ingens (2010) "*Høring om datalagring*" DKF - Det Kongelige Forsvarsdepartement

Finneid, Thomas (2010) "*Høringsuttalelse om Datalagringsdirektivet (2006/24/EC)*" Samfunnsorganisasjonen Demos

Folkets Høringsuttalelse mot datalagringsdirektivet (2010) "*Folkets høringsuttalelse mot datalagringsdirektivet*" Folkets Høringsuttalelse mot datalagringsdirektivet (Underskriftskampanje)

Floberghagen, Elin & Ina Lindahl (2010) "*Høring om datalagring*" Norsk Journalistlag

Fossum, Erik & Håkon Olderbakk (2010) "*Høring - Innføring av plikt til å lagre data framkommet ved bruk av elektronisk kommunikasjon (datalagringsdirektivet)*" Nærings- og handelsdepartementet

Frantsvold, Jan Olav (2010) "*Datalagringsdirektivet og politiets behov*" Politijuristene

Frigaard, Siri S. & Jan F. Glent (2010) "*Høring om datalagring*" Det nasjonale Statsadvokatembetet

Frost, Anna Marie (2010) "*Høringsuttalelse vedrørende Datalagrings-direktivet*" Vestfold Nei til EU

Gultvedt, Anette (2010) "*Datalagringsdirektivet - høringssvar fra NNPF*" NNPF - Norsk Narkotikapolitiforening

Galtrud, G. Helge (2010) "*Høringsuttalelse om datalagringsdirektivet*" Fagforbundet Lillehammer Avdeling 59

Gjedrem, Olaf (2010) "*Høringsuttalelse om Datalagringsdirektivet*" Rogaland Nei til EU

Gjengedal, Anstein (2010) "*Høring om datalagring*" Politidirektoratet

Giil, Håkån Steinar & Hege Lothe (2010) "*Høringssvar om Datalagringsdirektivet*" Sogn og Fjordane Nei til EU

Gundersen, Roar (2010) "*Høringssvar: Datalagringsdirektivet*" El & IT Forbundet

Haanes, Knut & Janicke Sæther Olsen (2010) "*Høring om datalagring*" Barneombudet

Halse, Marit (2010) "*Høringsuttalelse om datalagring fra Rødt - tillegg*" Rødts IT- og personvernutvalg

Halse, Marit (2010) "*Høringsuttalelse om datalagring fra Rødt*" Rødt

Hansen, Jostein & Magne Braadland (2010) "*Vedr. Høring om datalagring*" NHO Reiseliv

Haraldseid, Knut-Olav & Astrid Renland (2010) "*Datalagringsdirektivet, Direktiv 2006/24/EF av 15.mars 2006. Høring med frist 12.april 2010*" KROM - Norsk forening for kriminalreform

Hassel, Maja (2010) "*Høringsuttalelse - Implementering av Datalagringsdirektivet (2006/24/EC)*" Nardo og Nidarvoll Arbeidslag

Hauglie, Tore A. & Arne Hyttnes (2010) "*Høring - norsk gjennomføring av EUs datalagringsdirektiv (2006/24/EF)*" FNO - Finansnæringens Fellesorganisasjon

Hermansen, Bengt O. & Espen Arneberg Børset (2010) "*Høring om datalagringsdirektivet (2006/24/EF) - Høringssvar*" DKK - Det Kongelige Kulturdepartment

Hordaland Nei til EU (2010) "*Høyringsuttale på datalagringsdirektivet frå Hordaland Nei til EU*" Hordaland Nei til EU

Hordaland Senterungdom (2010) "*Høring - datalagringsdirektivet*" Hordaland Senterungdom

Hovdesnakk, Ingjerd & Jorunn Solgaard (2010) "*Høringssvar - datalagringsdirektivet*" Unio

Høgdahl, Kristin & Helle Holst Langseth (2010) "*Høring om datalagring*" UiO Juridisk Fakultet - Universitetet i Oslo

Ims, Leif (2010) "*Høring om datalagring*" Altibox

Ingerø, Odd Olsen (2010) "*Datalagringsdirektivet - Høringssvar fra Kripos*" KRIPOS

Irgens, Morten & Patrick Bours (2010) "*Høringsuttalelse*" HiG - Høgskolen i Gjøvik

Iversen, Carl Morten (2010) "*Forslag om å implementere EUs datalagringsdirektiv i norsk rett*" Norsk P.E.N

Jakobsen, Øystein B. (2010) "*Svar på høring om datalagring*" Øystein B. Jakobsen

Jensen, Arne (2010) "*Høring om datalagringsdirektivet*" Norsk Redaktørforening

Jensen, Willy (2010) "Høring om datalagring" Tele2 Norge AS

Jensen, Willy & Ørnulf Storm (2010) "*Høring om datalagringsdirektivet - Uttalelse fra Post- og teletilsynet*" Post- og Teletilsynet

Johannessen, Arne & Anne-Catherine Gustafson (2010) "*Høring - EUs datalagringsdirektiv*" Politiets Fellesforbund

Johansen, Mette E. (2010) "*Høringsuttalelse vedrørende notat om datalagring*" TDC AS

Johnsen, Kåre Rygg (2010) "*Høring om datalagring*" Tekna

Kandal, Ingunn (2010) "*Høringssvar om datalagringsdirektivet*" Raudt Sogn og Fjordane

Kokkvold, Per Edgar (2010) "*Høring om datalagring*" Norsk Presseforbund

Kristiansen, Janne (2010) "*Høring om datalagring*" PST - Politiets sikkerhetstjeneste

Krogh, Harald (2010) "*Høring om datalagring - Telenors høringssvar*" Telenor AS

Kvalheim, Tore Eugen & Ørnulf Kastet (2010) "*Hørig - Datalagringsdirektivet*" YS - Yrkesorganisasjonens Sentralforbund

Lund, Ketil & Jon Wessel-Aas (2010) "*Høringsuttalelse - Datalagringsdirektivet*" ICJ-Norge - Den internasjonale Juristkommisjon, norsk avdeling

Løkken, Erland & Arne Røed Simonsen (2010) "*Høring om datalagring*" NSR - Næringslivets Sikkerhetsråd

Lønnum, Lasse & Kai Mathisen (2010) "*Høring om datalagringsdirektivet*" UiT Avdeling for IT - Universitetet i Tromsø

Michelsen, Lars-Henrik Parup m. fl (2010) "*Høring om datalagringsdirektivet*" Stopp Datalagringsdirektivet

Myksvoll, Laila (2010) "*Høring om datalagring*" GET AS

Nauste, Jonny (2010) "*Høringsuttalelse om datalagring*" Norges Politilederlag

Nordbye, Christian (2010) "*Høringsuttalelse om datalagringsdirektivet fra Østfold Nei til EU*" Østfold Nei til EU

Nordby, Trygve G. (2010) "*Høringsuttalelse om datalagring*" Europabevegelsen

NUUG (2010) "*Høyring om datalagring*" Norweigan Unix User Group

Oma, R. (2010) "*Høyringsfråsegn om datalagringsdirektivet*" Lisboanemndi

Olaussen, Heming & Vigdis Hobøl (2010) "*Høringsuttalelse om Datalagringsdirektivet fra Nei til EUs Råd*" Nei til EU

Oppland Senterparti (2010) "*Stopp datalagringsdirektivet!*" Oppland Senterparti

Orderløkken, Tore Larsen (2010) "*Høring om datalagring*" NorSIS - Norsk senter for informasjonssikring

Punsvik, Randi (2010) "*Høringsuttalelse - gjennomføring av datalagringsdirektivet i Norge*" NetCom

Ranum, Merethe Baustad (2010) "*Oversendelse av folkets høringsuttalelse - Trondheim*" Stopp Datalagringsdirektivet Trondheim

Reiss-Andersen, Berit & Merethe Smith (2010) "*Høringsuttalelse om datalagring*" Advokatforeningen

Remme, Thomas (2010) "*Datalagringsdirektivet*" Thomas Remme

Roald, Eivind (2010) "*Høringsuttalelse - implementering av datalagringsdirektivet (2006/24/EC) fra Hewlett-Packard Norge AS*" Hewlett-Packard Norge AS

Ronge, Vilde (2010) "*Høring om datalagring*" NA - Norsk Akrivråd

Rysjedal, Einar (2010) "*Bruk reservasjonsretten mot datalagringsdirektivet*" Raudt Høyanger

Schea, Trond Eirik (2010) "*Høring - Implementering av datalagringsdirektivet*" Økokrim - Den sentrale enhet for etterforskning og påtale av økonomisk kriminalitet og miljøkriminalitet

Seip, Henrik & Kari Kjølhamar Johansen (2010) "*Høring om datalagring*" ITAKT - Internett og telebransjens anti-kriminalitets tiltak

Stenseth, Emma C. Jensen & Liv Westrheim (2010) "*Høring om datalagring*" DKNH - Det Kongelige Nærings- og Handelsdepartment

Skeidsvoll, Audun (2010) "*Høring om datalagring*" Forbrukerrådet

Skjelstad, Andre N. (2010) "*Høring om datalagring: Høringsuttalelse fra Nord-Trøndelag Venstre*" Nord-Trøndelag Venstre

Solbakken, Tor-Arne (2010) "*Høring - Om datalagring*" LO Norge - Landsorganisasjonen i Norge

Stopp DLD UiT (2010) "*Folkets høringsuttalelse mot datalagringsdirektivet*" Stopp Datalagringsdirektivet - Universitetet i Tromsø

Strand, Jon Olav (2010) "*Høringsuttalelse om Datalagringsdirektivet*" Telemark Nei til EU

Stykket, Marit & Beate Sire Dagslet (2010) "*Høringsuttalelse - Gjennomføring av datalagringsdirektivet i Norge*" NITO - Norges største organisasjon for ingenører og teknologer

Svendsen, Maria (2010) "*Høyringsfråsegn om datalagringsdirektivet (dir. 2006/24/EC)*" Norsk Målungdom

Senterungdom (2010) "*Høringsuttalelse - Datalagringsdirektivet*" Senterungdommen

Tengelsen, Henry (2010) "*Høringsuttalelse fra NJ-privat vedrørende datalagringsdirektivet*" NJ-Privat - Norges Juristforbund Privat

Thorsby, Marte (2010) "*Deres ref 09/585 - HF: Høring om datalagring*" IFPI

Tromsø Nei til EU (2010) "*Høringsuttalelse om Datalagringsdirektivet*" Troms Nei til EU

Tennøe, Tore & Christine Hafskjold (2010) "*Høringsuttalelse om datalagringsdirektivet*" Teknologirådet

Thunem, Hilde (2010) "*Høringssvar - datalagring*" UNINETT Norid AS

Vik, Sigbjørn (2010) "*Høringsuttalelse om datalagring*" Sigbjørn Vik

Øvrevåge, Stian (2010) "*Innspill til høring om datalagringsdirektivet*" Stian Øvrevåge

Wessel-Aas, Jon (2010) "*Høring - Datalagringsdirektivet*" NRK - Norsk Rikskringkasting

Westlie, Tone & Kristine Høgh (2010) "*Svar på høring om datalagring*" DKA - Det kongelige arbeidsdepartement

Willassen, Svein (2010) "*Datalagringsdirektivet - Verdi i etterforskning og risikofaktorer for personvern*" Svein Willassen AS

Winterseth, Torstein Adolf (2010) "*Ei oppfordring til å seie nei til datalagringsdirektivet*" Torstein Adolf Winterseth

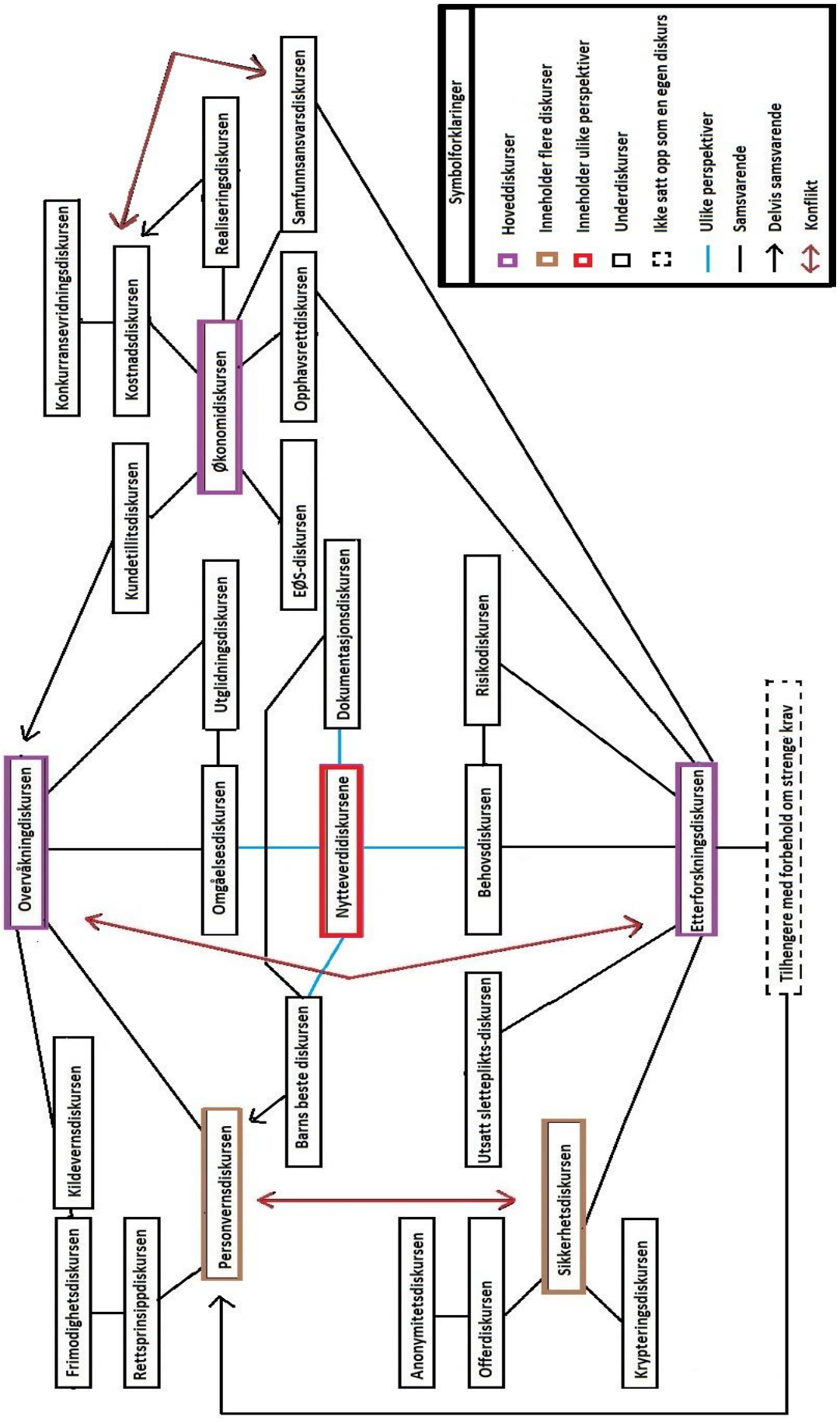
Ørebech, Peter (2010) "*Høringsuttalelse fra Foreningen Fritt Norden Norge*" Fritt Norden-Norge

Østmoen, Per Inge & Thomas Gramstad (2010) "*Høringsuttalelse - Mulig gjennomføring av Datalagringsdirektivet (2006/24/EC) om lagring av data fremkommet ved bruk av elektronisk kommunikasjon i norsk lovverk*" EFN - Elektronisk Forpost Norge

Øvigstad, Lasse, Tor-Aksel Busch, Kjersti A. Kvande & Tone Aase (2010) "*Høring om datalagring*" Oslo Statsadvokatembeter

Ågnes, Morten (2010) "*Høringsuttalelse om datalagring*" NextGenTel

Vedlegg 1: Diskurskart



Vedlegg 2: Appendix

Oversikt over datamateriale

Motstandere

- Krom, Norsk forening for kriminalreform (Foreninger og forbund)
- Advokatforeningen (Foreninger og forbund)
- EL & IT Forbundet (Foreninger og forbund)
- NITO – Norges største organisasjon for ingenører og teknologer (Foreninger og forbund)
- Norweigan Unix User Group (Foreninger og forbund)
- Yrkes og sentralforbundet (Foreninger og forbund)
- Norges Juristforbund (Foreninger og forbund)
- Datatilsynet (Myndigheter)
- IKT Norge (Næringslivet)
- Rødt (Inkludert: Sør-Trøndelag, IT- og personvernutvalg, Rødt Høyanger , Rødt Sogn og Fjordane)
- Senterparti Oppland (Politiske partier)
- Senterungdommen (Inkludert: Hordaland) (Politiske partier)
- Venstre Nord-Trøndelag (Politiske partier)
- Venstre Levanger (Politiske partier)
- Universitetet i Oslo, Matematisk-Naturvitenskapelig fakultet (Universiteter og høgskoler)
-- LO, Norge (Foreninger og forbund)
- LO i Trondheim (Foreninger og forbund)
- Anders Brenna (Privatpersoner)
- Øystein Bruås Jakobsen (Privatpersoner)
- Stian Øverevåge (Privatpersoner)
- Thomas Remme (Privatpersoner)
- Torstein Adolf Winterseth (Privatpersoner)
- FriBit (Foreninger og forbund)
- Nardo Nidarvoll Arbeidslag (Foreninger og forbund)
- Nei til EU (Inkludert: Nei til EU i Akershus, Nei til EU i Sør-Trøndelag, Nei til EU i Vestfold, Nei til EU i Rogaland, Nei til EU i Sogn og Fjordane, Nei til EU i Hordaland, Nei til

EU i Østfold, Nei til EU i Telemark og Nei til EU i Troms) (Interesseorganisasjoner)
- Stopp Datalagringsdirektivet (Inkludert: Trondheim, Universitet i Tromsø) (Interesseorganisasjoner)
- Samfunnsorganisasjonen Demos (Interesseorganisasjoner)
- Elektronisk Forpost Norge (Interesseorganisasjoner)
- ICJ-Norge ”Den internasjonale juristkommisjon, norsk avdeling” (Rettsystemet)
- Høgskolen i Gjøvik (Universiteter og høgskoler)
- Universitetet i Oslo, Juridisk fakultet (Universiteter og høgskoler)
- Folkets høringsuttalelse (Interesseorganisasjoner)
- Fagforbundet, Lillehammer, avdeling 59 (Foreninger og forbund)
- Fritt Norden (Foreninger og forbund)
- Norsk Journalistlag (Foreninger og forbund)
- Norsk Redaktørforening (Foreninger og forbund)
- Norsk Presseforbund (Foreninger og forbund)
- Norske PEN (Interesseorganisasjoner)
- Norsk rikskringkasting (Media)
- Universitet i Bergen, Institutt for informasjons- og medievitenskap (Universiteter og høgskoler)
- Nardo Nidarvoll Arbeiderlag (Foreninger og forbund)
- Norsk Målungdom (Foreninger og forbund)

Tilhengere

- Norsk Videogramforening (Foreninger og forbund)
- IFPI (Interesseorganisasjoner)
- Næringslivets Hovedorgansiasjon (Interesseorganisasjoner)
- Hewlett-Packard Norge AS (Interesseorganisasjoner)
- Lisboanemdi (Interesseorganisasjoner)
- Stine Sofies Stifelse (Interesseorganisasjoner)
- Kripos (Politi- og påtalemyndigheter)
- Norsk Narkotikapolitiforening (Politi- og påtalemyndigheter)
- Økokrim (Politi- og påtalemyndigheter)
- Politiets fellesforbund (Politi- og påtalemyndigheter)
- Politijuristene (Politi- og påtalemyndigheter)
- Politidirektoratet (Politi- og påtalemyndigheter)

- Riksadvokaten (Rettsystemet)
- Det Nasjonale Statsadvokatembetet (Rettsystemet)
- Finansdepartementet (Myndigheter)
- Finanstilsynet (Myndigheter)
- Hovedorganisasjonen for handel og tjenester i Norge
- Næringslivets sikkerhetsråd (Næringslivet
- Stine Sofies Stiftelse (Interesseorganisasjoner)
- Akademikerene (Foreninger og forbund)
- Svein Willassen AS (Interesseorganisasjoner)
- Næringslivet sikkerhetsråd (Næringslivet)
- Norges politilederlag (Politi- og påtalemyndigheter)

Tilhenger med forbehold om strenge krav

- Tekna (Foreninger og forbund)
- Akademikerne (Foreninger og forbund)
- ITAKT, Internett og Telebransjens Anti-Kriminalitets Tiltak (Foreninger og forbund)
- Unio (Foreninger og forbund)
- Post- og teletilsynet (Myndigheter)
- Norges Televisjon (Media)
- Politiets sikkerhetstjeneste (Politi- og påtalemyndigheter)
- Finansnæringens Fellesorganisasjon (Næringslivet)
- Norges Televisjon (Media)
- Post- og teletilsynet (Myndigheter)
- Forsvarsdepartementet (Myndigheter)
- Arbeidsdepartementet (Myndigheter)
- Utenriksdepartementet (Myndigheter)
- Norsk Arkivråd (Myndigheter)

Økonomiske hensyn

- Domstoladministrasjonen (Rettsystemet)
- Universitetet i Tromsø, Avdeling for IT (Universiteter og høgskoler)
- Brønnøysundregistrene (Myndigheter)
- Næringslivets Handelsorganisasjon, Reiseliv (Interesseorganisasjoner)
- Kulturdepartementet (Myndigheter)
- Stiftelsen Elektronikkbransjen (Næringslivet - Ekomtilbydere)

- Telenor (Næringslivet - Ekomtilbydere)
- Altibox AS (Næringslivet - Ekomtilbydere)
- Get AS (Næringslivet - Ekomtilbydere)
- NetCom (Næringslivet - Ekomtilbydere)
- NextGenTelAS (Næringslivet - Ekomtilbydere)
- TDC (Næringslivet - Ekomtilbydere)
- TELE 2 (Næringslivet - Ekomtilbydere)
- Ventelo (Næringslivet - Ekomtilbydere)

Behov for ytterligere dokumentasjon av nytteverdien

- Redd Barna (Foreninger og forbund)
- LO Norge (Foreninger og forbund)
- Albelia – Drivkraft for kunnskapssamfunn (Interesseorganisasjoner)
- Norsk senter for informasjonssikring (Interesseorganisasjoner)
- Europabevegelsen (Interesseorganisasjoner)
- Oslo Statsadvokatembeter (Rettsystemet)
- Barneombudet (Myndigheter)
- Redd Barna (Foreninger og forbund)
- Kabel Norge (Næringslivet - Ekomtilbydere)
- NTNU (Universiteter og høgskoler)
- Forbrukerrådet (Myndigheter)
- Nærings og handelsdepartementet (Myndigheter)
- NAV (Myndigheter)