DATALAGRINGSDIREKTIVET – RETTSLIGE KONSEKVENSER FOR NORGE

Universitetet i Oslo
Det juridiske fakultet

Kandidatnummer: 639

Leveringsfrist: 25.11.2010

Til sammen 17 918

18.11.2010

Innholdsfortegnelse

1 Innledning

Denne oppgaven går ut på å kartlegge hvilke forskjeller og konsekvenser det kan ha å implementere datalagringsdirektivet (DLD), Directive 2006/24/EC of the European Parliament i Norge.[1] Dette temaet har fått stor oppmerksomhet i media og befolkningen i Norge har engasjert seg for å sette seg inn i hva en eventuell implementering vil si for deres personvern. Et direktiv som går ut på å lagre trafikkdata for bruk til bekjempelse av alvorlig kriminalitet kan få borgerne i samfunnet til å føle seg overvåket. Det har per dags dato ikke blitt fattet noe vedtak for om direktivet skal implementeres i Norge. I den sammenheng mener jeg at det er viktig å se på de juridiske og reelle konsekvenser en eventuell implementering kan ha. Jeg har valgt å se på de dataene som lagres i dag etter gjeldende rett og konkret finne ut av om det vil medføre store forskjeller å implementere datalagringsdirektivet i Norge.[2]

1.1 Tema og problemstilling

Tema for oppgaven vil være datalagringsdirektivet generelt og konsekvensene direktivet kan gi og hvilke konsekvenser det kan ha å ikke implementere det. Jeg vil også, så godt det lar seg gjøre, oppliste hvilke data som lagres i dag. For å kunne gjøre det er jeg avhengig av opplysninger fra tele- og internettilbydere. Problemstillingen blir videre om kriminalitetsbekjempelse må gå på bekostning av personvernet. Jeg synes det er en interessant vinkling å se på hvilke muligheter politiet har til å innhente trafikkdata per i dag og hvilke forskjeller DLD eventuelt vil medføre for dem, samt se på hvilke konsekvenser det kan ha for deres arbeid om DLD ikke skulle bli implementert. Er politiet avhengig av å innhente denne type data for å oppklare saker? Hvor ofte tar politiet i bruk trafikk- og lokasjonsdata ved oppklaring av saker? Hvilken bevisverdi har det i retten? Jeg vil også

[1] Official journal of the European Union.

[2] Datalagringsdirektivet var oppe til høring i departementet i januar 2010.

gjennomgå gjeldende rett og sammenligne resultatene med lagringsplikten etter datalagringsdirektivet. En annen problemstilling er om politiet er avhengig av DLD for å kunne anvende trafikkdata. Hovedproblemstillingen blir dermed hvilke konsekvenser implementering av datalagringsdirektivet vil medføre i Norge. Både positivt og negativt. Det må vurderes om kriminalitetsbekjempelse skal gå på bekostning av personvernet og om datalagringsdirektivet setter et slikt ultimatum. Det vil også være viktig å drøfte om datalagringsdirektivet er en trussel for personvernet. I den sammenheng er det relevant å se på konsekvenser for teletilbyderne som blir pålagt å fysisk lagre all dataen, og om det kan gjøres på en sikker nok måte.

Dette vil i stor grad være en komparativ oppgave, samt inneholde rettspolitiske vurderinger fra flere ståsteder.

1.2 Generelt om direktivet og dets bakgrunn

I et samfunn hvor kriminalitet og terrorisme er en økende trussel er det på det rene at myndighetene stadig må være på utkikk etter nye metoder for å stoppe disse handlingene. Etter terrorangrepet 11. september 2001 i New York og bombene på undergrunnen i London 7. juli 2005 har det blitt satt et større fokus på overvåkning og kontroll av kriminelle i samfunnet.[3] I etterkant av disse angrepene har det kommet frem at det ble kommunisert via internett i planleggingsfasen, noe som kan tale for at angrepene kunne blitt avverget. Slik informasjon kan hjelpe til med etterforskning av fremtidige terrorangrep.

For å stoppe terrorisme er myndighetene og politiet avhengig av å kunne spore opp kommunikasjon mellom mistenkte personer og grupper. Kommunikasjon på tvers av landegrenser og kontinenter har blitt forenklet de senere år på grunn av hyppig bruk av internett og datatrafikk. En konsekvens av dette er at bekjempelsen av alvorlig kriminalitet

[3] http://eur-lex.europa.eu

har blitt betydelig vanskeligere å oppklare. I dag kan man gjemme seg bak IP-adresser[4] og ha kontakt via mobiltelefon og internett, noe som vanskeliggjør arbeidet for politiet. Etter gjeldende rett kan politiet her i landet be om overvåkning og avlytting av personer det er "skjellig grunn" til mistanke for skal begå kriminelle handlinger, jf. straffeprosessloven § 216 b[5].

Den 15. Mars 2006 påla den Europeiske Union (EU) alle medlemsstater å implementere et direktiv som går ut på lagring av datatrafikk, kjent som datalagringsdirektivet[6]. Dette direktivet går ut på lagring av trafikk- og lokasjonsdata i forbindelse med kommunikasjonstjenester. Formålet med DLD er etter direktivets artikkel 1 å bidra til "*investigation, detection and prosecution of serious crime*". Direktivet skal gjelde trafikkdata og lokasjonsdata[7] for både juridiske og fysiske personer. Men selv om datalagringsdirektivet skal hjelpe myndighetene i deres arbeid med å stanse alvorlig kriminalitet, er det ikke utelukkende positivt. Ved at all data blir lagret om alle som anvender telefoni og internett, uavhengig om man er mistenkt for en kriminell handling eller planlegging av det, er det lett å føle seg overvåket i sitt eget samfunn. Man kan si at dette strider mot prinsippet om at man er uskyldig inntil bevist motsatt.[8]

I dagens samfunn bruker de aller fleste mye tid på telekommunikasjon over internett eller telefon og på denne måten legger man igjen informasjon om seg selv og andre som skal lagres fra mellom 6 måneder og 2 år. For eksempel på nettstedet Facebook skriver man inn mye sensitiv informasjon om seg selv, og man fraskriver seg retten til bildene man laster opp. En slik utvikling kan være starten på ødeleggelsen av personvernet slik vi kjenner det i dag. Dette er imidlertid ikke direkte sammenhengende med datalagringsdirektivet. Direktivet vil kunne hjelpe med å spore opp identiteten til brukeren av fastnettelefoni,

---

[4] Forklaring av IP-adresse finnes i punkt 1.5.

[5] Lov om rettergangsmåten i straffesaker av 22. mai 1981

[6] Directive 2006/24/EC of the European Parliament. Heretter forkortet DLD

[7] Se 1.5 for definisjon.

[8] Uskyldspresumsjonen. EMK art. 6 nr. 2.

mobiltelefoni og internett. Det skal bli mulig å anvende data som ble lagret før vedkommende utførte den lovstridige handlingen.

DLD vil bidra til å gjøre det lettere å oppspore kriminelle, og identifisere disse, i følge direktivet.[9] Men ettersom informasjonen blir lagret om alle som bruker teleoperatørens nett, foregår lagringen av data helt uavhengig av om man er mistenkt for en kriminell handling eller ikke. Man legger igjen mange spor ved bruk av telefoni og internett, og man kan argumentere for at privatlivet blir svekket når det skal lagres med et slikt formål. De fleste synspunktene på DLD som har blitt publisert i media har vært negative og de fleste mener at dette er et stort inngrep i personvernet. Samtidig må jeg i denne oppgaven vurdere nyttigheten av et slikt tiltak. Er det slik at man vil kunne lettere oppklare og straffeforfølge kriminelle er jo det til fordel for alle, selv om personvernet kanskje ikke vil være like sterkt.

1.3 Metode

I den delen av oppgaven som omhandler datalagringesdirektivet og rettspolitiske drøftelser rundt dette, stammer mye av materialet fra høringssvar som ble tilsendt departementet etter høringsnotatet på datalagringsdirektivet. Jeg har også hatt nyttige samtaler med forskjellige organisasjoner og personer med tilknytning til direktivet for å få en beskrivelse av virkeligheten og underbygge de juridiske argumentene.

1.4 Avgrensning

I denne oppgaven vil jeg i hovedsak fremstille gjeldende rett for hva politiet kan foreta seg av avlytning og overvåkning, samt teleoperatørs adgang til lagring av trafikkdata. Det er imidlertid ingen uttømmende fremstilling. Det vil også bli fremlagt en gjennomgang av DLD generelt og rettspolitiske drøftelser rundt dette. I den komparative delen av oppgaven

[9] Politijuristene om DLD

vil jeg sammenligne hvordan rettstilstanden er i dag og hvilke endringer en eventuell implementering av DLD kan og vil medføre, også den prinsipielle endring. Når det gjelder forholdet mellom datalagringsdirektivet og EMK[10] art. 8 velger jeg å ikke skrive inngående om det. Jeg vil imidlertid komme inn på temaet og i den sammenheng kommer jeg til å gi en overfladisk gjennomgang. Det forholdet er såpass omfattende at en nøye gjennomgang av temaet vil passe best som en egen oppgave.

1.5 Begrepsforklaring

I en oppgave av denne art vil det være nødvendig å forklare visse tekniske begreper. Jeg vil under dette punktet gi definisjoner og forklaringer på tekniske fagord som går igjen i oppgaven.

IP-adresse: IP-adresse er en forkortelse på ”internet protocol address” og den består av 12 tall. En IP-adresse er en unik adresse som blir brukt for å gjengi brukeren av en pc på et nettverk.[11] Når man logger inn på internett får man gjerne tildelt en tilfeldig IP-adresse fra leverandøren man bruker, den kan være statisk eller dynamisk. Bak IP-adressen er man dermed anonym, men leverandøren av internett kan identifisere hvilket abonnement som brukte den spesifikke IP-adressen, innen 3 uker etter adressen ble tildelt. Etter 3 uker blir IP-adressen slettet fra leverandøren.

Trafikkdata: Når man kommuniserer via et fastlinjenettverk eller mobilnettverk vil data lagres. Denne dataen vil kunne avsløre hvem som har hatt kontakt med hvem, når kommunikasjonen fant sted og hvor lenge den varte. Telefonnummer, tekstmeldinger lagres da også. I de fleste tilfeller kan trafikkdata knyttes opp mot spesifikke brukere og det regnes derfor som personopplysninger.[12]

---

[10] Den europeiske menneskerettskonvensjon

[11] http://en.wikipedia.org/wiki/IP_address

[12] Teknologirådet (2005)

Lokasjonsdata: Lokasjonsdata vil kunne lokalisere hvor trafikkdataen ble overført. Det er altså teleoperatøren som lagrer hvilken telefonmast mobiltelefonen brukte for å kommunisere med sentralen.[13] Lokasjonsdata kan knyttes opp mot basestasjonssøk[14].

Basestasjon: En basestasjon er en radiosender som fungerer som bindeleddet mellom mobiltelefonen og telefonsentralen, eller mellom flere kommunikasjonsradioer. Skal en basestasjon dekke et stort område er det hensiktsmessig at denne blir plassert på en topp eller høyde. Dersom det er stor tetthet av apparater lønner det seg at basestasjonen settes opp for å dekke et mindre område og heller flere basestasjoner.[15]

Innholdsdata: Innholdsdata er en betegnelse man bruker på innholdet i trafikkdataen, altså hva som blir sagt og/eller skrevet i kommunikasjonen. Per dags dato skal innholdsdata ikke lagres av teleoperatøren, men i visse tilfeller kan politiet be om avlytning hvis det er skjellig grunn til mistanke om kriminell aktivitet hos en person.[16] Det er ingen plikt etter DLD å lagre innholdsdata.

Data: Se trafikkdata og lokasjonsdata for forklaring.

Bruker: En bruker er en fysisk eller juridisk person som anvender en offentlig tilgjengelig elektronisk kommunikasjonstjeneste til privat eller forretningsmessig bruk uten at den har abonnert på tjenesten.

Brukeridentitet: Det er en fast identifikasjon som opprettes når vedkommende tegner abonnement eller registrerer seg som bruker av internettilgangen eller en internettkommunikasjonstjeneste.

---

[13] Teknologirådet (2005)

[14] Se ”basestasjon”.

[15] http://www.nrpa.no

[16] Teknologirådet (2005)

Celle-ID: Det er en forkortelse på celleidentifikasjon.[17] Det er identiteten på den cellen hvor et mobiltelefonanrop kommer fra eller hvor det avsluttes. Det er en teknikk som kan lokalisere hvor mobiltelefonen befinner seg. Mobiltelefonen bruker den nærmeste telefonmasten for å få signaler, og legger dermed igjen et spor for hvor den befinner seg. Denne teknologien er ikke helt nøyaktig ettersom en telefonmast kan sende signaler i flere retninger.

A-nummer: A-nummeret er det nummeret som foretar en opprigning. B-nummeret blir dermed det nummeret som mottar anropet.

Statisk og dynamisk IP-adresse: En statisk IP-adresse er et nummer som tildeles PC-en av internettleverandøren, og det blir da den PC-ens permanente adresse på internett. Adressen er altså statisk.[18] PC-er kan bruke denne IP-adressen til å finne og kommunisere med hverandre, mye på samme måte som man bruker telefonnummer. En dynamisk IP-adresse er en adresse som endrer seg ved visse tidsrom. Internettleverandøren gir altså ikke ut noen fast adresse til den PC-en, men varierer med forskjellige adresser. Dette er på grunn av at det ikke er nok IP-adresser til bruk.

Dial-up tilgang: Dette er måten man ringer opp på internettleverandørens nett via PSTN (public switched telephone network).[19]

DSL: Det er en forkortelse på Digital Subscriber Line.[20] Det er ulike teknologier for å utnytte kobberbasert par-kabelnett til høyere båndbredder enn vanlig telefoni (ISDN).

IMSI-nummer: IMSI er en forkortelse på International Mobile Subscriber Identity.[21] Dette nummeret består av 15 siffer og brukes som identifikasjon for bestemmelsen av telefonen

[17] www.telebeans.org

[18] http://searchwindevelopment.techtarget.com/

[19] www.wikipedia.org

[20] www.wikipedia.org

eller SIM-kortet. Det gir en tilgang til nettverket til teletilbyderen, og plasseringen av enheten kan spores via dette nummeret.

IMEI-nummer: IMEI står for International Mobile Equipment Identity. Dette er en internasjonal standard som merker mobiltelefoner ved å gi de et unikt serienummer. Hver gang man slår på mobiltelefonen sjekkes IMEI-nummeret opp mot operatørens IMEI-register for at telefonen skal få adgang til mobilnettet. Slik kan operatøren til enhver tid ha oversikt over hvem som er bruker av deres nett.[22]

2 Gjeldende rett

I dette avsnittet vil jeg gå gjennom noen de viktigste bestemmelsene som anvendes i dag for å hente informasjon om trafikkdata.

2.1 Straffeprosessloven

Etter det som har kommet frem i media under debatten om DLD, kan det virke som politiet i dag ikke har noen adgang til å hente ut trafikkdata. Dette er ikke riktig. Politiet har muligheten til å foreta langt mer personvernrettslige inngripende handlinger med hjemmel i straffeprosessloven enn det som foreslås i datalagringsdirektivet, samt anvende de data som i dag lagres hos tilbyderne. Selv om dette ikke er et argument for DLD, er det viktig at samfunnet er klar over hvordan rettstilstanden er i dag. Dersom det foreligger skjellig grunn til mistanke har politiet adgang til å kreve romavlytting, telefonavlytting og annen

[21] www.wikipedia.org

[22] www.amobil.no

kommunikasjonskontroll etter straffeprosessloven[23]. Politiet kan også, med tillatelse fra Post- og teletilsynet (PT), få utlevert taushetsbelagt informasjon fra teletilbydere. Denne taushetsbelagte informasjonen er trafikk- og lokasjonsdata. Den kan være lagret i opp til 5 måneder.[24]

Videre i fremstillingen vil jeg komme med en oversikt over visse tiltak myndighetene kan sette i verk ved mistanke om kriminell handling.

2.1.1 Kommunikasjonskontroll

Kommunikasjonskontroll går ut på romavlytting og annen kontroll av kommunikasjonsanlegg som politiet kan foreta av personer som med skjellig grunn mistenkes for alvorlige kriminelle handlinger eller forsøk på slike.[25] Det er imidlertid en forutsetning at det er en mistanke for at politiet kan sette i gang med slike handlinger, og det er i hovedsak retten som gir tillatelse til kontrollen i det konkrete tilfellet. Dette gjøres ved en kjennelse. Det er et krav om at retten skal ta en avgjørelse i hvert enkelt tilfelle og politiet kan ikke av eget initiativ starte opp kontrollen. Det finnes et unntak fra denne hovedregelen, og det er dersom det er hastverk i saken. I situasjoner hvor det haster å starte opp med kommunikasjonskontrollen kan ordre fra påtalemyndigheten gi tillatelse til oppstart av kontrollen. Da må påtalemyndighetens beslutning forelegges retten til godkjennelse innen 24 timer etter at kontrollen startet, jf. strpl. § 216 d. Er det snakk om utlevering av taushetsbelagt informasjon er det Post- og teletilsynet[26] som avgjør om taushetsplikten skal fravikes. Er det snakk om romavlytting er det ikke tilstrekkelig at PT gir tillatelse. Grunnen til det er den inngripende naturen i vedtaket.

---

[23] Strpl. § 216 b

[24] Se punkt 2.4.

[25] Jusleksikon, Jon Gisle (2007) s. 170.

[26] Heretter forkortet PT.

To av de mest sentrale bestemmelsene på dette temaet er straffeprosessloven § 216 b og § 215 a.

2.1.1.1 Strpl. § 216 b

Denne paragrafen ligger under kapittel 16 a i straffeprosessloven, og den ble tilføyd loven i 1992 og senere endret i 2000. Her kommer det frem at retten kan gi politiet, ved kjennelse, tillatelse til å foreta annen kontroll av kommunikasjonsanlegg når noen med skjellig grunn mistenkes for en handling eller forsøk på en handling som kan medføre fengsel i 5 år eller mer. Hva som kan forstås som "skjellig grunn", er god eller rimelig grunn.[27] Det er på den rene at det må være en velbegrunnet mistanke. En oppfatning er at det kreves sannsynlighetsovervekt for at vedkommende har begått handlingen. Også hvis det mistenkes overtredelse av straffeloven[28] §§ 90, 91a, 94 jf. 90, 145 annet ledd, 162, 162c, 201a, 317, jf. §§ 162 eller 390a kan kommunikasjonskontroll tillates.

Hva denne kontrollen går ut på blir fremlagt i bestemmelsens tredje ledd litra a-d. For det første kan det være å innstille eller avbryte overføring av samtaler eller annen kommunikasjon til eller fra bestemte telefoner, datamaskiner eller andre kommunikasjonsanlegg den mistenkte besitter eller antas å vil bruke. Videre kan politiet stenge anlegg som nevnt i litra a for kommunikasjon. Kontrollen kan også anvendes for å identifisere anlegg som nevnt i litra a ved hjelp av teknisk utstyr. Til slutt kan politiet kreve at tilbyder av nett eller tjeneste skal gi de opplysninger om hvilke kommunikasjonsanlegg som i et bestemt tidsrom skal settes eller har vært satt i forbindelse med anlegg som nevnt i litra a og andre data knyttet til kommunikasjonen.

Det ble foreslått for straffeprosesslovkomiteen[29] på et tidligere tidspunkt, å danne generelle bestemmelser om adgang til telefonkontroll i særlig alvorlige saker og i visse saker hvor

---

[27] Norsk straffeprosess. Andenæs, 2009, s. 285.

[28] Almindelig borgelig straffelov av 22. mai 1902.

[29] Se Innst. S. 31 og s. 2257-258.

det var spesielt behov bruk av en slik etterforskningsmetode. Dette forslaget ble imidlertid ikke fulgt, etter som det ble stilt spørsmål ved at myndighetene kunne få muligheten til å avlytte telefoner. Tilbakeholdenheten rundt dette kan ses opp mot "storebror ser deg"-samfunnet, hvor myndighetene overvåker alle og alt som skjer. Dette er selvsagt ikke ønskelig. Personopplysningsloven[30] kap. VII skal sikre at personvernet blir ivaretatt på effektiv og sikker måte.

Før lovrevisjonen i 1999 var det mulig for politiet å kreve telefonavlytting i kun to ulike typer saker. Det kunne kreves i saker hvor det gjaldt rikets sikkerhet og i saker som gjaldt narkotika. I de sakene hvor det var rikets sikkerhet som stod i fare var det som regel snakk om spionsaker. Begrunnelsen for at akkurat disse to typer forbrytelser kunne gi adgang til bruk av telefonavlytting var at det kunne være svært vanskelig å etterforske slike saker på vanlig måte, fordi lovovertrederen ofte brukte tid på å sørge for at vedkommende ikke skulle bli avslørt. Det er heller ikke en privatperson som blir krenket ved disse forbrytelsene, men staten. Vanligvis er det til stor hjelp for politiet å avhøre fornærmede, men i spionsaker og narkotikasaker er det ikke like enkelt.[31] Hjemmelen for disse inngripende etterforskningsmetodene fantes i lov om kontroll med post- og telegrafforsendelser og med telefonsamtaler og straffeprosessloven kap. 16 a.

I 1999 ble det foretatt en revisjon av reglene som omhandlet telefonkontroll. Selv om det ble erkjent av Justisdepartementet at "*den enkeltes rett til privatliv og til å kunne meddele seg til andre uten innsyn fra utenforstående er en fundamental menneskerettighet*" ble det åpnet for telefonavlytting ved mistanke om andre grove forbrytelser.[32] Adgangen ble altså noe videre enn den var før. Som en begrunnelse for dette ble det pekt på at kriminaliteten har endret seg på den måte at tradisjonelle etterforskningsmetoder virket mindre effektivt enn før. Videre ble det åpnet for overvåkning av kommunikasjon mellom datamaskiner, og ordlyden ble endret fra "*telefonavlytting*" til "*kommunikasjonskontroll*". Som en

[30] Lov om behandling av personopplysninger av 14. april 2000.

[31] Ole Jakob Bae, Personvern i narkotikasaker og i saker om rikets sikkerhet, LoR 1993 s. 109.

[32] Ot. prp. nr. 64 for 1998-99 s. 46, 2. sp.

konsekvens av utvidelsen av den skjulte kommunikasjonskontrollen så myndighetene det som naturlig å opprette et kontrollorgan som kunne være overordnet og ha tilsyn til arbeidet. Dette organet er i dag kjent som PST, politiets sikkerhetstjeneste. Det skulle også opprettes et kontrollutvalg etter strpl. § 216 h som får tilgang til alle opplysningene og vurderer om det er kritikkverdige forhold som bør meldes fra til Justisdepartementet eller om kontrollen fungerer slik den skal.

Rt. 2009 s. 394

Denne saken gikk i korte trekk ut på om strpl. § 216 b gir adgang til kommunikasjonskontroll når det gjaldt å identifisere en bestemt person som brukte en mobiltelefon, og ikke selve kommunikasjonsanlegget. Det var politiet som la frem en begjæring om kommunikasjonskontroll av en bestemt mobiltelefon. De hadde grunn til å tro at det var en annen person enn telefonens registrerte bruker som anvendte telefonen til narkotikakriminalitet. I første instans tok tingretten begjæringen til følge, men denne avgjørelsen ble anket til lagmannsretten og videre til Høyesterett etter lagmannsrettens medhold med tingretten.

Lagmannsretten la vekt på de reelle hensyn ved det store behovet for å identifisere den mistenkte og mente at dette tilfellet også var ment å falle inn under bestemmelsen dersom lovgiver vært oppmerksom på en slik problemstilling. Videre ble det vist til hovedhensikten ved kontroll av trafikkdata etter strpl. § 216 b annet ledd var å skaffe opplysning om hvor det mistenkte oppholdt seg. Lagmannsretten mente at det var et større inngrip i personvernet å få kontroll over hvem den mistenkte kommuniserte med og i hvilket område vedkommende befant seg i, enn hans identitet og eventuelt adresse. Selv om Høyesterett (HR) var enig i flere av argumentene i lagmannsrettens avgjørelse, kom de enstemmig til at dommen måtte oppheves på grunnlag av feil lovtolking. HR var enige i at verken ordlyden i strpl. § 216 b eller forarbeidene ga uttrykk for at oppregningen av vilkår i litra a-d var en uttømmende liste.

Videre viste HR til at en avgjørelse på dette området må hvile på en klar lovhjemmel. Man er såpass nær legalitetsprinsippet i norsk rett, samt EMK art. 8 om retten til privatliv at det må være et strengt lovskrav. HR viste også til en kommentar fra forarbeidene Ot. prp. nr. 60 (2004-2005) s. 109 hvor det ble slått fast at ”*slik departementet oppfatter gjeldende rett, kan politiet ikke ta i bruk GSM-identifiseringssystemer uten lovhjemmel. Selv i situasjoner hvor de aktuelle anleggenes identitet kan fanges opp uten at kommunikasjon avlyttes, innbærer bruk at slike systemer et så vidt følbart inngrep for de som berøres av undersøkelsene, at det ikke bør åpnes for bruk at slikt utstyr for Stortinget har tatt stilling til spørsmålet*”.

Dette er et eksempel på hvordan reglene fungerer i dag og at det skal noe til før lovskrav er oppfylt og politiet får adgang til å kontrollere kommunikasjon.

2.1.1.2 Strpl. § 215 a

Etter denne bestemmelsen kan påtalemyndigheten gi pålegg om sikring av elektroniske lagrede data som antas å kunne ha bevisverdi ved en eventuell rettssak. Dette er et vilkår som fremkommer i paragrafens første ledd. Denne bestemmelsen ligger noe utenfor temaet i så måte, men jeg ser det som nyttig å ta med en rask gjennomgang for å få en noe bedre oversikt over politiets etterforskningsmetoder. Etter det jeg har funnet ut ser det ut til at det er PST som anvender denne bestemmelsen mest.

Videre er det slik at dette pålegget kun kan gis dersom det er ”*grunn til å tro at det er begått en straffbar handling*”, jf. annet ledd. For at det skal være ”grunn til å tro” at det foreligger et kriminelt forhold må det altså være visse objektive elementer i saken som peker i den retning. Det kreves ikke sannsynlighetsovervekt for å gi et slikt pålegg og det er heller ikke et krav om skjellig grunn til mistanke.

Etter strpl. § 215 a tredje ledd skal en mistenkt underrettes straks dataene er sikret og vedkommende har fått status som siktet.

Det er ikke spesifisert hvilke data som er omfattet, derfor må man etter en antitetisk tolkning anta at det gjelder alle data, uten hensyn til om det er tall, symboler eller bokstaver. Det har heller ikke betydning om dataen er kryptert eller av mening. Det er på det rene at både trafikkdata og innholdsdata faller inn under denne bestemmelsen. I tillegg til lyd, bilder og tekst. Det eneste vilkåret er at dataene er elektronisk lagret når politiet gir pålegg om sikring.[33]

Man kan altså se her at også innholdsdata er inkludert. Denne bestemmelsen går i så måte lenger enn bestemmelsene etter DLD vil gjøre. Der vil det ikke bli inkludert innholdsdata. Man kan argumentere for at DLD er en mellomløsning mellom de dataene som lagres i dag og hvilke metoder politiet har for å etterforske mistenkte. Det er et vesentlig poeng at politiet her kan kreve såpass inngripende etterforskningsmetoder i de tilfellene hvor det kun er en objektiv indikasjon på bevisverdi.

Etter de argumentene som blir brukt mot implementering av DLD er det mye som tyder på at ikke alle er klar over hvilke etterforskningsmetoder politiet bruker i dag og hvor mye data som allerede blir lagret hos teleoperatørene. Det kan være et argument som trekker i retning av at dersom folk hadde vært bedre opplyst på dette punkt, ville de ikke reagert like sterkt på de bestemmelsene som innføres med datalagringsdirektivet. Et annet poeng er jo selvsagt om borgerne i samfunnet i det hele tatt har lyst til å ha en slik lagring av data. Det må også presiseres at det her innhentes informasjon i sanntid, av person(er) som allerede er mistenkt og en etterforskning allerede er startet opp. Her vil altså ikke all informasjon og alle borgere lagres til enhver tid i tilfellet den skulle bli mistenkt for en kriminell handling.

2.1.2 Kommunikasjonskontrollforskriften

Den 31. mars 1995 ble det opprettet en forskrift for å regulere kommunikasjonskontrollen nærmere. Den er laget med hjemmel i strpl. § 216 k.

[33] Kommentarer til Straffeprosessloven v/ Geir Sunde Haugland for rettsdata (2010)

I forskriftens første paragraf blir det slått fast at det er påtalemyndigheten som avgjør om det skal bes om rettens samtykke til kommunikasjonskontroll. I hastesaker kan påtalemyndigheten selv treffeavgjørelsen, dette med hjemmel i strpl. § 216 d.

Forskriften har bestemmelser som skal klargjøre praksisen rundt kommunikasjonskontroll. Som tidligere nevnt er det et stort inngrip i den personlige sfære og må utøves ved varsomhet. Denne forskriften er opprettet for å sikre best mulig behandling i de tilfellene kommunikasjonskontroll er nødvendig.

2.2 Ekom-loven

Ekomloven er en forkortelse på lov om elektronisk kommunikasjon av 4. juli 2003. Formålet bak denne loven er å sikre brukere i hele landet gode, rimelig og fremtidsrettende elektroniske kommunikasjonstjenester, jf. § 1-1. Lovens virkeområdet er knyttet til elektronisk kommunikasjon med tilhørende infrastruktur, tjenester, utstyr og installasjoner.

Etter ekoml. § 2-7 annet ledd er det adgang til lagring av data i en viss periode. Dataen det er snakk om her er trafikkdata som for eksempel kan identifisere hvem og hvor lenge man har ringt. Teleoperatørene skal kunne lagre data for bruk til fakturering av sine kunder. Selskapene har altså en mulighet til å lagre trafikkdata i dag, så fremt det er behov for det for å utføre en nøye fakturering. Det kommer frem bestemmelsens andre ledd at trafikkdata[34] skal slettes eller anonymiseres så fort informasjonen ikke lenger er relevant for kommunikasjons- eller faktureringsformål, med mindre annet er bestemt i medhold av lov. Etter en antitetisk tolkning må man kunne slå fast at det er en lagringsadgang her, men ingen plikt.

I ekoml. § 2-8 er det bestemmelser om tilrettelegging for lovbestemt tilgang til informasjon. Det er operatøren selv som må sørge for at lovbestemt tilgang til informasjon

[34] Se punkt 1.5.

om sluttbruker og elektronisk kommunikasjon sikres. Det siktes her til her er typisk politiets kommunikasjonskontroll eller strpl. kap 16a. Etter bestemmelsens annet ledd blir det lagt til grunn at de driftskostnader som knytter seg til oppfyllelse av denne tilretteleggingsplikten skal dekkes av staten. Man kan kanskje her også anta at det er staten som vil stå for merkostnadene som vil følge av implementeringen av datalagringsdirektivet, selv om det på ingen måte er sikkert.

2.2.1 Taushetsplikt – e-koml. § 2-9

Ekomloven § 2-9 omhandler taushetsplikt. Denne bestemmelsen er videreført fra den tidligere teleloven fra 1995. I denne bestemmelsen kommer det frem at leverandøren og den som installerer apparatet har en streng taushetsplikt om innholdet av den elektroniske kommunikasjonen og andres bruk av elektronisk kommunikasjon. Leverandøren må selv gjennomføre tiltak som hindrer at andre kan få tak i informasjonen, og de kan heller ikke selv ta nytte av informasjon etter kommunikasjonen ifølge bestemmelsen. Dette er en noe uheldig formulering. Det sies at hensikten var å videreføre taushetspliktbestemmelsen fra telegrafloven av 1899 § 5 hvor det gjaldt taushetsplikt ovenfor ”uvedkommende” og at leverandøren selv ikke er omfattet. At denne ordlyden ble borte fra bestemmelsen i teleloven av 1995 skulle ikke medføre noen realitetsendring.[35] Man må derfor tolkes ekoml. § 2-9 første ledd innskrenkende. Det foreligger meget strenge regler for de bedrifter som tilbyr kommunikasjonstjenester i Norge.

Man finner imidlertid et unntak i § 2-9 tredje ledd. Her kommer det frem at den nevnte taushetsplikten ikke er til hinder for ”*at det gis opplysninger til påtalemyndigheten eller politiet*” om hemmelige nummer og andre opplysninger i forbindelse med abonnementet. Det er her i følge Rønnevig ment opplysninger om hvilke SIM-kort som kan knyttes til et IMEI-nummer, hvilket telefonnummer som hører til et SIM-kortnummer samt hvilket SIM-kort og dermed telefonnummer som kan knyttes til en oppladning som er type abonnementsopplysninger som politiet og påtalemyndigheten i henhold til bestemmelsens

[35] Rønnevig (2010) note 39, Gyldendal Rettsdata.

tredje ledd kan kreve utlevert, uavhengig av taushetsplikten.[36] Det kommer ikke klart frem i bestemmelsen, men Rønnevig mener dette er en feil som fulgte med ved oppdatering av loven og at man må se hen til forarbeidene for å komme frem til det lovgiver mente.[37] Taushetsplikten er heller ikke til hinder for at leverandøren kan oppgi informasjon til annen myndighet med hjemmel i lov, jf. e-koml. § 2-9 femte ledd.

2.2.2 Unntak fra taushetsplikt – Post- og teletilsynets avgjørelse

Etter e-komloven § 2-9 følger det en lovpålagt taushetsplikt om innhold av elektronisk kommunikasjon for tele- og internettilbydere. Et unntak fra dette følger etter strpl. § 118 første ledd og § 230 første og fjerde ledd. Her kommer det frem at retten og politiet, via påtalemyndigheten, kan be om fritak fra taushetsplikten. En slik anmodning blir vurdert av Post- og teletilsynet (PT) etter delegasjon fra Samferdselsdepartementets vedtak av 15. september 1995.

PT legger i en slik vurdering vekt på forskjellige momenter. For det første må det være innledet en etterforskning eller være en mistenkt person, jf. strpl. § 224 for at PT skal gi tillatelse til å vike fra taushetsplikten. Dette gjelder spesielt i de tilfeller det gjelder trafikkdata.[38] PT er svært restriktive med å gi fritak for taushetsplikten når det er trafikkdata som knyttes til en person som ikke er mistenkt for en kriminell handling, dette på grunn av personvernhensyn.[39] Det skal ikke være slik at politiet skal kunne lete etter kriminelle handlinger.

Videre blir det lagt vekt på om det allerede er en etterforskning av et straffbart forhold og hvor viktig de elektroniske sporene er for den konkrete etterforskningen. Denne

---

[36] Rønnevig (2010) note 42

[37] Ot.prp. nr. 58 (2002-2003) s. 93

[38] Post- og teletilsynet (2010)

[39] Post- og teletilsynet (2010)

vurderingen blir gjort skjønnsmessig av departementet, ved Post- og teletilsynet. Det skal også bli lagt vekt på muligheten for bruk av andre etterforskningsmetoder.

Gjelder forespørselen basestasjonsøk[40] (kan sammenlignes med lokasjonsdata) skal tilsynet vurdere befolkningstettheten i det området det anmodes trafikkdata fra, samt graden av alvorlighet rundt det straffbare forholdet og hvilken tid på døgnet anmodningen omhandler. Politiet skal med andre ord ikke kunne få utlevert trafikkdata i området hvor en sykkel ble stjålet.

Saksbehandlingen i slike saker er ikke omfattet av forvaltningsloven § 4 b, og avgjørelsen kan ikke påklages etter vanlige forvaltningsrettslige bestemmelser. Retten kan imidlertid overprøve avgjørelsen, jf. strpl. § 118 annet ledd. Det er også en mulighet for politiet å innhente trafikkdata uten samtykke fra PT med hjemmel i strpl. § 216 b annet ledd litra c.

2.3 Personopplysningsloven

Etter personopplysningsloven (popplyl.) § 1 er lovens formål å beskytte hver enkelts personvern slik at det ikke blir krenket gjennom behandling av personopplysninger. Loven skal sørge for at personopplysninger blir behandlet i samsvar med personlig integritet og privatlivets fred, jf. popplyl. § 1 annet ledd. Ordet personvern må sies å være et norsk begrep. I andre land hører man gjerne ”privacy” og ”integrity”. Her i landet går man ut fra at personvern betyr vern av ens personlige integritet og individets ukrenkelighet.[41] I tillegg skal loven bidra til at det blir tilstrekkelig kvalitet på behandling av personopplysninger.

Personopplysninger defineres i § 2 som opplysninger og vurderinger som kan trekkes opp mot en enkeltperson. Det er altså direkte informasjon om et individ som faller under bestemmelsene i loven. Bestemmelsene i personopplysningsloven har et virkeområde som

[40] Se punkt 1.5.

[41] NOU 1997:19 s.17

inkluderer behandling av personopplysninger som skjer helt eller delvis med elektroniske hjelpemidler, jf. § 3.

Videre i § 8 kommer det frem at personopplysninger bare kan behandles hvis den registrerte har samtykket eller hvis det er fastsatt i lov at det er adgang til slik behandling.

Det er på det rene at det er svært viktig at personopplysningene blir lagret på en sikker måte. I popplyl. § 13 kreves det at den som er behandlingsansvarlig skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet. Det vil si at for eksempel teletilbydere må sørge for at opplysninger som innhentes blir lagret på en sikker måte. At noe er en sikker måte betyr at det må være en viss sikkerhetsklarering i bedriften, og at ikke alle kan få tak i informasjonen. Personopplysninger må ikke havne i andres hender. Det er viktig og påbudt etter loven å gå gjennom planlagte og systematiske tiltak som skal hindre at dette skjer, jf. § 13 første ledd.

Man kan kreve å få innsyn i hvordan den behandlingsansvarlige foretar behandlingen av personopplysningene. Dersom dette også skal gjelde hvis DLD blir implementert vil det si at teletilbyderne må kunne vise til hvordan de lagrer og behandler personopplysningene som blir lagret i form av trafikkdata, lokasjonsdata[42] og lignende informasjon direktivet krever lagret.

I lovens kapittel VI blir bestemmelsene for melde- og konsesjonsplikt lagt frem. I § 31 kommer det frem at den behandlingsansvarlige plikter å gi melding til Datatilsynet før den starter behandling av personopplysninger med elektroniske hjelpemidler, ved opprettelse av manuelt personregister som inneholder sensitive personopplysninger. Man må få tillatelse fra Datatilsynet for å starte opp en slik virksomhet. Denne tillatelsen gis i form av en konsesjon.

[42] Se punkt 1.5 for definisjon.

For å drive med behandling av sensitive opplysninger må man få konsesjon fra Datatilsynet, jf. popplyl. § 33 første ledd. Hva som kan regnes som sensitive opplysninger opplistes i personopplysningsloven § 2. Informasjonen kan være om rase, etnisk bakgrunn, helseforhold, medlem i fagforbud og lignende. Kravet om konsesjon gjelder så lenge personopplysningene ikke er oppgitt uoppfordret. Denne konsesjonens vilkår sikrer at myndigheten får en oversikt over hvem her i landet som lagrer sensitiv informasjon og måten det blir gjort på. Likevel bør det nevnes at konsesjonen for telesektoren er fra 2003, og kunne trengt en oppdatering.

Videre etter EMK[43] art. 8 har man en rett til privatliv og dette gjelder også opplysninger om personen. Datatilsynet har også muligheten til å avgjøre om det skal kreves konsesjon for behandling av andre ikke-sensitive opplysninger. De ser da til personopplysningens art, mengde og formålet med behandlingen, jf. § 33 annet ledd. I dag er det slik at det skal en del til for at det kreves konsesjon for ikke-sensitive personopplysninger, men Datatilsynet har muligheten til å kreve det.

I popplyl. § 34 er det gitt visse retningslinjer for avgjørelsen om konsesjon skal gis. Det kommer frem i bestemmelsen at det skal vurderes om behandlingen av personopplysninger kan medføre ulemper for enkeltindivider som ikke kan avhjelpes etter bestemmelsene i popplyl. kapittel II-V samt § 35. Er det slik at det vil foreligge ulemper, er det nødvendig å foreta en avveining om ”*ulempene blir oppveid av hensyn som taler for behandlingen*”, jf. § 34 annet punktum. Det skal her veies om det likevel er såpass viktig at selskapet får konsesjon for å lagre personopplysninger at det overgår hensynene for personvern. Det kan settes vilkår for konsesjonen etter § 35 og det er med hjemmel i denne paragrafen at det er opprettet konsesjonsbetingelser for teleoperatører spesifikt.

[43] Europeiske menneskerettskommisjon.

2.3.1 Personopplysningsforskriften

Det er et forslag om at det skal kreves konsesjon for å kunne behandle personopplysninger i Lov om behandling av personopplysninger av 14. april 2000 § 31 fjerde ledd, jf. Kgl. res. av 15. desember 2000 § 7-1[44]. Denne bestemmelsen foreslår at det skal kreves konsesjon for å kunne behandle personopplysninger innenfor telesektoren. Det er Datatilsynet som har laget en slik konsesjon for teletilbydere. Denne går ut på behandling av personopplysninger i forhold til kundeadministrasjon, fakturering og gjennomgåelse av tjenester forbundet med abonnentens bruk. Vilkårene er satt er i medhold av popplyl. §§ 34 og 35. Det er i alt 11 vilkår for drift av teletjenester.[45]

2.3.1.1 Konsesjonsvilkår for teletilbydere

Under dette punktet vil jeg gjennomgå de vilkårene som knyttes til konsesjonen til å behandle personopplysninger i telesektoren. Som nevnt under punkt 2.3.1 er det Datatilsynet som har utformet vilkårene i samsvar med popplyl. §§ 34 og 35. Disse vilkårene sørger for at tele- og internettilbyderne følger bestemmelser som skal verne kundenes sensitive opplysninger og bruk av tjenester i henhold til loven.

I det første vilkåret blir det gjort rede for formålet med behandlingen, som skal være behandling av kundeadministrasjon, opplysningstjeneste, fakturering og gjennomføring av tjenester i forbindelse med abonnentens bruk av telenett og samtrafikkavregning. Det er på det rene at personopplysningene kun skal anvendes til disse formålene. Dersom opplysningene skulle brukes til noe annet vil den behandlingsansvarlige måtte sørge for at det skjer i henhold til personopplysningsloven.[46]

---

[44] Personopplysningsforskriften.

[45] Datatilsynet.

[46] All informasjon om konsesjonsvilkårene er fra Datatilsynet.

Det andre vilkåret legger til grunn at det utelukkende skal behandles opplysninger som er nødvendige for gjennomføring og fakturering av tjenesten. Selv om det er mulig for teletilbyderen å lagre annen data, skal det ikke gjøres dersom det ikke er behov for det for faktureringen. Det skal altså ikke lagres informasjon som kan være nyttig til andre deler av bedriften eller for andre, for eksempel politiet.

Det tredje vilkåret definerer hvem som er behandlingsansvarlig. Eksempler fra i dag kan være Telenor, NetCom og lignende selskaper. Videre ligger det daglige ansvaret for behandlingen hos den administrerende direktøren. Det er på det rene at det er den behandlingsansvarlige som må sørge for at bestemmelsene i popplyl. med forskrifter og konsesjonen blir fulgt av selskapet og dets ansatte.

Behandlingens omfang blir omtalt i konsesjonens fjerde vilkår. Konsesjonen omfatter all behandling av personopplysninger som kommer av abonnentens bruk av telenettet. Den gjelder da også for alle typer tjenester. Dersom det er mulig skal også teleoperatøren tilby alternative tjenester der opplysninger om brukeren ikke er nødvendig.

Det femte vilkåret går ut på innsamling av opplysninger. For det første skal opplysningene kun innhentes fra abonnenten direkte og gjennom dens bruk av teletjenester på telenettet. For det andre skal den som er behandlingsansvar kontrollere at de opplysningene som er innsamlet er riktige, komplette og aktuelle for det formålet de er samlet inn for.

Bestemmelser for utlevering av opplysninger er omhandlet i konsesjonens sjette vilkår. Hovedregelen er at personopplysningene ikke må utleveres til utenforstående. Dette hindrer teleoperatøren å selge informasjonen videre til for eksempel telefonselgere. Unntakene blir listet opp i fire forskjellige punkter. I det første punktet blir det gjort rede for at utlevering av personopplysninger kan skje når den opplysningen gjelder har gitt sitt samtykke til det. Det må være en frivillig, uttrykkelig og informert erklæring om at vedkommende godtar utlevering av opplysninger om seg selv.

I det andre punktet blir det lagt til grunn at utlevering av opplysninger kan skje med hjemmel i lov, eller i forskrift med hjemmel i lov.

Personopplysninger kan utleveres som ledd i betalingsinnkreving (inkasso) kommer det frem i det tredje punktet. Og til sist, i det fjerde punktet, blir det slått fast at opplysninger også kan utleveres som ledd i regnskapsbehandling.

Dersom noen benytter seg av utlevering med hjemmel i lov, forskrift eller etter enkeltvedtak fra Datatilsynet skal den opplysningene gjelder få informasjon om dette, så lenge ikke annet følger av lov. Vedkommende skal få oppgitt hva som skal utleveres, til hvilket formål det er og hvem som mottar opplysningene. Et ytterligere unntak gjelder når det er snakk om oppbevaring eller behandling av opplysninger hos et databehandlingsforetak. Det regnes da ikke som utlevering dersom dette skjer på oppdrag fra den behandlingsansvarlige.

Det syvende vilkåret gjelder utlevering gjennom katalogutgivelse og opplysningstjeneste. Her er det listet opp fire vilkår teletilbyderen må følge. På tross av at det ikke foreligger samtykke som nevnt i vilkår 6, kan det utleveres personopplysninger gjennom utgivelse av trykte eller elektroniske kataloger eller opplysningstjenester. Det er opplistet fire punkter for hvordan dette skal foregå.

Opplysningene skal kun brukes til utgivelse av trykte eller elektroniske abonnentkataloger eller opplysningstjenester. Videre skal virksomheten informere abonnenten om oppføring i katalog eller opplysningstjeneste.

Abonnenten skal også få informasjon om at vedkommende kan reservere seg mot å bli oppført. I det tredjepunktet blir det sagt at abonnenten skal gis en rimelig frist for å reservere seg mot oppføringen og dette skal skje kostnadsfritt. Til slutt er det kun de opplysningene som er nødvendig for å identifisere en bestemt abonnent som skal utleveres. Andre opplysninger krever samtykke som nevnt i vilkår 6 punkt 1.

Vilkår åtte går ut på sletting av opplysninger. Dersom det lagres opplysninger som ikke er relevante for formålet, må den behandlingsansvarlige slette eller anonymisere disse. Den som er behandlingsansvarlig skal også av eget tiltak rette, slette eller supplere opplysninger som ikke er korrekte, såfremt det er av betydning for vedkommende opplysningene gjelder. Hvis det skulle ha blitt utlevert feilaktige opplysninger skal den behandlingsansvarlige sørge for at dette ikke får noen konsekvenser for vedkommende opplysningene gjelder. Behandlingsansvarlige skal informere den opplysningene gjelder så raskt som mulig.

Når det kommer til sletting av opplysninger, er det slik at opplysningene kun skal lagres så lenge de benyttes til fakturaformål eller når en eventuell klagefrist utgår. Er det kvartalvis fakturering skal opplysningene slettes senest 5 måneder etter de ble registrerte. Om fakturaen ikke blir betalt eller det er en rettslig tvist om betalingsplikten har behandlingsansvarlige mulighet til å bevare opplysningene inntil kravet er avgjort. Dersom fakturaen er betalt kan det for den perioden lagres navn og adresse på kunden, i tillegg til beløpet som ble betalt.

Lagres det opplysninger som kun er nødvendig for oppkobling eller gjennomføring av tjeneste, må disse opplysningene slettes så fort som mulig etter tjenesten er nedkoblet. Er det opplysninger som må oppbevares for å ha en tilfredsstillende informasjonssikkerhet kan disse oppbevares så lenge det er påkrevet etter reglene i forskriftens kapittel 2 for informasjonssikkerhet ved behandling av personopplysninger § 2-16. Dersom opplysningene kreves lagret i henhold til annen lovgivning er ikke dette punktet til hinder for det. Dette viser hvor strenge regler det er i dag i forhold til lagring og bruk av personopplysninger.

I det niende vilkåret blir det slått fast at registeret ikke skal sammenstilles med andre personregistre, dersom det ikke har annen hjemmel i lov.

Abonnenten skal få en uspesifisert regning etter vilkår 10. Abonnenten kan imidlertid kreve spesifisert regning som viser hvilke numre som ble oppringt i fakturaperioden og lengden på anropet.

Vilkår 11 omhandler fortsatt behandling. Det blir krevet av den behandlingsansvarlige at det skal sendes bekreftelse på at behandlingen av personopplysninger skjer i tråd med konsesjonsvilkårene, til Datatilsynet hvert tredje år.

2.4 Rettstilstanden i dag vedrørende lagring og utlevering av data

Etter det som kommer frem i punkt 2 i oppgaven kan man se at utgangspunktet er at teletilbydere ikke skal lagre trafikkdata eller lignende. Likevel er det et unntak som åpner for lagring av informasjon som skal brukes til fakturering av abonnenten. Det er denne informasjonen politiet kan kreve å få utlevert, dersom de får fritak fra taushetsplikten etter ekomloven. Samfunnet i dag er kanskje ikke klar over i hvor stor grad dette utøves. Derfor har jeg hentet informasjon utlevert fra NetCom og Telenor om henvendelser fra politiet. Dette underbygger argumentet til Kripos som er at dette er spor politiet ofte anvender i etterforskninger.

2.4.1 Statistikk over henvendelser fra politiet om utlevering av data

Både NetCom og Telenor har utlevert statistikk over antall henvendelser fra politiet om utlevering av lagrede data. Statistikken går tilbake til 2004 og man kan derfor se utviklingen i henvendelser fra politiet oppgjennom årene. Jeg velger likevel å fokusere mest på tallene som er fra 2008 og 2009 ettersom disse årene er nærest i tid, og kanskje derfor mer relevant.

Tabell 1 – tall fra NetCom[47]

År	Henvendelser
2005	1288
2006	1501
2007	1513
2008	**1693**
2009	**1730**

Tabell 2 – tall fra Telenor[48]

År	Nummersøk	Basestasjonssøk[49]	Identitet/IMEI
2004	2441	1312	3725
2005	2397	2040	1402
2006	2624	1924	2085
2007	2196	2534	2438
2008	**3321**	**2561**	**2181**
2009 (9 mnd.)	**2571**	**2067**	**1921**

Etter denne statistikken kan man se at politiet i mange tilfeller søker om å få innsyn i trafikkdata og lokasjonsdata. Det er altså ikke slik at politiet ikke har noen mulighet i dag til å få tak i slik type data som skal lagres etter DLD. Selv om det ikke foreligger noen lagringsplikt for teleoperatørene slik reglene er utformet i dag, er det på det rene at det lagres en mengde data likevel med tanke på fakturering. Det er altså ingen tvil om at politiet bruker muligheten for å skaffe seg bevis i form av trafikk- og lokasjonsdata i dag, selv om DLD ikke er implementert her i landet. Det er viktig å legge merke til at politiet

[47] Tall hentet fra rapport skrevet av Svein Willassen (2010).

[48] Svein Willassen (2010).

[49] Se punk 1.5 om lokasjonsdata.

selv ikke fører noen statistikk over hvor ofte de har hatt bruk for trafikkdataen de har fått utlevert. Derfor er det vanskelig å vurdere hvor nyttig dataen er.

Når det gjelder statistikk for 2010 har Post- og teletilsynet (PT) ført en nøye oversikt fra og med 1.1.2010.[50] Det kommer frem i PTs høringssvar til departementet at det i første kvartal av 2010 var 616 begjæringer fra politiet om fritak for taushetsplikten. Disse begjæringene gikk ut på trafikkdata, basestasjonssøk og PUK-koder fra telefoni. Av disse tilfellene var det 469 begjæringer som fikk fritak for taushetsplikten, altså 76%. PT har dokumentert at av de 469 begjæringene, gjaldt 73% av de trafikkdata, 15% basestasjonssøk og 12% utlevering av PUK-koder.

2.4.2 Nærmere om trafikkdata

Det er interessant å se hvor ofte politiet ønsker å anvende trafikkfata. Etter PTs høringsvar til departementet var det snakk om utlevering av trafikkdata for til sammen 888 telefonnummer for personer som var mistenkte eller siktede i saker under etterforskning hos politiet. Når det gjelder utlevering av trafikkdata for fornærmede i saker, ble det kun gitt fritak for til sammen 18 telefonnummer. Det har blitt registrert hos PT at politiet fikk innvilget tilgang til trafikkdata som er lagret i maksimal lovlig periode som er 3-5 måneder, avhengig av hvilken tilbyder det er snakk om, i 78% av tilfellene. Videre i 22% av tilfellene ble det gitt innvilgelse for en begrenset periode, som var mindre enn maksimal lovlig lagringstid. Grunnen for dette var fordi politiet selv kun hadde begjæret å få tilgang for en kortere periode, eller at PT begrenset tilgang til en viss periode av annen grunn.

2.4.3 Nærmere om basestasjonssøk

Hos PT ble det i første kvartal av 2010 registrert fritak fra taushetsplikten for basestasjonssøk for 101 geografiske adresser og totalt 545 timer. I det fritaket hvor det ble

[50] Tallene baseres på høringssvaret fra Post- og teletilsynet (2010).

gitt kortest tid, var det 3 minutter av basestasjonssøk som ble utlevert til politiet, og 60 timer i det lengste søket.

2.4.4 Nærmere om PUK-koder

Det ble gitt fritak for utlevering av PUK-koder for 118 telefonnummer. Disse numrene ble anvendt av person(er) som var siktet eller mistenkt i etterforskning hos politiet. Det ble videre gitt fritak for PUK-koder for 4 telefonnummer som tilhørte fornærmede i etterforskningen.

3 Datalagringsdirektivet

3.1 Generelt

Traktaten om den Europeiske Union oppsto først ved Maastrichavtalen av 1992. Under denne traktaten er det opplistet tre samarbeidsområder, også kjent som tre pilarer. Den første pilaren er det tradisjonelle EF[51]-samarbeidet, den andre pilaren er samarbeid om utenriks- og sikkerhetspolitikk og den tredje pilaren er samarbeidet om rettslige og indre anliggender.[52]

Dette direktivet er fremsatt under den første pilaren, med hjemmel i den daværende EF-traktaten artikkel 95, nå er det traktaten om den europeiske unions funksjonsområde (TEUF) artikkel 114. Ved å forankre direktivet i denne hjemmelen tilsier det at også er relevant for stater som er medlem av EØS-avtalen. Det har imidlertid vært diskusjoner om direktivet er relevant for oss som EØS-stat. I vurderingen av om DLD er relevant for EØS-

[51] Traktaten om opprettelse av det Europeiske Fellesskap, EFT.

[52] EØS-rett. Sejersted, Fredrik, (2005) s. 22.

avtalen tar man gjerne utgangspunkt i om innholdet i direktivet faller naturlig innenfor EØS-avtalens virkeområde. Det finnes argumenter både for og mot en slik relevans. Et argument som taler for er som tidligere nevnt at det er hjemlet i første pilar og at det er snakk om å regulere ekomsektoren, altså harmonering av lovverk i Europa. Et argument mot EØS-relevans er at det i all hovedsak er snakk om kriminalitetsbekjempelse. Om direktivet kan hjemles i EØS-avtalen skal ikke jeg avgjøre i oppgaven og jeg legger heretter til grunn at DLD er relevant for Norge.

3.2 Hvordan implementeres et direktiv fra EU

En eventuell implementering av DLD i norsk rett vil være som følge av EØS-avtalen. Denne avtalen er en folkerettslig traktat og det er da et alminnelig krav om at traktater skal gjennomføres lojalt i nasjonal rett.[53] I EØS art. 3 er det en generell forpliktelse til å gjennomføre EØS-retten i nasjonal rett på korrekt måte. Når det gjelder gjennomføring av direktiver er det artikkel 7 som regulerer dette. Her kommer det frem at de nasjonale myndighetene står fritt til å velge form og midler, såfremt det materielle innhold forblir det samme som direktivets innhold. Det er imidlertid er krav om at rettstilstanden skal være klar og utvetydig og gi borgerne i samfunnet mulighet til å forutsi sin rettsstilling. Nasjonale myndigheter kan selv velge om et direktiv skal gjennomføres ved lov eller forskrift.

3.2.1 Gjennomføring i norsk rett

I Norge har man to forskjellige måter å gjennomføre folkerett. Det er en henvisningsteknikk og en gjengivelsesteknikk. Dersom henvisning brukt blir det vedtatt en paragraf i norsk rett som henviser til traktaten og slår fast at denne skal gjelde som norsk lov.[54] Blir denne metoden brukt har man en fordel ved at man ikke har behov for å

[53] EØS-rett. Sejersted, Fredrik (2005) s. 185.

[54] EØS-rett. Sejersted, Fredrik (2005) s. 188

oversette direktivet eller traktaten, og på den måten er det enklere å holde seg lojal mot originalteksten.

Er det slik at gjengivelsesteknikken blir brukt må man skrive om den folkerettslige teksten og lage den i samme utseende som en annen, vanlig norsk lovtekst. Dette blir da i form av en ny lov eller forskrift, eller som del av en allerede eksisterende lov. På denne måten blir folkeretten en mer naturlig del av norsk rett, men det er en fare for at oversettelsen er ugrundig og ikke betyr det samme på norsk som originalspråket. Begge metoder blir brukt i dag.

3.3 Om datalagringsdirektivet (DLD)

Datalagringsdirektivet går ut på å lagre data fremkommet ved bruk av elektroniske kommunikasjonsmidler, nærmere bestemt trafikkdata[55] og lokasjonsdata[56], fra alle teleoperatører i landet. Formålet med direktivet er å harmonisere lovgivning knyttet til lagring av data i EU- og EØS-stater. Hensikten bak direktivet er at bestemmelsene skal være med på å avdekke, etterforske og rettsforfølge alvorlig kriminalitet. Det har vært diskusjoner om denne type data kan være med på å oppklare saker. Politiet selv hevder at de har stor bruk for trafikk- og lokasjonsdata når det kommer til etterforskning og som bevis i retten. Tabell 1 og 2 underbygger også dette argumentet, hvor man kan se hvor mye politiet søker om unntak fra taushetsplikten i e-komloven, i alle fall at denne type data ofte kreves utlevert. Akkurat hva som regnes som ”alvorlig kriminalitet” er det medlemsstaten selv som skal definere. Men man må kunne anta at definisjonen av alvorlig kriminalitet skal føres opp mot hensikten bak direktivet. Det har ofte blitt sammenlignes med terrorhandlinger i media.

Dette direktivet innebærer lagring av data som kan spore og identifisere kilden til den elektroniske kommunikasjonen som ble anvendt av en bruker. I dag plikter ikke

[55] Se punkt 1.5 for forklaring

[56] Se punkt 1.5 for forklaring

teleoperatørene å lagre data fra abonnentenes bruk. Det er imidlertid gitt adgang til å lagre slik data som er nødvendig for faktureringsbehov, med hjemmel i e-koml. § 2-7. Lovens § 2-8 pålegger også teletilbyderen å holde det åpnet for spesiell lovbestemt tilgang til lagret data. Det er verdt å legge merke til at en eventuell implementering av DLD vil endre tilstanden fra lagringsadgang til lagringsplikt for teleoperatørene. Også hensynet bak lagringen vil endres fra faktureringsbehov til bekjempelse av alvorlig kriminalitet. Hva som er konsekvensen av at staten skal pålegge tele- og internettilbyderne en slik byrde er også et interessant spørsmål.

Det er på det rene at implementering av direktivet vil vesentlig endre de bestemmelsene som foreligger i dag når det gjelder data teleoperatørene kan og skal lagre. I korte trekk vil teleoperatørene måtte lagre data fra minimum 6 måneder til maksimum 2 år og dataen vil lagres med et helt annet formål enn før. Det er opp til hvert enkelt medlemsland å sikre at prinsipper for datasikkerhet som direktivet fremmer blir overholdt i lagringsprosessen. Medlemslandet skal også selv opprette en eller flere offentlige grupper som skal ha ansvaret for sikkerheten rundt lagringen. Denne gruppen skal jevnlig føre oversikt over lagring og utlevering av lagret data, jf. DLD artikkel 9.

Videre kreves det også at det skal føres statistikk over hvor mange saker politiet har krevet informasjon om lagret data, jf. direktivets artikkel 10. Da må også datoen for lagringen oppgis, samt datoen for etterspørselen. Dersom det er forespørsler om data som ikke ble møtt skal dette også oppgis i statistikken. Man ser her at det legges opp til et mer nøye system rundt lagring og utlevering av informasjon. Som det har kommet frem i oppgaven er det slik at teleoperatørene har adgang til å lagre visse type data til formål for fakturering, og mye tyder på at forskjellen mellom hva som allerede lagres i dag og hva som kreves lagret etter DLD ikke er så betydelig som man kan tro. Det er imidlertid rutinene og bestemmelsene rundt som vil få en gjennomgang. Personvernmessig er det ønskelig og nødvendig at slike regler er klare og tydelig, både for teleoperatørene og borgerne i samfunnet. Man er likevel ikke avhengig av implementering av DLD for å gjøre dette. Som man ser under gjeldende rett får politiet adgang til å hente ut en rekke data i dag.

Når det kommer til konsekvenser av implementering kan man regne med at det vil bli utvidede tilsynsoppgaver for Post- og teletilsynet og Datatilsynet. DLD kan også gi økonomiske konsekvenser for teletilbydere som plikter å lagre dataen, så lenge dette ikke blir finansiert av staten. Men dette er ikke de eneste konsekvensene. Det kan også føles som en slags overvåkning av menneskene i samfunnet. Likevel må det også vektlegges at det er tale om informasjon som politiet har nytte av i sammenheng med etterforskning av alvorlig kriminalitet og som bevis i retten.

Det er videre blant annet tre viktige hensyn som må vurderes. For det første må man se på justissektorens behov for et bedre verktøy for kriminalitetsbekjempelse.[57] Er det slik at politiet er avhengig av utvidet lagringsplikt av data for å kunne oppklare saker? For det andre må man se på konsekvensene det har for personvernet. Det er klart at borgerne i samfunnet legger igjen en rekke spor og sensitiv informasjon over internett og telefoni. At politiet skal få en enklere og utvidet tilgang til dette vil tilsi at personvernet blir betydelig svekker. Og til sist er det nødvendig å ta hensyn til konkurransen på telemarkedet. Lagringsplikten vil øke kravene til sikkerhet, rutiner og lagringsplass. I Norge har man mange små operatører, som kanskje ikke vil kunne etterkomme kravene, og dermed blir det kun de største operatørene som overlever implementeringen.

3.4 Hva skal lagres

I direktivets artikkel 5 er det opplistet hvilke data som skal lagres etter bestemmelsene i DLD. Hver medlemsstat plikter å sikre at data som er nødvendig for å spore opp og identifisere kilden til kommunikasjonen blir lagret. Det er en meget omfattende liste som regulerer hva som skal lagres. For ordens skyld har jeg valgt å dele opp disse kategoriene i egne underoverskrifter for at det skal være enklere å sette seg inn i de forskjellige data. Etter samtaler med NetCom og Telenor har det kommet frem at kravene i DLD er diffuse.

[57] www.jasiden.no

Det betyr at det til en viss grad er vanskelig for leverandørene å vite akkurat hva direktivet krever.

3.4.1 Fastnettelefoni og mobiltelefoni

Ved bruk av fastnettelefoni og mobiltelefoni skal nummeret som foretar oppringningen (A-nummeret) lagres, samt navn og adresse til den registrerte brukeren[58]. B-nummeret(ene) skal også lagres, det er altså nummeret A-nummeret ringer opp. Dette nummeret skal lagres selv om oppringningen skjer gjennom viderekobling eller overføring. Et typisk eksempel på dette er å ringe opplysningen eller lignende tjenester. Navn og adresse som er lagret på B-nummerets abonnement skal også lagres. Dato og klokkeslett for kommunikasjonens begynnelse og slutt skal lagres. Også den anvendte telefontjeneste skal lagres.

Det skal også lagres data for å identifisere hva slags utstyr brukeren anvender. For fastnettelefoni gjelder det kun A-nummeret og B-nummeret. Kravene blir noe mer omfattende for bruk av mobiltelefoni. Da skal også A-, og B-nummeret lagres, samt begge abonnenters IMSI-nummer og IMEI-nummer. Dette er for å kunne identifisere brukeren og dens utstyr, dette er i trå med direktivet. Har det blitt brukt forhåndsbetalte, anonyme tjenester skal dato og tidspunkt for første aktivering av tjenesten lagres, i tillegg til celle-IDen og hvor aktiveringen ble foretatt.

3.4.2 Internettilgang, e-post og telefoni via internett

Ved bruk av internett, e-post og telefoni via internett skal den tildelte brukeridentiteten lagres. Brukeridentifikasjon og telefonnummer tildelt all kommunikasjon i det offentlige telenettet skal lagres. Navn og adresse på den abonnent eller registrerte brukeren av IP-adresse og brukeridentitet eller telefonnummer var tildelt på kommunikasjonstidspunktet.

[58] Se punkt 1.5 for definisjon av tekniske termer

Det skal lagres data for å fastslå kommunikasjonens bestemmelsessted, altså lokasjonsdata[59]. Videre skal brukeridentiteten eller telefonnummeret på mottakeren som internettanropet er rettet til også lagres. Navnet og adressen på abonnenten eller den registrerte brukers brukeridentitet på mottakertidspunktet av kommunikasjonen. Det må også lagres data som kan angi kommunikasjonens dato, klokkeslett og varighet.

Nærmere skal det lagres dato og klokkeslett for inn- og utlogging av internettjenester basert på en bestemt tidssone og den dynamiske eller statiske IP-adressen som teleoperatøren av internettadgangen har tildelt kommunikasjonen, samt brukeridentiteten på abonnenten eller den registrerte brukeren. Det skal videre lagres data som kan angi dato og klokkeslett for inn- og utlogging av e-posttjeneste og telefonitjenester på internett basert på en bestemt tidssone. Det skal videre lagres hvilken internettjeneste det er anvendt, typisk hvilken internettilbyder det er brukt, som Get, Nextgentel og lignende selskaper.

Også for denne type kommunikasjon skal det lagres data som kan avsløre hva slags kommunikasjonsutstyr brukeren anvender, samme som IMSI-nummer og IMEI-nummer ved mobiltelefoni. Det skal for det første lagres A-nummeret med tanke på dial-up adgangen. Den digitale abonnentlinje (DSL) eller annet endepunkt for kommunikasjonens opprinnelse. Dataen skal også kunne lokalisere mobilt utstyr. Dette gjøres ved at lokaliseringskoden (celle-ID) ved kommunikasjonens begynnelse lagres, samt data med henvisning til celle-IDens geografiske lokalisering i den periode kommunikasjonen lagres.

Det kommer uttrykkelig frem i direktivets artikkel 5 andre ledd at innholdsdata ikke kan lagres med hjemmel i dette direktivet.

[59] Se punkt 1.5 for forklaring

3.4.3 Hva omfattes ikke av DLD

Samferdselsdepartementet presiserte i høringsnotatet at innholdet i trafikk- og lokasjonsdataen ikke skal lagres. Innholdsdataen[60] skal med andre ord ikke lagres etter DLD. Heller ikke data som kan avsløre innholdet i kommunikasjonen skal lagres. Departementet mener med dette at det ikke skal lagres data som viser eller tilkjennegir kommunikasjonens innhold. Hvilken internettside brukeren besøker skal for eksempel ikke lagres. Heller ikke innholdet i en SMS/MMS, eller innholdet i en e-post skal lagres.

Når det benyttes en applikasjon som ikke er definert som offentlige ekomtjenester skal ikke data i tilknytning kommunikasjonen lagres. Det betyr tjenester som ikke er regnet som offentlige ekomtjenester, ikke skal falle inn under DLDs lagringsplikt. Det er nærmere bestemt tjenester som ikke er definert i ekomloven. Et eksempel som har blitt mye brukt i media, og i høringsnotatet er applikasjonen Skype. Dette er en taletjeneste som gjør det mulig å ringe via internett til andre med Skype-applikasjonen, et telefonnummer og sende multimediameldinger og tekstmeldinger. Det blir lagt til grunn i høringsnotatetat at bruk av slike typer tjenester ikke gir internettleverandøren noen mulighet til å identifisere hvilke tjenester som benyttes og hvem som kommuniserer med hvem. Brukeren selv kan imidlertid se hvem og hvor lenge den har kommunisert med de siste 12 månedene.

Det blir videre slått fast i høringsnotatet at politiet må bruke såkalt sanntids kommunikasjonskontroll for å kunne identifisere hvilke tjenester som anvendes og hvem som kommuniserer med hvem.[61] Det er kun IP-telefoni og epost tjenester som er operatørbasert som skal lagres, ikke de samme tjenestene som er nettbaserte. Bakgrunnen for dette er at direktivet kun gjelder tele- og internettleverandører som direkte er tilknyttet landet eller medlemsstaten. Skype er ikke registrert som teletilbyder i Norge, og heller ikke definert i ekomloven og vil derfor ikke rammes av direktivet. Det er altså definisjonen i

[60] Se punkt 1.5 for forklaring.

[61] Høringsnotat, Samferdselsdepartementet s. 32

dokumentet som utelukker at Skype, Google GMail og lignende tjenester skal lagres etter DLDs plikt.[62] Hvorfor nettopp dette har blitt bestemt har ikke kommet klart frem.

Etter dette må man kunne legge til grunn at internettbaserte e-posttjenester og kommunikasjonstjenester ikke skal falle inn under datalagringsdirektivet.

Videre er det også verdt å merke seg at flere epost tjenester er lokalisert utenfor Europa, og faller av denne grunn utenfor datalagringsdirektivets bestemmelser. De største på markedet er Yahoo Mail, Google GMail og Microsoft Hotmail. Det er på det rene at alle disse tre befinner seg på servere plassert utenfor Europa. I Norge vil DLD kun omfatte sending og mottak av eposter gjennom norske leverandører.

Det kan etter dette virke som det er måter man kan ”omgå” direktivets bestemmelser på. Bakgrunnen for dette er kanskje at EU ikke kan lage et direktiv som vil gjelde utenfor Europa og medlemsstatene i EU/EØS. Videre er det verdt å merke seg at det finnes tilsvarende bestemmelser også i USA, hvor de tidligere nevnt eposttjenestene har lokalisert sine servere. I 1992 ble foreslått to forskjellige modeller for lagring av data der. I den første modellen ble det foreslått at IP-adressen som ble tildelt en kunde skulle lagres.[63] I den andre modellen ble det foreslått at det skulle lagres hvilke telefonnummer som ble oppringt, innholdet i besøkte websider og mottakere av e-postmeldinger. Denne informasjonen skulle lagres av internettleverandøren på ubestemt tid. Det er på det rene at dette andre forslaget er mest likt det datalagringsdirektivet fra EU. I 2009 slo ”Stopping Adults Facilitating the Exploitation of Today’s Youth Act” fast at tilbydere av internett og tilbydere av eksterne databehandlingstjenester var pliktig å lagre ”all records or other information pertaining to the identity of a user of a temporarily assigned network address the service assigns to that user”.[64] [65] Det vil si at tilbyderne måtte lagre all data og

[62] janhenrik.com

[63] cnet News article

[64] crn.com

[65] cnet News

informasjon som kunne spore opp identiteten til brukeren av nettverket. All data må lagres i minimum to år ifølge loven. På denne måten vil mye av bruken lagres uavhengig av EUs datalagringsdirektiv.

3.5 Lagringstid

Etter bestemmelsene som fremkommer i DLD blir det ikke satt noen fast lagringstid. Det er slik at det er opp til hver enkelt medlemsstat å avgjøre hvor lenge dataen skal lagres. Det oppgis imidlertid visse rammer som statene må holde seg innenfor i direktivets artikkel 6. Her blir det lagt til grunn at dataen skal lagres i minimum 6 måneder og opp til maksimum 2 år. Hvor denne tidsrammen stammer fra kommer ikke klart frem, og heller ikke hensynet bak at staten selv kan velge tidsrommet. I dag har teleoperatørene mulighet til å lagre data i opp til 5 måneder etter Datatilsynets konsesjon, med unntak av IP-adresser som må slettes etter 3 uker, som følge av Datatilsynets regulering i 2009.

3.5.1 Krav til lagring av data

I artikkel 8 blir det slått fast at medlemsstatene skal lagre data etter direktivet på en slik måte at dataen og opplysningene kan fremsettes til statens kompetente myndigheter uten unødig forsinkelse. Det er altså ikke satt opp noen krav til hvordan teletilbyderne skal lagre all den sensitive informasjonen som de vil pliktes å gjøre etter dette direktivet. Det må være grunn til å anta at å lagre slik data på en sikker måte vil koste teleoperatørene betydelige summer. Man kan spørre seg om hvem som skal ta denne kostnaden. Skal det være en forutsetning for å kunne drive med telefoni og internett, at man kan sørge for sikker og effektiv lagring av en mengde data i opp til to år og at det dermed blir teleoperatøren selv som må ta kostnaden? Eller burde staten dekke dette? I NetComs høringssvar til høringsnotatet[66] våren 2010 peker de på at denne kostnaden bør dekkes av myndighetene.

[66] Høringsnotat fra 8.1.2010 (Samferdselsdepartementet, Justisdepartementet og Fornyings- og administrasjons- og kirkedepartementet)

Deres argumenter er at en slik omfattende lagring av data ikke tilfører deres selskap noe merverdi, og det kun er til nytte for myndighetene/politiet.

3.5.2 Hvem skal ha tilgang på lagret data

Det er ingen konkret bestemmelse i DLD som avgjør hvem som skal ha tilgang på den lagrede data. Det står imidlertid i art. 4 at dataen ”*kun udleveres til de kompetente nationale myndigheter i særlige sager og i overnsstemmelse med national lovgivning*”. Etter dette kan man legge til grunn at det er politiet som er den kompetente myndigheten her i landet. Politiet har med hjemmel i straffeprosessloven adgang til å innhente informasjon om mistenkte i saker. Se mer om dette under gjeldende rett, punkt 2 i oppgaven.

3.5.3 Hva lagres i dag

Det er på det rene at det også lagres data i dag som definerer forbrukerens bruk av telefoni. A-nummeret blir lagret ved bruk av fasttelefon og mobiltelefon, men dette er kun for bruk ved fakturering. Teleoperatøren må ha fått godkjent konsesjon fra datatilsynet, og dataen kan lagres i 3-5 måneder avhengig av hvor lang faktureringsperioden er. Også navn og adresse registrert på dette nummeret vil bli lagret. Dette er data som hjelper med å spore opp og identifisere kilden til en kommunikasjon. Det kan også være aktuelt å lagre identiteten til den abonnenten som anvender IP-telefoni.

Med andre ord lagres det også en mengde trafikkdata og lokasjonsdata i dag, uten at det har vært noen større diskusjon rundt dette. En stor forskjell er imidlertid hensynet bak lagringen. I dag lagres dataen for faktureringens del. Men selv om det er hensynet bak lagringen, betyr ikke det at politiet ikke få uthentet slik informasjon.

For at teleoperatørene skal kunne sette opp en nøyaktig faktura må de lagre trafikkdata, som hvilket nummer som har ringt hvem, og hvor lenge denne samtalen foregikk. Det er også slik at noen operatører opererer med forskjellige priser for samtaler til forskjellige nettverk. Da må det også kunne identifiseres hvilket nettverk og annen informasjon om B-

nummeret, altså det nummeret som blir oppringt. For å lokalisere en mobiltelefon er det vanlig at politiet innhenter oversikt over basestasjonssøk. Denne dataen viser hvilke nummer som brukte vedkommende basestasjon for kommunikasjon med telesentralen, og angir dermed i hvilket område telefonen befant seg. Det er med andre ord en betydelig forskjell på hva som er formålet bak det som lagres i dag og hva som skal lagres etter DLD, men selve innholdet forblir relativt likt. Man må ta høyde for at det kan bli vedtatt lagring i 2 år, og dette utgjør en vesentlig forskjell fra dagens lagringslengde. Det har ennå ikke blitt vedtatt hvor lang lagringstiden eventuelt skal være i Norge.

4 Synspunkter på datalagringsdirektivet

4.1 Kripos

Kripos er den nasjonale enheten vi har i Norge som arbeider for bekjempelse av organisert og annen alvorlig kriminalitet. Dette er en politietat under justis- og politidepartementet.[67] I denne sammenheng har jeg funnet det nyttig å finne ut hvilke synspunkter og meninger Kripos har om DLD. Kripos er en av flere enheter som anvender trafikkdata og lignende spor i dag og det er på det rene at Kripos stiller seg positive til datalagringsdirektivet.

Kripos mener at lagring av data (DLD) er et meget viktig politisk og juridisk tema som ikke har fått en grundig nok gjennomgang. Slik Kripos ser det virker det som den negative omtalen i media har fått folket og politikere til å konkludere på forhånd og finne argumentene dernest. Diskusjonen om DLD er på ingen måte svart-hvitt. Det er mange aspekter som må vurderes opp mot hverandre og konsekvensene av avgjørelser som blir tatt. Det må vurderes hvor viktig det er at politiet får dataen som lagres gjennom DLD for å oppklare saker. Implementering av DLD har stor betydning for politiet og deres arbeid.

[67] www.politi.no

Politiet jobber stadig med å finne ut av hvordan kriminelle kommuniserer med hverandre. Hvis det ikke skulle bli mulig å innhente datatrafikk vil de få konsekvenser for dette arbeidet.[68]

Kripos argumenterer for at datalagringsdirektivet faktisk kan føre til et bedret personvern. Det er ikke slik at man må implementere EUs datalagringsdirektiv slik det er utformet i dag. Man har her muligheten til å gjennomgå behovet for slik lovgivning i Norge og deretter foreslå oppdatering av nåværende lovgivning. Mange organisasjoner og politikere argumenterer med at det vil være stor fare for spredning av data dersom denne ikke lagres på sikker nok måte. Dette er også en fare i dag. Det finnes mange teletilbydere som ikke anses for å være seriøse, og implementeringen av DLD vil kunne luke ut disse aktørene og gjøre det strengere å få konsesjon for lagring av data. Man vil få større grad av personvern enn det er i dag. Det vil bli større bevissthet ved lagring av dataen og det vil kanskje være mulig å få en sentralisert lagringsplass.

Ifølge politiinspektør Reidar Bruusgaard er innhenting av trafikkdata ofte første skritt politiet tar, før tyngre metoder som rom- og/eller telefonavlytting blir aktuelle.[69] Han mener at man kan på denne måten sjekke folk inn eller ut av saker.

4.1.1 Personvern

En annen problemstilling Kripos syns har fått for liten fokus er personvern versus personvern. Man kan spørre seg om hvem sitt personvern det er snakk om. I overgrepssaker som foregår over internett blir den mindreåriges personvern krenket. Det blir vanskelig for politiet å beskytte fornærmedes personvern når regelverket ikke sikrer sporene overgriperen legger igjen etter seg. Det er vanskelig å etterforske saker hvor IP-adressen spiller en avgjørende rolle for identifisering av abonnenten, ettersom disse skal slettes fra tilbyderen etter tre uker.

---

[68] Intervju med politiinspektør Reidar Bruusgaard

[69] Fra møtet med Politiinspektør Bruusgaard.

Et annet argument Kripos er kritiske til er det at kriminelle vil finne andre måter å kommunisere på. Det er på det rene at ikke alle etterforskningsmetoder fungerer i dag, men man kan heller ikke slutte å bruke de på grunnlag av at de kun fungerer 8 av 10 ganger. Politiet trenger nye verktøy for å følge med i den generelle utviklingen.

Mange har uttrykt skepsis over om dataen vil bli lagret sikkert nok. I dag finnes det flere register med sensitiv informasjon, som for eksempel DNA-register og register over fingeravtrykk. Det er nødvendig å kryptere informasjonen slik at uvedkommende eller ansatte hos teletilbyderen ikke får anledning til å skaffe informasjon om abonnenter og hvem den kontakter, mener Kripos. Når man ser at andre registre fungerer i dag, må man kunne anta at også et register med trafikk- og lokasjonsdata vil fungere.

4.1.2 Utviklingen i samfunnet krever oppdatering av etterforskningsmetoder

Det har vært en stor utvikling i bruk av internett og elektronikk de siste 10 årene. Og i den sammenheng er det på det rene at politiet må fornye sine arbeidsmetoder for å fortsatt kunne forebygge og etterforske kriminalitet. Kripos mener at DLD vil hjelpe samfunnet med å beskytte seg selv ved at lagring av trafikk- og lokasjonsdata vil hjelpe betydelig i deres etterforskninger. Når verden og kriminaliseringen forandrer seg vil det alltid være nødvendig å se på hvilke etterforskningsmetoder politiet har. Samtidig vil DLD være med på å beskytte samfunnet selv. Det er ikke politiet som vil ha informasjonen for egen del, men den er til stor hjelp ved oppklaring av kriminelle handlinger.

4.1.3 Samarbeid i politiet på tross av landegrenser

Videre er det et vesentlig poeng at vi i Norge så godt det går vil samarbeide med politi fra andre land i Europa. Kripos kan for eksempel få et tips fra politiet i utlandet om at den og den IP-adressen bedriver seksuelle overgrep på barn. Hvem som sitter bak en IP-adresse blir lagret hos teletilbyderen i 3 uker og så blir det slettet. For at politiet skal kunne få greie på hvem som bedriver overgrep på barn, må handlingen, tipset og etterforskningen foregå

innenfor tre uker. Det er klart at det er svært problematisk og urealistisk. Man kan si at det blir et slags rettstomt rom når lovgivningen forholder seg slik. Kripos mener at politiet må være mer synlig på internett, i den grad det er mulig. Det er viktig at også Norge kan samarbeide med annet politi internasjonalt, spesielt innen Europa. Det ville vært uheldig om kriminelle kunne såkalt shoppe regelverk og begå den kriminelle handlingen hvor det vil være vanskeligere å spore opp vedkommende.

4.1.4 Konsekvenser for politiet

I diskusjonen om DLD må man se på og vurdere konsekvensene av at et slikt direktiv eller lignende lovgivning ikke blir gitt. Det er svært viktig for politiet i deres arbeid om å bekjempe kriminalitet. Det trengs ikke å innhente data fra en mistenkts mobiltelefon når det er snakk om et sykkeltyveri. Det skal ikke være slik at politiet skal gå inn og se hvilke mobiltelefoner som befant seg i det området det tidspunktet sykkelen ble borte. Det må være mulig å sette en grense for når man skal innhente data- og lokasjonstrafikk, for eksempel ut fra strafferammen på handlingen.

Det at det i dag ikke er noen lagringsplikt for teleoperatørene gjør at det er usikkert for fremtiden om de vil fortsette å gjøre det dersom det ikke er behov for det i forhold til fakturering. Etter personopplysningsloven og konsesjonen med hjemmel i den loven skal det heller ikke lagres data dersom det ikke er behov for det i dag. Det er grunn til å tro at teleoperatørene mest sannsynlig vil gå over til fastprisfakturering, noe som resulterer i at det ikke er nødvendig for dem å lagre trafikkdataen til abonnentene. Og et spørsmål Kripos da stiller er om et så viktig element, gjerne det som virker som inngangsbilletten i flere saker, være opp til direktøren i teleselskapet, eller skal det være lovgivning som er tuftet på samfunnsmessige vurderinger? Politiinspektør Bruusgaard mener at i slike tilfeller må de kommersielle interessene være sekundære.[70] Det er imidlertid ikke sikkert hva som vil lagres ved fastpris. Det blir nevnt hos NetCom at de kan se for seg å lagre mindre med

[70] Fra samtale med Bruusgaard hos Kripos.

tiden, mens Telenor og Tele2 hevder at de fortsatt vil ha bruk for å lagre data, ettersom fastprisavtaler alltid vil ha en øvrig grense.

4.2 NetCom

NetCom er en av landets største teletilbyder og en implementering av DLD vil ha direkte innvirkninger på deres daglig drift. Derfor så jeg det som nyttig og ha en samtale med en av deres ansatte, Randi Punsvik.

NetCom er den andre største teletilbyderen i Norge, og har av den grunn skrevet inn et høringssvar på departementets høringsnotat ettersom selskapet og deres kunder vil bli påvirket av en eventuell implementering av DLD. Innføring av et slikt direktiv er først og fremst politisk, men NetCom ønsker å ivareta personvernet til deres kunder og har av den grunn engasjert seg i debatten.

NetCom mener at det positivt at befolkningen engasjerer seg mer for hvilke metoder politiet bruker for oppklaring av saker. Det er på det rene at det i dag lagres trafikkdata og lokasjonsdata som kan avsløre identiteten til en abonnent. NetCom lagrer først og fremst data for egen bruk, altså faktureringshensyn, men denne informasjonen kommer også godt med når politiet ønsker å få innsyn for oppklaring og etterforskning av saker. Hos NetCom er det per i dag to ansatte som utelukkende jobber med å ha kontakt med politiet og utlevere den informasjonen de krever fritatt fra taushetsplikten. For å få tilgang til slik informasjon må politiet, som gjennomgått over, søke om opphevelse av taushetsplikten via post- og teletilsynet.

Slik jeg forstod det er det hvem som helst i et politidistrikt som kan kreve å få informasjon utlevert etter at taushetsplikten er opphevet for et telefonnummeret eller lignende. Dette kan tyde på at profesjonaliteten blir svekket. Man kan ikke regne med at alle i politiet skal ha inngående kunnskap om det tekniske rundt de lagrede data, og det er et moment som taler for at det kanskje burde vært et eget utvalg eller enhet som tok seg av begjæringene

om utlevering av trafikk- og lokasjonsdata. Dette er en aktuell problemstilling i dag og aktualiteten vil bare øke ved en implementering av DLD.

4.2.1 Konsekvenser av en eventuell implementering av DLD

NetCom mener klart at det vil ha konsekvenser for bedriften om DLD skal implementeres i Norge. For det første er det et spørsmål om hvordan dataen skal lagres. Alternativene er at NetCom bruker to databaser, en med informasjon for fakturering og en med informasjon til politiet. Ellers kan alt lagres i en felles database, og det er helst slik de ser for seg at det vil fungere best. Det har imidlertid vært diskusjoner om det skal være slik at all data politiet har adgang til å få skal lagres i en felles database for alle teleoperatører. Om det skulle bli aktuelt er det viktig å legge vekt på at informasjon om norske borgere som anvender elektronikk med telefonsignaler er lagret på ett og samme sted. Man kan argumentere med at dette er risikabelt, ettersom det er sensitiv informasjon som lagres.

NetCom mener videre at kravene i DLD må presiseres og konkretiseres nærmere. Det må komme klart frem av direktivet hva som skal lagres.

Det kunne også diskuteres om det er riktig at det er post- og teletilsynet som skal avgjøre om taushetsplikten skal oppheves. Når det er spørsmål om å utlevere slik type informasjon kunne det med fordel diskuteres om ikke domstolen skulle avgjort det.

En annen konsekvens av implementering er svekkelse av konkurransen på området. I dag finnes det 90 operatører som tilbyr bruk av fasttelefon, 30 operatører for mobiltelefoni og 167 operatører som tilbyr internett.[71] Det er på det rene at NetCom og Telenor har store deler av disse markedene. Det kan bli vanskelig for mindre tilbydere å klare å lagre dataen som DLD krever og i det tidsrommet regjeringen vil sette. På denne måten kan DLD eliminere sunn konkurranse i markedet. Dette er imidlertid kun relevant dersom staten ikke står for kostnadene ved endring av databaser og lagringsmetoder.

[71] Tilbydere som registerte seg som aktive til ekomrapporten, post- og teletilsynet 2009.

En positiv side ved implementering er at det kan bli større åpenhet rundt lagring av trafikk- og lokasjonsdata. Slik det er i dag er det ikke sikkert at forbrukerne er klar over hvor mye data som blir lagret om dem. Det kan også bli andre rutiner for lagring og sletting av data, som kan øke sikkerheten rundt det.

4.2.2 Andre bekymringer fra NetCom

Under intervjuet med NetCom ble det ytret bekymring ved andre myndigheters mulige tilgang til dataen som lagres. Det kan tenkes at det utvikler seg slik at både banker og NAV kan få tilgang til denne type data. Da vil man ende opp med en totalitær overvåkning på flere plan i samfunnet. Man kan i dag se at NAV tar kontakt med teletilbydere for å få opplysninger fra trafikkdata.[72] Det er på det rene at dette ikke er et argument for eller mot innføring av DLD, men heller en bekymring for utvikling i samfunnet generelt og hvilke konsekvenser det kan ha å implementere direktivet i Norge.

Videre kan teletilbyderne rammes av brudd på taushetsplikt ved utro tjenere. Det er personer som må utlevere dataen politiet krever, og disse vil sitte inne med stor mengde sensitiv informasjon, og få innblikk i saken fra både politiets og teleoperatørens side. Det er en mulighet for misbruk av informasjon på dette punkt. Og det er også andre ansatte som er avhengig av å kunne sjekke en abonnents trafikkdata, som for eksempel kundebehandlere. Man kan ikke lage et system som er 100% sikkert.

Det er to viktige temaer man veier opp mot hverandre, personvernet til kundene og effektiv bekjempelse av alvorlig kriminalitet og terror.

[72] Stopp DLD seminar

4.3 Datatilsynet

Etter samtale med Cecilie L. B. Rønnevik og Jørgen Skorstad. Det er Datatilsynet som har ansvar for lagring og sletting av personopplysninger. Av denne grunn så jeg det som nødvendig å høre på deres synspunkter på datalagringsdirektivet.

4.3.1 Datalagringsdirektivet vil endre et grunnprinsipp i norsk rett

Datatilsynet har som hovedoppgave å holde seg orientert og informere om den nasjonale og internasjonale utviklingen i behandlingen av personopplysning. De skal også ha oversikt over problemene som knytter seg til slik behandling. Datatilsynet skal identifisere farer for personvernet og gi råd om hvordan de kan unngås eller begrenses.[73] Med grunnlag i dette har Datatilsynet måtte gjennomgå DLD og de konsekvenser det etter deres mening kan ha i vårt samfunn. Det har kommet klart frem i deres høringsnotat at de er mot implementering av DLD. Det har mange grunner for seg. Et hovedpoeng fra deres side er at et slikt direktiv vil drastisk forandre et av grunnprinsippene i norsk rett, som er at man er uskyldig inntil motsatt bevist, uskyldspresumsjonen.

I norsk rett er det slik at det må foreligge mistanke om kriminell handling eller andre omstendigheter som indikerer kriminelle handlinger for at politiet skal få innhente informasjon fra teletilbyderne. Dersom DLD blir implementert vil det bli en form for kontroll over personer som også ikke er mistenkt for en kriminell handling. Det er i følge Datatilsynet ikke juridisk riktig.

4.3.2 Fare for misbruk

Datatilsynet kan også se for seg at det vil være mulig for politiet å misbruke informasjonen som er lagret, for eksempel for å oppklare saker som ikke går inn under ordlyden ”serious crime”. Videre er det deres mening at departementet ikke har gjennomgått direktivet grundig nok og heller ikke vurdert alternative løsninger til det. De kan være enig i at det er

[73] www.datatilsynet.no

noen gode bestemmelser i DLD, men at det fremstår som et slags pakketilbud. Tilsynet savner også en gjennomgang av hvilken bevisverdi den innhentede dataen vil gi.[74]

Datatilsynet mener også at det er et poeng at personer som er innblandet i alvorlig kriminalitet vil finne andre måter å kommunisere på.

4.3.3 Konsekvenser implementering vil kunne medføre

Et annet argument fra Datatilsynet er pressens kildevern. I dag har de som snakker med journalister et krav om å kunne holdes anonyme. DLD vil kunne bidra til at kildevernet blir svekket eller borte. I de tilfellene journalister får tips per e-post om kriminell adferd, har ikke politiet mulighet for å sjekke opp hvem som tipset, og de kan heller ikke kreve at journalisten oppgir det. Dersom tipset til journalisten er om ”serious crime” vil det være en mulighet for politiet å kreve utlevering av data som identifiserer e-postsenderen, og dermed avslører kilden.

Datatilsynet mener også, som flere andre, at direktivet som ble laget i 2006 er utdatert og trenger en ny vurdering. Bruken av smarttelefoner har utviklet seg enormt og dette har ikke blitt tatt med i vurderingen, etter deres mening. Bruker man for eksempel en iPhone, er det vanlig at denne logger på internett og sjekker epost fire ganger i timen, eller oftere. Da vil telefonen sende signaler til basestasjonen så ofte at man i realiteten vil kunne overvåke hvor en person befinner seg til enhver tid av døgnet.

Et annet argument er at mengden data vil bli så stor at det kan også vanskeliggjøre arbeidet for politiet. Her kan man se opp mot etterretningstjenesten hvor det lagres store mengder data, men det bidrar likevel ikke til 100% oppklaring og avverging av kriminelle handlinger. Selv om det vil bli lagret store menger data, vil det være til bruk på en annen måte enn etterretningstjenesten. Politiet vil kreve innsyn i det saker hvor de mistenker at det har blitt begått en kriminell handling, og på denne måten blir det et mer konkret søk,

[74] Fra samtalen med Datatilsynet

enn der hvor man følger med på all data som kommer inn, for så å vurdere om det kan inneholde trusler.

Datatilsynet frykter også at innholdsdataen kan bli lagret automatisk og at politiet også vil kunne kreve å få denne utlevert etter hvert. De mener det er lettere å få tilgang på data som allerede er lagret. Datatilsynet er ikke overbevist om at ikke også innholdet i for eksempel eposter følger automatisk med når til og fra adressen lagres. Det ble ikke gjennomgått på tilfredsstillende måte av departementet i deres høringsnotat.

Datatilsynets forslag er å ha en prøveperiode, hvor bestemmelsene kunne prøves og vurderes nøyere. Et slikt inngrep i den personlige sfære må avgjøres på tilstrekkelig grunnlag, og som tidligere nevnt, synes ikke tilsynet at departementet har gjort en grundig nok jobb på dette området. Datatilsynet er ikke alene om denne meningen og det kommer også frem i flere høringsnotater.

5 Erfaringer og evaluering av direktivet

5.1 Hvor er direktivet implementert (helt eller delvis)

Storbritannia, Frankrike, Finland, Danmark, Bulgaria, Kypros, Tyskland (Domstolen har kommet til at DLD bryter med konstitusjonen), Tsjekkia, Estland, Ungarn, Latvia, Litauen, Italia, Malta, Nederland, Polen, Portugal, Romania (Domstolen har kommet til at DLD bryter med konstitusjonen), Slovenia, Slovakia og Spania. Liechtenstein og Sveits er de EFTA statene som har implementert helt eller delvis.[75]

[75] crn.com

5.2 Hvor er direktivet ikke implementert

Irland, Sverige, Østerrike, Belgia, Hellas, Luxemburg og Norge.[76]

5.3 Danmark

Danmark var den første staten i EU som implementerte direktivet, og det tråde i kraft 15. september 2007. Etter retsplejelovens § 786, stk. 4 kommer det frem at *"det påhviler utbydere af telenet eller teletjenester at foretage registrering og opbevaring i 1 år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold. Justisministeren fastsætter efter forhandling med ministeren for vitenskap, teknologi og udvikling nærmere regler om denne registrering og opbevaring"*. I logningsbekendtgørelsen kapittel 1 og 2 blir det gjort rede for hva som skal lagres i Danmark. Dette kan i de store trekk sammenlignes med det som blir opplistet ovenfor i punkt 3.4. Videre har det kommet frem i media at det lagres mer data i Danmark, enn det DLD krever. Etter de danske reglene pålegges teletilbydere å lagre informasjon om steder på nettet brukeren besøker.[77] Dette er ikke krevet fra EU. Teletilbyderne må altså ha en vesentlig større kapasitet for å lagre slik data i tillegg til det som kreves etter direktivet. At internettsidene man besøker skal lagres i ett år, øker spørsmålet om overvåkning. Man må kunne konkludere med at det er særdeles inngripende at slik innholdsdata også lagres.

Henning Mortensen, sjefskonsulent i Itek Danmark, er ikke positivt innstilt til direktivet. Han mener at *"det svarer jo til at skyde gråspurve med kanoner. Jeg stiller mig stærkt tvivlende over for, hvorvidt den mængde data, man har valgt at logge i Danmark, står i forhold til, hva man faktisk får ud af det"*. [78] Han mener videre at det er mulig for terrorister å omgå direktivet og dermed fremstår direktivet som en overvåkning av befolkningen ellers.

---

[76] crn.com

[77] ing.dk

[78] ing.dk

Videre har Jacob Mchangama utarbeidet en rapport for Cepos[79]. Her legger han vekt på at det har gått 2 og et halvt år siden DLD ble implementert og det er foretatt milliarder av registreringer av alminnelige lovlydige borgere og dette har påført teletilbyderne omkostninger for over 100 millioner danske kroner. På tross av dette er det lite som tyder på at terrorbekjempelsen i Danmark er styrket på noe vis.

Logningsbekendtgørelsen (LG), som er tilsvarende datalagringsdirektivet, inneholder en revisjonsbestemmelsen som åpner for at man kan evaluere loven etter noen år, og deretter avgjøre om bestemmelsene er effektive. I mars 2010 sendte den danske justisministeren et høringsforslag om å endre denne bestemmelsen slik at det ikke skulle være noen mulighet for revisjon. Dette forslaget ble trukket etter mange negative reaksjoner.

Det viser seg at politiet sjelden har behov for historisk lagret data. Etter erfaringene fra Danmark kommer det frem at politiet får en rettskjennelsen for å få tilgang til lagret data, og den registrerte data kun er aktuell i de tilfeller hvor politiet er i en etterforskning og har mistanke om kriminelle forhold. På denne måten kan politiet, som før, starte hemmelig overvåkning av vedkommende og får informasjon på denne måten. Det viser seg å være mer effektivt enn historisk lagrede data. Dette stemmer også overens med det lekkede dokumentet fra EUs evaluering av DLD. Her kommer det frem at i de aller fleste tilfellene søker politiet om utlevering av data som er yngre enn 3 måneder og ikke eldre enn 7 måneder.

Ifølge den danske telekombransjens bransjeforening og fagforening for IT profesjonelle (Prosa) brukes lagret data primært til etterforskning av mildere former for kriminalitet.[80] Dette strider mot bakgrunnen for direktivet, som er bekjempelse av alvorlig kriminalitet. Alvorlig kriminalitet har ofte blitt forstått som bekjempelse av terrorisme.

---

[79] Center for politiske studier (2010).

[80] Telekommunikationsindustrien i Danmarks høringssvar af 24. marts 2010 og PROSA's høringssvar af 16. marts 2010.

Jacob Mchangama kommer inn på at kostnaden for lagringsplikten er svært høy og ettersom effekten er noe tvilsom burde man kanskje vurdere om pengene kunne brukes på en annen måte som ikke vil krenke borgernes privatliv.

5.4 EUs evaluering av direktivet

EU skulle komme med en evaluering av DLD som skulle publiseres 15. september 2010. Denne ble imidlertid utsatt, men det har likevel lekket ut en versjon som bekreftes som ekte av utgiveren.[81] I dokumentets første del kan man lese hvordan EU selv evaluerer direktivet og dets nytte i de statene som har implementert det. For det første blir det lagt til grunn at det varierer stort mellom medlemsstatene (MS) hvor mange forespørsler de får for uthenting av lagret data. Det varierer fra under 100 forespørsler, til nesten en halv million (Storbritannia). Det er på grunn av dette noe vanskelig å sammenligne de tallene som er oppgitt til EU fra den enkelte stat.

Når det gjelder dataens alder, viser tallene i rapporten at data som kreves utlevert som oftest er mellom 3-7 måneder gamle. Det kommer frem at det er yngre data som er mest forespurt. Men det må legges til grunn at ikke alle MS leverte tall til EU før utkastet til evalueringen ble skrevet, noe som tilsier at tallene som er oppgitt ikke kan generaliseres.

Lagringstiden har vært oppe til diskusjon her i landet flere ganger. I flere av høringssvarene til departementet blir det sagt at den korteste lagringstiden anbefales. På dette punkt ser man en sprik i resten av Europa. Gjennomsnittstiden for lagring er 12 måneder, men man ser at flere MS har lagringstid i 6, 18 og 24 måneder. Dette viser jo at harmonering av bestemmelser innad i EU ikke har skjedd slik det skulle i henhold til direktivet. Et hensyn bak DLD var nettopp å harmonisere lovgivningen i Europa på dette punkt.

[81] www.uhuru.biz

Videre vises det til at ordlyden ”serious crime” blir definert på forskjellige måter i de forskjellige statene. Visse MS har satt et krav til hvor lang minstestraffen er for å definere det, mens andre har gitt domstolen som skal avgjøre utlevering en diskresjonær kompetanse til å avgjøre om handlingen faller inn under ”serious crime”. At det ikke foreligger en unison forståelse av dette begrepet kan være forvirrende, nettopp fordi direktivet skal samle EUs bekjempelse av alvorlig kriminalitet.

Det kommer også frem i evalueringen at flere stater bruker den lagrede dataen til andre formål enn bekjempelse av kriminalitet. For eksempel blir det i en MS brukt til å ”maintain public order”.

Det er på det rene at implementering av DLD medfører store kostnader. I rapporten kommer det frem at hvem som står for disse kostnadene varierer fra stat til stat. Det blir lagt til grunn at de fleste stater ikke tilbakebetaler teletilbyderne for de kostnader DLD påfører dem. Det er imidlertid et fåtall MS som tilbakebetaler visse kostnader som følge av DLD. Dette underbygger argumentet om at det vil ødelegge konkurransen i telemarkedet, ettersom det vil være vanskelig for de mindre tilbyderne å ta en slik kostnad og i tillegg konkurrere om prisene.

Det evalueres ikke hvor stor verdi trafikkdata har som bevis i denne rapporten, dette er fordi MS ikke har kunnet oppgi en slik statistikk. Det foreligger uttalelser fra stater om at trafikkdata ofte har stor betydning, men at det som regel ikke er det eneste beviset i saken.

Når det kommer til innhenting av data og samarbeid mellom medlemsstatene er ikke resultatet særlig bra. Etter det som kommer frem i evalueringen kan det ta rundt 10 dager å få besvart en henvendelse og opp til 20 dager å få identifisert et telefonnummer eller lignende data.

Videre blir det uttalt fra en MS at DLD har ”catastrophic impacts” og at direktivet medfører økede priser i telemarked, restriksjoner for konkurranse og frihet, samt systematisk mangel på tillit til borgerne. Flere stater mener også at DLD ikke harmonerer bestemmelsene innad i EU, og at det heller ikke har bidratt til en nedgang av kriminalitet eller økning av oppklaring av saker.[82] Dette er ikke positive uttalelser for direktivet. Og man kan spekulere i om dette er av denne grunnene til at evalueringen ble utsatt publisert på ubestemt tid.

Noen MS har foreslått at direktivet burde avsluttes nå, eller ha en åpning for at statene selv skal velge om de ønsker å følge direktivet. Det er i det minste et sterkt ønske om at ”serious crime”, ”data” og ”service” defineres klart i direktivet, samt å sette en felles frist for lagringstiden for alle stater. De fleste punkter i rapporten bringer frem mye misnøye ved direktivet.

Også endringene i hvordan vi bruker internett i dag blir nevnt i rapporten. En medlemsstat mener at disse endringene er så store at artikkel 5 i direktivet må revideres. Det sies at ”*data about internet use and location should no longer be retained*”.[83]

Når det gjelder lagring av trafikkdataen har det ikke blitt bestemt hvordan det eventuelt skal gjøres i Norge. I denne rapporten kommer det frem at flere MS bruker andre stater for å lagre sin trafikkdata. Dette gjør det vanskelig å overvåke hvem dataen utgis til. Spørsmålet om korrupsjon melder seg også på dette punkt. Videre stilles det også spørsmål om hvilken jurisdiksjon dataen da vil ligge under. Det kommer også frem at teleoperatører lagrer data på forskjellige måter, også innad i samme stat. Deutsche Telekom måtte forøvrig bruke 5,2 millioner euro for å oppgradere sine systemer ved implementering av direktivet. I tillegg til denne betydelige utgiften har selskapet også blitt påført store kostnader ved lagring og utlevering av data.[84]

---

[82] Room Document. Evaluation of Directive 2006/24/EC.

[83] Evaluering av DLD (2010)

[84] Evaluering av DLD (2010) s. 9

Det er i dokumentets første del at EU evaluerer DLD.[85] Det er på det rene at det ikke fremkommer noen form for statistikk i denne evalueringen og det er fordi ingen av MS har innlevert det til EU. Den informasjonen og de uttalelsene som kommer frem i dokumentet taler ikke i særlig stor grad for implementering av datalagringsdirektivet.

6 Oversikt over forskjellene DLD kan medføre

Her vil jeg sette opp en enkel oversikt (figur 1) som viser hvilke trafikkdata som pliktes å lagre i dag, samt hvilke data som vil pliktes å lagres etter DLD.[86] Det er av stor interesse å finne ut hva som faktisk lagres i dag, på tross av at det ikke foreligger noen plikt til å gjøre det. Denne informasjonen har jeg fått fra NetCom og Telenor. Det som lagres i dag lagres mellom 3-5 måneder, og dette er i henhold til sletteplikten i konsesjonen omtalt i punkt 2.3.1.1. Noen felter er ikke fylt ut, og dette er på grunn av at jeg ikke fikk informasjonen oppgitt fra operatørene.

Trafikkdata		**Plikt til å lagre i dag**	**Plikt til å lagre med DLD**	**Lagres det i dag?**
Data som er nødvendig for å spore og identifisere kilden til kommunikasjonen	Fasttelefon og mobil: A-nummeret	Ja	Ja	Ja, jf. ekomforskriften § 6-2
	Fasttelefon og mobil: Navn og adresse på abonnenten eller den	Ja	Ja	Ja

[85] www.uhuru.biz

[86] Stoppdld.no

	registrerte bruker			
	Internettelefoni: Tildelt bruker-id	Nei	Ja	Nei
	Internettilgang: Tildelt bruker-id	Nei	Ja	
	E-post: Tildelt bruker-id	Nei	Ja	Ja
	Internettilgang, e-post og internettelefoni: Den bruker-id og det tlf. nr., som er tildelt kommunikasjoner, som inngår i et offentlig telefonnett	Nei	Ja	Ja, men ikke for epost.
	Internettilgang, e-post og internettelefoni: Navn og adressen på den abonnent eller reg. bruker, til hvem en IP-adresse, en bruker-id eller et tlf. nr. var tildelt på kommunikasjonstidspunktet	Nei	Ja	Ja, i 3 uker
Data som er nødvendig for å fastslå en kommunikasjons bestemmelsessted	Fasttelefon og mobil: Det eller de valgte numre (B-nummeret) og, hvis det er tale om supplerende tjenester slik som viderestilling og omstilling, de eller de numre, som oppkallet ledes videre til.	Nei	Ja	Ja, etter konsesjonen
	Fasttelefon og mobil: Navn og adresse på abonnement eller den registrerte brukeren.	Ja	Ja	Ja
	E-post og internettelefoni: Bruker-id eller telefonnummer på den mottaker som et internettelefon anrop er rettet til.	Nei	Ja	Nei
	E-post og internettelefoni: Navn og adresse på abonnenten eller den registrerte brukeren og bruker-id på den mottaker som kommunikasjonen er rettet til.	Nei	Ja	Nei
Data som er nødvendig for å fastslå kommunikasjonens dato, klokkeslett og type	Fasttelefon og mobil: Dato og klokkeslett for kommunikasjonens begynnelse- og sluttidspunkt.	Nei	Ja	Ja, fakturabehov
	Internettilgang, e-post og internettelefoni: Dato og klokkeslett for inn- og utlogging av internettadgangstjenester basert på en bestemt tidssone og den dynamiske eller statiske IP-adresse, som tilbyderen av internett har tildelt en kommunikasjon, samt bruker-id på abonnementet eller den registrerte bruker.	Nei	Ja	Ja
	Internettilgang, e-post og internettelefoni: Dato og klokkeslett for inn- og utlogging av e-posttjeneste og telefontjenester på internett basert	Nei	Ja	Ja, til dels*

	på en bestemt tidssone.			
Data som er nødvendig for å fastslå kommunikasjonens type	Fasttelefon og mobil: Den anvendte telefontjeneste.	Nei	Ja	Ja
	E-post og internettelefoni: Den anvendte internettjeneste.	Nei	Ja	Ja
Data som er nødvendig for å identifisere kommunikasjonsutstyret eller det som fremstår som brukerens utstyr	Fasttelefon: A-nummer, B-nummer	Ja	Ja	Ja
	Mobil: A-nummer, B-nummer	Ja	Ja	Ja
	Mobil: A-nummer og IMSI-nummer	Nei	Ja	Kan lagres etter forespørsel fra politiet
	Mobil: A-nummer og IMEI-nummer	Nei	Ja	Kan lagres etter forespørsel fra politiet
	Mobil: B-nummer og IMSI-nummer	Nei	Ja	
	Mobil: B-nummer og IMEI-nummer	Nei	Ja	
	Mobil: Ved forhåndsbetalte anonyme tjenester, dato og tidspunkt for første aktivering av tjenesten og celle-ID fra aktiveringen tok sted.	Nei	Ja	Det finnes ikke slike tjenester i Norge
	Internettilgang, e-post og internettelefoni: A-nummer med henblikk på dial-up-tilgang.	Nei	Ja	Det varierer fra leverandør til leverandør
	Internettilgang, e-post og internettelefoni: DSL eller annet endepunkt for kommunikasjonens opphavsmann	Nei	Ja	Vanskelig å identifisere en bruker, men husstanden
Data som er nødvendig for å foreta en lokalisering av mobilt utstyr	Lokaliseringskoden (celle-ID) ved kommunikasjonens begynnelse.	Nei	Ja	Ja
	Data som med henvisning til deres celle-ID viser cellenes geografiske lokalisering i den periode hvor det lagres kommunikasjonsdata.	Nei	Ja	Ja, teknisk behov

Det kommer frem i samtalen med Telenor at hva som lagres kan variere stort mellom leverandørene. Det er ofte hva slags tilbud og hva slags system leverandøren anvender som avgjør dette. Det er også vanskelig å slå fast konkret hva direktivet mener. Det viser seg at det er vanskelig å forstå nøyaktig hva det siktes til. De teknologiske ordene skiller seg fra hva som brukes i bransjen i dag.

Når det gjelder internettbruk er det vanskelig å identifisere brukeren. Dette er fordi det ofte er flere bruker av et nettverk i en husstand. Det kan være familiemedlemmer som anvender

nettverket, eller noen som har brutt seg inn på det aktuelle nettverket. Det gjør at det alltid vil være den som står registrert som abonnent som utleveres, og ikke nødvendigvis den faktiske brukeren.

Videre når det er slik at det varierer fra leverandør til leverandør, gjør det at dette skjemaet ikke kan være 100% korrekt. Jeg har fått informasjon fra de to største leverandørene i Norge, Telenor og NetCom til å fylle ut dette skjemaet.

*På den måten direktivet forklarer det, er ikke slik det fungerer i praksis i dag. Når en epost blir lest i dag, vil det til slutt bli lagt inn at eposten er lest, men ikke inn- og utlogging av eposttjenesten. Det ville vært mer relevant ved en nettbasert eposttjeneste.[87]

7 Vurdering

Om datalagringsdirektivet ikke skulle bli implementert i Norge, kan det argumenteres for at personvernet står i veien for bekjempelse av alvorlig kriminalitet, som for eksempel terrorisme. Politiet, ved Kripos, har opplistet flere tilfeller hvor trafikkdata har hatt avgjørende rolle i en etterforskning.[88] Et eksempel er Nokas-saken[89] fra 2004. I denne saken var trafikkdata, lokasjonsdata og sporing av IP-adresser nødvendig for å pågripe de siktede. Det var utskrifter fra basestasjonene som kunne avsløre hvilke telefonnummer gjerningsmennene hadde brukt, og de samme utskriftene kunne identifisere vitner som hadde vært i nærheten. Også fluktruten kunne spores ved hjelp av trafikk- og lokasjonsdata. Videre ble det brukt utlevering av trafikkdata for å sjekke om flere mistenkte virkelig hadde alibi, slik de selv hevdet. Det blir også sagt at pågripelsen av David A. Toska var et

[87] Telenor

[88] Kripos høringssvar til departementet s. 9

[89] Ran av Norsk Kontantservice, Stavanger 2004.

resultat av sporing og identifisering av IP-adresser for den bruk av epost han hadde hatt i ettertid. At politiet hadde muligheten til å gå tilbake i tidligere lagret trafikk- og lokasjonsdata var i denne saken helt nødvendig. Det er vanskelig å si hvilket resultat det hadde blitt av etterforskning om de ikke hadde disse sporene å gå etter. Og et poeng i saken rundt DLD er om vi i Norge vil havne i den situasjonen der politiet ikke kan anvende trafikkdata for planlagt kriminalitet. Dette er dersom teletilbydere stopper lagring av data for faktureringen. Det skal ikke være slik at man skal gå tilbake i tid med tanke på ressurser, at politiet skal få mindre og mindre å bruke i etterforskningen. Man kan se at politiet har hatt bruk for trafikkdata som bevis i flere saker. Dette tilsier at det er nødvendig å sikre at de også i fremtiden får anledning til å uthente samme type data.

Et positivt punkt ved direktivet vil være den eventuelle kriminalitetsbekjempelsen. Dette er et hensyn som bør veie tungt, men ikke utelukkende gå på bekostning av personvernet. Det har ikke etter EUs evaluering av direktivet bidratt til noen større oppklaringsprosent. Når det ikke rettslig eller statistisk kan vises at direktivet bidrar til bekjempelse av kriminalitet er det få argumenter som taler for implementering. Det er tilfeldig hvilke spor en kriminell legger igjen etter en straffbar handling er begått, og dette gjør oppklaring av saker vanskelig. Forebyggelse og oppklaring av kriminelle saker har alltid vært vanskelig, uavhengig av bruk av internett eller telefontjenester.

Et tema som går igjen flere steder i oppgaven er at en plikt for teletilbyderne til å lagre denne type data vil fremstå som overvåkning av personer som ikke er mistenkt for noen alvorlig kriminell handling. I dag er det kun en plikt om sletting. Man kan si at lagring med bakgrunn i dette strider mot uskyldspresumsjonen slik vi kjenner den i dag.

Det er på det rene at mye av den samme dataen lagres allerede i dag, selv om det ikke foreligger noen plikt til det. Et argument her er at det i vesentlig grad ikke blir noen realitetsendring for borgerne i samfunnet. Likevel er det begrunnelsen bak lagringen som prinsipielt gjør at DLD blir problematisk juridisk sett og personvernsmessig. Et grunnleggende rettssatsprinsipp er at man skal ses som uskyldig inntil skyld er bevist etter

loven. Dette kan man lese ut av EMK art. 6 nr. 2. Det er på det rene at det er påtalemyndigheten som må påvise denne skylden, for at den tiltalte skal kunne dømmes. Det kan være en vanskelig oppgave for politiet å bevise skyld, ettersom retten stiller strenge krav. Men det skal ikke gå på bekostning av borgernes frihetsfølelse. Og selv om det er interessant og til hjelp for politiets arbeid kan det ikke være slik at alt skal lagres. Da kunne man til slutt strekke det så langt at man videoovervåket alle til enhver tid, for sikkerhetsskyld, og kun bruke sporene ved en eventuell kriminell handling.

Det er også slik at man må vurdere de mulighetene det er for å omgå direktivet. Slik DLD er utformet i dag er det flere kommunikasjonstyper som utelukkes. Dette kan tale for at lagringen ikke vil ramme bekjempelse av for eksempel terror, da det er veldig vanlig å anvende Skype og nettbasert epost. I alle fall etter en eventuell implementering må man kunne regne med at grupper som planlegger alvorlig kriminalitet benytter seg av tilbud som faller utenfor lagringsplikten.

Det er ikke en oppstramming av dagens praksis rundt innhenting av lagret data som bør stoppes, eller lagringen i seg selv. Det er plikten til å lagre data til spesifikk bruk av politiet til bekjempelse av alvorlig kriminalitet som er kritikkverdig. Denne endringen kan man se på som et paradigmeskifte i strafferetten og rettsstaten.[90] Man kan kanskje påstå at en oppdatering av nåværende lovgivning ville være det mest hensiktsmessige.

DLD blir i prinsippet en bevissikring før den kriminelle handlingen har blitt begått. Det er altså en bevissikring uavhengig av en etterforskning. Dette bryter med etterforskningsbestemmelsene- og prinsippet vi har i dag. I dag er det i all hovedsak krav om skjellig grunn til mistanke før man kan starte etterforskning. Ved at trafikkdataen lagres på forhånd, og brukes dersom en borger skulle begå en kriminell handling, anvendes etterforskningsmetoden før handlingen er begått. Juridisk sett klinger ikke dette i ørene.

[90] Samtale med Torgeir Waterhouse, IKT-Norge.

Man kan kanskje gå så langt at man sier at man ved bruk av elektronisk kommunikasjonsutstyr blir mistenkeliggjort.

I dag har vi utviklet en generelt stor toleranse for utlevering av personopplysninger. Dersom man er uføretrygdet vil NAV følge med på pengebruk og hvor man befinner seg. Det er et viktig spørsmål om vi faktisk ønsker å utvide denne toleransen ytterligere. Selvsagt er det nyttig for politimyndigheten å ha oversikt over borgerne og hva de foretar seg. Men skal man da akseptere å bli overvåket? Det har blitt argumentert med at opplysningene kun skal anvendes når mistanken oppstår. Da kan man også si at det skal settes opp overvåkningskamera i alle hjem, i tilfelle det skjer en kriminell handling der. Da vil det være svært nyttig å ha det materialet for å oppklare forbrytelsen.[91] Et viktig poeng i diskusjonen om DLD er om det er et slikt samfunn vi ønsker å ha. Man skulle ikke tro at det er nødvendig for allmennheten å oppgi sin frihet for bekjempelse av kriminalitet.

8 Konklusjon

I denne oppgaven har jeg valgt å se på nåværende bestemmelser og sammenlignet denne tilstanden opp mot hvordan det kan bli ved en eventuell implementering av datalagringsdirektivet i Norge. For å gjøre dette har jeg gjennomgått mye av gjeldende rett, og hvordan disse bestemmelsene brukes i praksis. På denne måten kan man få et innblikk i hvordan politiet arbeider i dag og i hvilke situasjoner de har bruk for lagret trafikkdata. Dette er viktig for å forstå hva DLD forplikter staten til å lagre. Det er nettopp denne plikten til å lagre som blir en diskusjon i oppgaven. At slik data skal lagres er neppe veldig oppsiktsvekkende, ettersom mye av det lagres allerede i dag. Men det at det lagres etter faktureringsbehov for teletilbyderne, og ikke til politiets bruk er viktig. Det er denne endringen som har fått samfunnet til å engasjere seg i dette temaet.

[91] Seminar av Stopp DLD.

Det er vanskelig å komme med en presis konklusjon på spørsmålet oppgaven reiser, det er vurderingsdelen som svarer på hvilke konsekvenser det kan ha for Norge, om direktivet blir implementert. Videre syns jeg det har vært interessant å se hvor aktivt politiet i dag bruker trafikk- og lokasjonsdata i mange forskjellige typer saker. Dette taler for at deres bruk av slike spor ikke burde innskrenkes, men lovgivningen vi har i dag trenger kanskje en oppdatering. Det er ikke nødvendigvis datalagringsdirektivet som må sikre at politiet også i fremtiden kan anvende slik data i sine etterforskninger. At Norge ikke vil ha lik lovgivning som resten av Europa er et svakt argument med tanke på den dårlig harmoneringen som er i dag etter DLD, jf. evalueringen fra EU.

9 Litteraturliste

9.1 Forarbeider

Ot.prp.nr. 58 (2002-2003) Om lov om elektronisk kommunikasjon (ekomloven)

Ot.prp.nr. 92 (1998-1999) Om lov om behandling av personopplysninger (personopplysningsloven)

9.1.1 Offentlige utredninger

NOU 1997:19 Et bedre personvern

9.2 Lovgivning

9.2.1 Norsk lovgivning og forskrifter

1902 Alminnelig borgerlig Straffelov (straffeloven) av 22. mai 1902 nr. 10

1978 Lov om personregistre m.m. (personregisterloven av 9. juni 1978 nr. 48 (opphevet)

1981 Lov om rettergangsmåten i straffesaker (straffeprosesslove) av 22. mai 1981 nr. 25

1992 Avtale om Det europeisk økonomiske samarbeidsområde (EØS-avtalen) av 27. november 1992 nr. 109

1995 Lov om telekommunikasjon (teleloven) av 23. juni 1995 nr. 39 (opphevet)

1995 Forskrift om kommunikasjonskontroll (kommunikasjonskontrollforskriften) av 31. mars 1995 nr. 218

2000 Lov om behandling av personopplysninger (personopplysningsloven av 14. april 2000 nr. 31

2000 Forskrift om behandling av personopplysninger (personopplysningsforskriften) av 15. desember 2000 nr. 1265

2003 Lov om elektronisk kommunikasjon (ekomloven) av 4. juli 2003 nr. 83

2004 Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften) av 16. februar 2004 nr. 401

9.2.2 Traktater og konvensjoner

EMK Den europeiske menneskerettskonvensjonen, Roma 1950

TEUF Traktaten om den europeiske unions funksjonsområde

9.2.3 Utenlandske lover

2009 Retsplejeloven, Danmark

9.3 Rettsavgjørelser

Rt. 2009 s. 394

9.4 Artikler

Bruce, Ingvild. Datalagringsdirektivet – en menneskerettskrenkelse eller forpliktelse?
I: Lov og Rett, Årg. 49 (2010), s. 6-26

Wessel-Aas, Jon. EUs datalagringsdirektiv – et angrep på den liberale rettstaten etter et nødvendig tiltak i moderne kriminalitetsbekjempelse.
I: Pacta, Årg. 4 (2010), s. 47-53.

Wessel-Aas, Jon. Datalagringsdirektivet og EMK – Kommentarer til Ingvild Bruce.
I: Lov og Rett, Årg. 49 (2010), s. 154-164.

9.5 Bøker

Andenæs, Johs. Norsk straffeprosess. 4. utgave. Samlet utgave ved Tor-Geir Myhrer. Oslo (Universitetsforlaget), 2009.

Gisle, Jon. Jusleksikon. 3. utgave. Oslo, 2007.

Sejersted, Fredrik, Arnesen Finn, Rognstad, Ole-Andreas, Foyn, Sten og Kolstad, Olav. EØS-rett. 2. utgave. Oslo (Universitetsforlaget), 2005.

9.6 Nettdokumenter

CEPOS. Logningsbekendtgørelsen bør suspenderes med henblik på rettssikkerhedsmæssig revidering.
http://www.cepos.dk/fileadmin/user_upload/billeder/juli/Notat_-_Logningsbekendtgoerelsen_boer_suspenderes_med_henblik_paa_retssikkerheddsmaessig_vurdering.pdf [sitert 4. oktober 2010]

cnet News. FBI wantts records kept of websites visited.

http://news.cnet.com/8301-13578_3-10448060-38.html [sitert 28. september 2010]

cnet News. ISP snooping gaining support. http://news.cnet.com/ISP-snooping-gaining-support/2100-1028_3-6061187.html [sitert 28. september 2010]

CRN. Proposed child pornography laws raise data retention concerns. http://www.crn.com/news/networking/214502232/proposed-child-pornography-laws-raise-data-retention-concerns.htm [sitert 28. september 2010]

CRN. Lessons learned from Europe's data retention laws. http://www.crn.com.au/News/215135,lessons-learned-from-europes-data-retention-laws.aspx [sitert 2. oktober 2010]

Datatilsynet. Konsesjon teletjenester med merknader. http://www.datatilsynet.no/upload/Dokumenter/konsesjoner/konsesjon_tele_m_merkn.pdf [sitert 20. september 2010]

Datatilsynet. Datalagringsdirektivet – mer enn et spørsmål om lagringstid. http://www.datatilsynet.no/templates/Page____2230.aspx [sitert 2. september 2010]

Datatilsynet. Høringssvar – implementering av datalagringsdirektivet (2006/24/EC). http://datatilsynet.no/upload/hoering/2010/hoering_datalagring.pdf [lastet ned 10. september 2010]

Datatilsynet. Om datatilsynet. http://www.datatilsynet.no/templates/AboutPage____220.aspx [sitert 4. september 2010]

EU Directive 2006/24/EC – Why it won't work.

http://www.janhenrik.com/blog/2010/04/eu-directive-200624ec-datalagringsdirektivet-why-it-wont-work/ [sitert 18. oktober 2010]

Europabevegelsen. Datalagringsdirektivet. http://webcache.googleusercontent.com/search?q=cache:heeMJdKaB7EJ:www.jasiden.no/Fakta-om-EU/Direktiver-fra-EU/Datalagringsdirektivet+http://www.jasiden.no/Fakta-om-EU/Direktiver-fra-EU/Datalagringsdirektivet&cd=1&hl=en&ct=clnk&client=safari [sitert 17. september 2010]

Haugland, Geir Sunde. Kommentar til straffeprosessloven. I: Norsk Lovkommentar nettversjon. [22. september 2010]

ing.dk. Danmark logger mer trafik end EU kræver. http://ing.dk/artikel/96386-danmark-logger-mere-trafik-end-eu-kraever [sitert 4. oktober 2010]

Kambe, Arve. Ja til datalagringsdirektivet. http://arvekambe.blogspot.com/2010/05/ja-til-datalagringsdirektivet_07.html [sitert 10. september]

Kripos. Høring om datalagringsdirektivet. http://www.regjeringen.no/pages/2281080/kripos.pdf [sitert 19. oktober 2010]

NetCom. Høringssvar datalagringsdirektivet. http://www.regjeringen.no/pages/2281080/NetCom.pdf [sitert 25. september 2010]

Noreide, Ragnar. Kommentar til EMK. I: Norsk Lovkommentar nettversjon. [sitert 22. september 2010]

Official Journal of the European Union. Directive 2006/24/EC.

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF [sitert 21. august 2010]

Politi. Om Kripos. https://www.politi.no/kripos/om_kripos/ [sitert 30. september 2010]

Post- og teletilsynet. Det norske markedet for elektroniske kommunikasjonstjenester 2009. http://www.npt.no/ikbViewer/Content/119027/Ekomrapport_2009_.pdf [sitert 20. september 2010]

Post- og teletilsynet. Begjæring om fritak fra tilbyders lovpålagte taushetsplikt. http://www.npt.no/portal/page/portal/PG_NPT_NO_NO/PAG_NPT_NO_HOME/PAG_NPT_NO_TEKSTVISNING?p_d_i=-121&p_d_c=&p_d_v=103728 [sitert 25. september 2010]

Post- og teletilsynet. Høring om datalagringsdirektivet. http://www.npt.no/ikbViewer/Content/121404/datalagringsdirektivet.pdf [sitert 27. september 2010]

Room Document. Evaluation of Directive 2006/24/EC. https://docs.google.com/fileview?id=0B2Rh7x7YpF3KNTZlNTU0NDAtZjgwMS00YzJkLWFiODktMDQwNTUxMjE3MTcz&hl=en [sitert 11. oktober 2010]

Rønnevig, Leif-Henrik. Kommentar til ekomloven. I: Norsk Lovkommentar nettversjon. [sitert 22. september 2010]

Samferdselsdepartementet. Høringsnotat datalagringsdirektivet. http://www.regjeringen.no/pages/2281081/hnotat_datalagring.pdf [sitert 27. september 2010]

SearchWinDevelopment. Definition of statick IP-address and dynamic IP-address. http://searchwindevelopment.techtarget.com/definition/static-IP-address-dynamic-IP-address [sitert 1. september 2010]

Statens strålevern. Basestasjoner. http://www.nrpa.no/eway/default.aspx?pid=239&trg=Center_6310&Main_6251=6309:0:15,4813&CenterAndRight_6309=6310:0:15,6269:1:0:0:::0:0&Center_6310=6473:80558: [sitert 28. september 2010]

Stopp DLD. Hva skal lagres. http://stoppdld.no/kunnskapsbanken/hva-skal-lagres/ [sitert 17. september 2010]

Svein Willassen. Datalagringsdirektivet – verdi i etterforskning og risikofaktorer for personvern. Rapport utarbeidet på oppdrag fra Datatilsynet. http://www.regjeringen.no/nb/dep/jd/dok/nouer/2004/nou-2004-6/8/12.html?id=385449 [sitert 27. september 2010]

Teknofil. Alt om datalagringsdirektivet. http://www.teknofil.no/wip4/alt-om-datalagringsdirektivet/d.epl?id=27313 [sitert 2. september 2010]

Teknologirådet. Kommunikasjonsdata. http://www.teknologiradet.no/FullStory.aspx?m=104&amid=488 [sitert 15. september 2010]

Teknologirådet. Datalagringsdirektivet: Saken forklart. http://www.teknologiradet.no/FullStory.aspx?m=28&amid=4824 [sitert 13. september 2010]

Telebeans. Technical questions.
http://www.telebeans.org/telco/towers/faq/technical.html#gsm_cid_fmt [sitert 27. september 2010]

Uhuru. Lekket, foreløpig EU-evaluering av Datalagringsdirektivet.
http://www.uhuru.biz/?p=282 [sitert 11. oktober 2010]

Wikipedia. Dial-up internet access.
http://en.wikipedia.org/wiki/Dial-up_Internet_access [sitert 26. september]

Wikipedia. International Mobile Subscriber Identity.
http://en.wikipedia.org/wiki/International_Mobile_Subscriber_Identity [sitert 3. september 2010]

Wikipedia. Digital Subscriber Line.
http://en.wikipedia.org/wiki/Digital_Subscriber_Line [sitert 1. september 2010]

9.7 Personlige meddelelser

Bruusgaard, Reidar. Samtale/intervju om datalagringsdirektivets betydning for politiet/kripos. 13. september 2010.

Punsvik, Randi. Samtale med NetCom om datalagringsdirektivet. 22. september 2010.

Rønnevik, Cecilie og Skorstad, Jørgen. Samtale om Datatilsynets meninger om datalagringsdirektivet. 15. september 2010.

Stopp DLD. Foredrag av John Christian Elden, Axel Arnbak, Marie Simonsen og Merethe Ranum. Seminar 4. november 2010.

Telenor. Informasjon om hva som lagres i dag. 25. oktober 2010

Waterhouse, Torgeir. IKT-Norge. 8. november 2010

Wessel-Aas, Jon. Samtale om datalagringsdirektivet og dets konsekvenser i samfunnet. 12. oktober 2010.

10 Lister over tabeller og figurer m v

Tabell 1:

År	Henvendelser
2005	1288
2006	1501
2007	1513
2008	**1693**
2009	**1730**

Tabell 2:

År	Nummersøk	Basestasjonssøk[92]	Identitet/IMEI
2004	2441	1312	3725
2005	2397	2040	1402
2006	2624	1924	2085
2007	2196	2534	2438
2008	**3321**	**2561**	**2181**
2009 (9 mnd.)	**2571**	**2067**	**1921**

Figur 1:

Trafikkdata	**Plikt til å lagre i dag**	**Plikt til å lagre med DLD**	**Lagres det i dag?**

[92] Se punk 1.5 om lokasjonsdata.

Data som er nødvendig for å spore og identifisere kilden til kommunikasjonen	Fasttelefon og mobil: A-nummeret	Ja	Ja	Ja, jf. ekomforskriften § 6-2
	Fasttelefon og mobil: Navn og adresse på abonnenten eller den registrerte bruker	Ja	Ja	Ja
	Internettelefoni: Tildelt bruker-id	Nei	Ja	Nei
	Internettilgang: Tildelt bruker-id	Nei	Ja	
	E-post: Tildelt bruker-id	Nei	Ja	Ja
	Internettilgang, e-post og internettelefoni: Den bruker-id og det tlf. nr., som er tildelt kommunikasjoner, som inngår i et offentlig telefonnett	Nei	Ja	Ja, men ikke for epost.
	Internettilgang, e-post og internettelefoni: Navn og adressen på den abonnent eller reg. bruker, til hvem en IP-adresse, en bruker-id eller et tlf. nr. var tildelt på kommunikasjonstidspunktet	Nei	Ja	Ja, i 3 uker
Data som er nødvendig for å fastslå en kommunikasjons bestemmelsessted	Fasttelefon og mobil: Det eller de valgte numre (B-nummeret) og, hvis det er tale om supplerende tjenester slik som viderestilling og omstilling, de eller de numre, som oppkallet ledes videre til.	Nei	Ja	Ja, etter konsesjonen
	Fasttelefon og mobil: Navn og adresse på abonnement eller den registrerte brukeren.	Ja	Ja	Ja
	E-post og internettelefoni: Bruker-id eller telefonnummer på den mottaker som et internettelefon anrop er rettet til.	Nei	Ja	Nei
	E-post og internettelefoni: Navn og adresse på abonnenten eller den registrerte brukeren og bruker-id på den mottaker som kommunikasjonen er rettet til.	Nei	Ja	Nei
Data som er nødvendig for å fastslå kommunikasjonens dato, klokkeslett og type	Fasttelefon og mobil: Dato og klokkeslett for kommunikasjonens begynnelse- og sluttidspunkt.	Nei	Ja	Ja, fakturabehov
	Internettilgang, e-post og internettelefoni: Dato og klokkeslett for inn- og utlogging av internettadgangstjenester basert på en bestemt tidssone og den dynamiske eller statiske IP-adresse, som tilbyderen av internett har tildelt en	Nei	Ja	Ja

	kommunikasjon, samt bruker-id på abonnementet eller den registrerte bruker.			
	Internettilgang, e-post og internettelefoni: Dato og klokkeslett for inn- og utlogging av e-posttjeneste og telefontjenester på internett basert på en bestemt tidssone.	Nei	Ja	Ja, til dels*
Data som er nødvendig for å fastslå kommunikasjonens type	Fasttelefon og mobil: Den anvendte telefontjeneste.	Nei	Ja	Ja
	E-post og internettelefoni: Den anvendte internettjeneste.	Nei	Ja	Ja
Data som er nødvendig for å identifisere kommunikasjonsutstyret eller det som fremstår som brukerens utstyr	Fasttelefon: A-nummer, B-nummer	Ja	Ja	Ja
	Mobil: A-nummer, B-nummer	Ja	Ja	Ja
	Mobil: A-nummer og IMSI-nummer	Nei	Ja	Kan lagres etter forespørsel fra politiet
	Mobil: A-nummer og IMEI-nummer	Nei	Ja	Kan lagres etter forespørsel fra politiet
	Mobil: B-nummer og IMSI-nummer	Nei	Ja	
	Mobil: B-nummer og IMEI-nummer	Nei	Ja	
	Mobil: Ved forhåndsbetalte anonyme tjenester, dato og tidspunkt for første aktivering av tjenesten og celle-ID fra aktiveringen tok sted.	Nei	Ja	Det finnes ikke slike tjenester i Norge
	Internettilgang, e-post og internettelefoni: A-nummer med henblikk på dial-up-tilgang.	Nei	Ja	Det varierer fra leverandør til leverandør
	Internettilgang, e-post og internettelefoni: DSL eller annet endepunkt for kommunikasjonens opphavsmann	Nei	Ja	Vanskelig å identifisere en bruker, men husstanden
Data som er nødvendig for å foreta en lokalisering av mobilt utstyr	Lokaliseringskoden (celle-ID) ved kommunikasjonens begynnelse.	Nei	Ja	Ja
	Data som med henvisning til deres celle-ID viser cellenes geografiske lokalisering i den periode hvor det lagres kommunikasjonsdata.	Nei	Ja	Ja, teknisk behov