Datalagringsdirektivet:
Historie, status og utfordringer

INTRODUKSJON

4. april 2011 vedtok norske politikere at EU-direktiv 2006/24/EF, også kjent som datalagringsdirektivet, skal implementeres i Norge, slik EØS-avtalen krever. Da var nesten fem år gått siden vedtak om direktivet ble fattet i EU. Det norske vedtaket kom kun dager før Europakommisjonen (Kommisjonen) presenterte sin evaluering av direktivet 18. april. Evalueringen gjorde lite for å stilne kritikken fra direktivets motstandere. Det europeiske datasikkerhetstilsynet konkluderte i sin uttalelse til evalueringen at direktivet ikke oppfyller formålet, og at det ikke oppfyller nødvendige krav til personvern og datasikkerhet. Den norske implementeringen av direktivet bør strekke seg så langt det er mulig for å sikre at sentrale verdier som personvern, ytringsfrihet og rettssikkerhet bevares.

Implementeringen av direktivet i resten av Europa har vært problemfylt. Noen medlemsland har av politiske årsaker ennå ikke innført direktivet i nasjonal lovgivning. Noen har innført direktivet, men nasjonale domstoler har annullert innføringen. I andre land er rettslige prosesser underveis. Og i landene som faktisk har implementert direktivet, er de nasjonale reguleringene langt fra harmonisert, slik hensikten var.

Dette notatet vil gi en kort innføring i innholdet i selve datalagringsdirektivet, beskrive datalagringsdirektivets historie, gi en oversikt over dagens status for implementering i Europa, samt ta for seg de viktigste juridiske, ideologiske, praktiske og økonomiske innvendingene mot direktivet og implementeringen av det.

HVA ER DATALAGRINGSDIREKTIVET?

Det formelle navnet på DLD er ”Europa-parlamentets og Rådets direktiv 2006/24/EF av 15. mars om lagring av data fremkommet ved bruk av offentlig elektronisk kommunikasjonstjeneste eller offentlig elektronisk kommunikasjonsnett og om endring av direktiv 2002/58/EF” (*Direktiv 2006/24/EF*). Det ble vedtatt som et markedsdirektiv, og er derfor også bindende for de land som står utenfor EU men er EØS-medlemmer, nemlig Island, Liechtenstein og Norge.

I DLD slås det fast at visse tilbydere av telekom-tjenester plikter å lagre et gitt sett av data som angår deres kunders kommunikasjon. Det spesifiserer i tillegg nedre og øvre grenser for hvor lenge denne informasjonen kan bli lagret, og visse andre aspekter ved lagringen.

Formålet med DLD

Det uttrykte målet med direktivet var å harmonisere de ulike lands nasjonale krav til europeiske telekom-leverandører vedrørende lagring av trafikkdata for kommunikasjon. Imidlertid er den viktigste hensikten, som også er spesifisert i direktivet, "etterforskning, oppdagelse og påtale av alvorlig kriminalitet". Det er åpenbart at datalagring handler om politisamarbeid, og ikke om telekommarkeder. Telekomleverandørene har for eksempel ikke etterspurt direktivet, og mange av dem var imot innføringen, deriblant Telenor, NetCom, Tele2 og Ventelo i Norge (Samferdselsdepartementet 2010). Som fagområde i Kommisjonen er det en del av EUs politisamarbeid, og i Norge er det Justisdepartementet som har vært den varmeste forsvareren i regjeringsapparatet, noe som går klart frem av departementets nettsider om datalagring (Justisdepartementet 2011).

Hvilke tilbydere er forpliktet til å lagre data?

Direktivet forplikter "tilbydere av offentlig tilgjengelige elektroniske kommunikasjonstjenester eller tilbydere av et offentlig kommunikasjonsnettverk" til å lagre de spesifiserte trafikkdata. I Norge vil dette sannsynligvis omfatte de som Post- og teletilsynet har registrert som offentlige tilbydere, med unntak av de som bare tilbyr overføringskapasitet. Dette er imidlertid ikke avklart, og verken Post- og teletilsynet eller bransjerepresentanter kan svare på hvem som konkret vil være forpliktet til å lagre data (Teknofil.no 2011).

Hvilke data skal lagres?

Ifølge artikkel 5(1) krever direktivet at seks kategorier av data lagres. Disse omfatter data som er nødvendige for å fastslå

1. kilden til kommunikasjonen (hvem som initierte kommunikasjonen)
2. målet for kommunikasjonen (hvem som blir nådd)
3. dato, tidspunkt og varighet for kommunikasjonen
4. typen kommunikasjon (hvilken tjeneste som benyttes)
5. brukernes kommunikasjonsutstyr
6. lokasjonen til mobilt kommunikasjonsutstyr gjennom hele kommunikasjonen.

Hvilke typer kommunikasjon omfattes?

Informasjonen spesifisert over skal lagres for fem typer kommunikasjon:

1. Fasttelefoni
2. Mobiltelefoni
3. Internettilgang
4. E-post over internett
5. Internettelefoni

Tilgangen til og bruken av lagrede data

DLD ble introdusert som et markedsharmoniserende tiltak for det europeiske telekom-markedet, under det som på det daværende tidspunktet var artikkel 95 i Roma-traktaten. Dette var en del av EUs felles indre marked, eller "første søyle". Reguleringer vedrørende bruk av og tilgang til slike data ville blitt vurdert som en del av det politi- og strafferettsslige samarbeide, eller "tredje søyle" (Bignami 2007b). Følgelig inneholder DLD kun et minimum av bestemmelser for tilgang til og bruk av data.

Men noen finnes:

- Hensikten ved å lagre trafikkdataene må være begrenset til etterforskning, oppdagelse og påtale av alvorlig kriminalitet (som definert av den enkelte nasjon)
- Reglene for tilgang til og bruk av data må respektere de individuelle rettighetene i EU-lovgivning så som databeskyttelsesdirektivet (direktiv 95/46/EF), e-personsvernsdirektivet (direktiv 2002/58/EF) og EMK (se liste for forkortelser bakerst)
- Teknologinøytrale minimumskrav for sikkerhet er oppgitt, om enn svært generelle
- En offentlig myndighet skal utnevnes til å overvåke implementeringen av sikkerhet

DLD i Norge

I vedtaket fra 4. april endres ekomloven og straffeprosessloven i tråd med datalagringsdirektivet. Her defineres "alvorlig kriminalitet" til å være kriminalitet med strafferamme på over fire år, eller over tre år i kombinasjon med mistanke om organisert kriminalitet, eller for spesielle typer kriminalitet. Rettskjennelse kreves for å kunne få utlevert trafikkdata.

Det norske vedtaket inkluderer også en formulering om at myndighetene kan kreve politiattest fra personer som skal behandle lagringspliktige data hos leverandørene.

DATALAGRINGSDIREKTIVETS HISTORIE

Debatten om overvåkning og informasjonsinnhenting for kriminalitetsbekjempende formål går langt tilbake i EUs historie, men grunnlaget for det nåværende DLD regnes ofte å være et dokument kalt ENFOPOL 98 (ENFOPOL er en standard EU-forkortelse for Law Enforcement/Police, brukt for en rekke dokumenter om politisamarbeid i Europa).

ENFOPOL 98

I 1998 ble et utkast til en beslutning i Rådet angående telekom-overvåkning (Rådet 1998) diskutert på et ekspertmøte i Arbeidsgruppen for politisamarbeid. Utkastet, som også kalles ENFOPOL 98, tar for seg hvordan Rådets resolusjon om lovlig avlytting av telekommunikasjon (Council 1996) burde utvides til også å gjelde de (nokså) nye teknologiområdene kommunikasjon via mobil satellitt og internett.

ENFOPOL 98 og de påfølgende versjoner av dokumentet (ENFOPOL 19, 29 og 55) ble sterkt kritisert av menneskerettighetsorganisasjoner, og ble innstilt avvist av EU-parlamentets komité for borgerrettigheter og rettslige og indre anliggender (LIBE) (1999). Til slutt valgte Rådet ikke å vedta resolusjonen. Detaljene rundt denne avgjørelsen ble aldri klarlagt, men det ser ut til at Tysklands intervensjon var viktig (Statewatch 2002).

Utkast fra Rådet

EU-institusjonene fortsatte etter ENFOPOL-dokumentene å diskutere hvordan man kunne sikre elektroniske kommunikasjonsdata for kriminalitetsbekjempende formål i Europa, som et ledd i utviklingen av en felles, intern sikkerhetspolitikk. Innsatsen ble intensivert etter terroristangrepene i New York 11. september 2001. I et møte om rettslige og indre anliggender 20. september samme år vedtok Rådet en uttalelse angående et "spekter av tiltak for å opprettholde den høyeste sikkerhetsstandard og andre tiltak nødvendige for å bekjempe terrorisme" (Rådet 2001). Rådet anmodet Kommisjonen om å levere et forslag for å "sikre at politimyndigheter er i stand til å etterforske kriminelle handlinger som involverer bruken av elektroniske kommunikasjonssystemer".

I 2002 vedtok Parlamentet og Rådet et nytt direktiv om personvern og elektronisk kommunikasjon (*Direktiv 2002/58/EF*). Det nye direktivet ga rom for flere unntak fra den generelle plikten for teleleverandører til å slette trafikkdata som ikke lenger er nødvendig for fakturaformål.

Gjennom 2002 og 2003 arbeidet medlemslandene både gjennom Rådet og hver for seg med ulike forslag for datalagring i sine land. Ifølge personvernsorganisasjonene Statewatch og Electronic Frontier Foundation planla ni av 15 medlemsland nasjonale datalagringsreguleringer (Statewatch 2003). På samme tid (i august 2002) ble et konfidensielt utkast til en rammeavgjørelse lekket til Statewatch. Utkastet var ført i pennen av belgiske myndigheter, og inneholdt forslag til harmoniserte regler for datalagring i EU (Norton-Taylor og Millar 2002).

I 2004 ble et nytt forslag fremmet av Sverige, Frankrike, Irland og Storbritannia (Rådet 2004). Dette utkastet lignet på det lekkede, belgiske utkastet fra 2002, og inkluderte lagring av en langt mer omfattende datamengde enn det endelige utkastet. Dette gjaldt spesielt data som ble generert ved bruk av HTTP ("vanlig" bruk av nettleser). Det ble foreslått som en rammeavgjørelse under området politisamarbeid og rettslig samarbeid i kriminalsaker, eller med andre ord som et tiltak under tredje søyle, som ville krevd enstemmighet i Rådet.

Rådets forslag ble debattert og endret, og det fantes i ulike versjoner. Men det ble stilt spørsmålstegn ved den juridiske basis for forslaget, samt ved om de foreslåtte tiltakene utviste proporsjonalitet og var i tråd med menneskerettighetene. LIBE-komitéen avviste derfor forslaget i sin rapport fra mai 2005 (LIBE 2005).

Kommisjonens forslag, trialoger og raskt vedtak

21. september 2005 la Kommisjonen frem sitt eget forslag til et direktiv. Nå var det rettslige grunnlaget endret fra politisamarbeid og den tredje søylen til markedsharmonisering, artikkel 95 og den første søylen (det indre marked). Å vedta direktivet ville derfor ikke lenger kreve enstemmighet i Rådet, men på den annen siden ville Parlamentet nå bli direkte involvert gjennom medbestemmelsesprosedyren, og ikke bare konsultert, slik de ville blitt ved et vedtak under den tredje søylen.

Rådet var ikke kommet til enighet når forhandlingene med Parlamentet om endringer ble innledet sent i 2005 (Rådet 2005a). Begge muligheter for juridisk grunnlag ble holdt åpne: Et direktiv under første søyle, eller en rammeavgjørelse under tredje søyle. Dette går frem av et brev Charles Clarke, representant for det britiske presidentskapet for Rådet, skrev til Jean Marie Cavda, direktør for LIBE (Clarke 2005).

Selv om Rådet slet med å bli enige om sitt eget forslag, ble Parlamentet presset til å ta en rask avgjørelse. Brevet fra Clarke kan tolkes som en trussel: Dersom Parlamentet ikke kom til enighet før årets slutt, kunne Rådet gå tilbake til forslaget om en beslutning under tredje søyle, noe som ville holde Parlamentet helt utenfor beslutningen.

14. desember 2005 vedtok Parlamentet DLD i første behandling (EP 2005). Vedtaket inkluderte en endringspakke som man hadde kommet frem til i uformelle "trialogmøter" mellom de største partifraksjoner i Parlamentet samt Kommisjonen og Rådet før sesjonen i Parlamentet (Rådet 2005b, 2005d).

Lite demokratisk

DLD har dessverre ikke vært et utstillingsvindu for pan-europeisk demokrati, selv om det ble besluttet gjennom medbestemmelsesprosedyren. Den innledningsvise avvisningen av direktivet fra LIBE ble raskt snudd til støtte hos majoriteten i Parlamentet. Dette skjedde uten substansielle endringer i direktivet, og gjennom lite transparente trialogmøter. I trialogmøtene deltar kun de største partifraksjonene, og ingen referater publiseres offentlig. Den korte tiden fra det endelige forslaget ble lagt frem og til Parlamentet vedtok det, styrker ikke oppfatningen av en grundig demokratisk prosedyre.

Kontroversene om den juridiske basis

DLD ble implementert som et markedsharmoniserende tiltak. Men dette var, som tidligere forklart, ikke noe selvsagt valg. Det opprinnelige forslaget var å vedta DLD som en del av EUs politi- og rettssamarbeid (Bignami 2007b, s. 12). I et notat fra presidenskapet til Rådet (Rådet 2005c) erkjente de at dersom Kommisjonen gikk videre med et vedtak under tredje søyle, kunne man risikere at vedtaket ble annullert. Rettsutvalget anbefalte i mai 2005 et delt direktiv, hvor det som gjaldt harmonisering av selve lagringen av data ble implementert som et markedsdirektiv, mens det som hadde med bruk og deling av data ble implementert som en rammeavgjørelse for politi- og rettssamarbeid.

Som kjent ble det til slutt vedtatt ett direktiv under første søyle (det interne marked). Etter vedtaket trakk da også Irland saken for EU-domstolen med krav om annullering. De hevdet at det korrekte rettslige grunnlaget var det originalt foreslåtte, nemlig artiklene 31(1)(c) og 32(4)(b). Irland tapte saken (C-301/06).

Grunnen til at juridisk grunnlag var så viktig, er at det avgjør hvordan beslutningsprosessen foregår. Beslutninger under det som tidligere ble kalt første søyle krever en flertallsavgjørelse i Rådet, mens et vedtak under tidligere tredje søyle krever enstemmighet. I tillegg er det forskjellige regler for hvordan Parlamentet skal involveres.

Etter at Lisboa-traktaten trådde i kraft 1. desember 2009 er ikke spørsmålet om korrekt juridisk grunnlag for DLD like relevant lenger. Det meste av det som tidligere ble definert som EUs tredje søyle er slått sammen med den tidligere første søyle. Dette går nå gjennom den "ordinære lovgivende prosedyre", hvor en kvalifisert majoritet i de fleste tilfeller er nok til å sikre vedtaket, og hvor Parlamentet har medbestemmelsesrett.

Fremover bør det derfor være mulig å inkludere flere reguleringer også når det gjelder tilgang til og bruk av data i direktivet. Dette kan gi rom for å eliminere eller i hvert fall redusere konfliktene med EMK. Generelt vil det bety at man ikke er begrenset av markedsregulering for å regulere et sikkerhetstiltak.

STATUS FOR IMPLEMENTERING

Ifølge direktivets tekst var medlemslandene forpliktet til å innføre DLD i nasjonal lovgivning innen 15. september 2007. Medlemslandene kunne be om utsettelse frem til 15. mars 2009 for internettrelaterte trafikkdata.

Status for implementering september 2011

Etter at Østerrike vedtok implementering av direktivet i slutten av april 2011, er det nå fem land hvor direktivet ikke er vedtatt (eller er vedtatt, men avvist av høyesterett eller tilsvarende som grunnlovsstridig). I tillegg er det to land, Ungarn og Irland, hvor prosesser mot direktivet pågår i rettsvesenet.

- I **Belgia** er direktivet kun delvis innført som en del av lovgivning som stammer fra 2005, altså før DLD ble innført. Belgias problemer med å få vedtatt nasjonal DLD-lovgivning skyldes først og fremst andre politiske problemer i landet.
- I **Tsjekkia** ble loven annulert i mars 2011, og ingen ny lov er på plass.
- I **Romania** ble loven annulert i oktober 2009, og ingen ny lov er på plass.
- I **Tyskland** ble loven annullert 2. mars 2010, og alle data som var lagret på basis av denne loven måtte slettes. I juni 2011 har ennå ikke koalisjonspartnerne i den tyske regjeringen blitt enige om en ny lov (Spiegel Online 2011b).
- I **Sverige** er nasjonal lov for å implementere direktivet ennå ikke vedtatt.
- I **Ungarn** er den nasjonale loven som implementerer DLD klaget inn for rettsvesenet, og venter på behandling.
- I **Polen** ble tilgangen til lagrede data klaget inn for rettsvesenet i februar 2011.
- I **Irland** pågår saken også i rettsvesenet. Høyesterett har videresendt spørsmål om lovligheten av DLD i lys av EMK til EU-domstolen.

Selv om de fleste land nå har innført direktivet, er det store sprik i *hvordan* direktivet er innført.

Manglende implementering klages inn til EU-domstolen

Når et land ikke implementerer et direktiv innen tidsfristen, kan Kommisjonen gå til juridiske skritt mot medlemslandet, under artikkel 258 og artikkel 260 i TFEU. Dette involverer i første omgang en uformell forespørsel for å få mer informasjon om saken, slik at den kan undersøkes nærmere. Dersom et avtalebrudd avdekkes, må Kommisjonen gi en begrunnelse, som inkluderer en tidsfrist for medlemslandet å etterleve regelverket. Dersom dette ikke fører fram, kan Kommisjonen oversende saken til EU-domstolen, som i siste instans kan ilegge bøter i form av éngangsbeløp eller dagsbøter inntil direktivet implementeres (Fairhurst 2010, s. 208).

Selv om implementeringen av et direktiv dømmes til å være i strid med grunnloven i et medlemsland får ikke medlemslandet unntak fra plikten til å innføre direktivet. Kommisjonen har gått til slike skritt mot flere av landene som har vært trege til å innføre DLD. Sakene mot Hellas og Nederland ble trukket etter at de implementerte direktivet. Men sakene mot Østerrike og Sverige ble oversendt EU-domstolen, som dømte dem for ikke å ha implementert direktivet (EU-domstolens sak C-185/09). Sverige har ennå ikke innført direktivet, og Kommisjonen har sendt saken deres tilbake til EU-domstolen, denne gangen med en anbefaling om å ilegge landet bøter (Kommisjonen 2011b). Østerrike har nå vedtatt sin nasjonale implementeringslov, og unngår dermed videre forfølgelse i EU-domstolen.

Kommisjonen har uttrykt at den vil fortsette å gå til rettslige skritt mot land som ikke implementerer

direktivet, om nødvendig (Kommisjonen 2011a). Det virker nå klart at Kommisjonen vil klage inn Tyskland for EU-domstolen, dersom de ikke kan vise til en konkret plan for snarlig implementering (Spiegel Online 2011a).

Innvendinger mot DLD

DLD har blitt beskyldt for å være inkonsistent med annen EU-lovgivning, så som EMK. Og i flere medlemsland stilles spørsmål ved om DLD er i tråd med nasjonal grunnlov, eller om nasjonale domstoler må avvise direktivet når det implementeres. I tillegg har mange ideologiske og prinsipielle innvendinger mot direktivet, uavhengig av hva de spesifikke regelverk sier.

Innføringen av DLD byr også på praktiske problemer. Det innføres på forskjellige måter i de ulike landene, og det er ingen som har noen god oversikt over de økonomiske konsekvensene. Det er heller ikke gjort noen utredning av effekten av direktivet, selv om EU har lovet at dette skal komme. I en uttalelse fra september 2011 om Kommisjonens evaluering av direktivet, konkluderer det europeiske datasikkerhetstilsynet (EDPS) meget klart med at direktivet ikke oppfyller formålet om markedsharmonisering, det oppfyller ikke nødvendige krav til personvern, og Kommisjonen rådes til enten å forkaste hele direktivet, eller i det minste fullstendig revurdere det (EDPS 2011).

Minimums- eller maksimumsstandard?

Så langt har kommisjonen kun gått til rettslige skritt mot land som ikke har innført DLD. Den har ikke gjort det samme mot land som har implementert DLD i uoverensstemmelse med direktivets retningslinjer.

Danmark er et eksempel på et land hvor massive datamengder lagres i tillegg til de som spesifiseres i direktivet. Andre land har andre typer utvidede datalagringsordninger (Kommisjonen 2011a, s. 7). Dersom Kommisjonen fortsetter å straffe kun de land som ikke går langt nok i sin nasjonale lovgivning, vil DLD bli en de facto minimumsstandard for datalagring. Dersom et land kan pålegge telekomleverandører å lagre data som ikke er spesifisert i direktivet, er det opprinnelige målet om markedsharmonisering fullstendig forlatt. Dette er også en av konklusjonene i EDPS' uttalelse (EDPS 2011, s. 9): "The Evaluation report shows that the Directive has failed to meet its main purpose, namely to harmonise national legislation concerning data retention."

Direktivet beskyldes også for at toårsgrensen for å lagre data ikke er en reell maksimumsgrense. Direktivet bygger nemlig på e-personvernsdirektivet fra 2002. I dette direktivet gis det anledning til å lagre data lenger dersom det foreligger "særskilte grunner" for det. Slike "særskilte grunner" er ikke videre spesifisert, og mange hevder derfor at en hvilken som helst grunn fra et lands myndigheter kan være en særskilt grunn.

Personvern og DLD

Et grunnleggende problem i en liberal rettsstat er balansegangen mellom frihet og beskyttelse. Når en borgers fysiske eller økonomiske sikkerhet er truet, er det politi- og sikkerhetsmyndighetenes oppgave å beskytte denne sikkerheten. Dette vil i de aller fleste tilfeller føre til at myndighetene søker informasjon som de kan bruke til å avverge eller undersøke kriminell aktivitet. Ofte må retten til personvern vike dersom myndighetene skal få tilgang til informasjonen de har behov for. Spørsmålet er hvilke tilfeller av faktiske eller potensielle brudd på sikkerheten som rettferdiggjør hvilke metoder for informasjonsinnhenting.

Respekten for personvern har dype røtter i europeisk kultur, og er grunnlaget for blant annet posthemmelighetsprinsippet, som også omfatter elektronisk korrespondanse, som er beskyttet

av grunnloven eller har sterk presedens i de aller fleste europeiske land. Mange europeiske land har i tillegg hatt separate data- og personvernslover siden 70-tallet, når mulighetene for storskala datainnhenting og –prosessering ekspanderte i takt med spredningen av datamaskiner. Disse rettighetene er en del av et større sett sentrale rettigheter i liberale demokratier.

DLD og annen EU-lovgivning

All sekundær EU-lovgivning må harmonere med EUs charter for fundamentale rettigheter og EMK (Feiler 2010). Etter hvert finnes mye presedens for at artikkel 8 i EMK betyr at prosessering av personlige data i kriminalitetsbekjempende øyemed utgjør et inngrep i privatlivets fred (Bygrave 1998). Det er derfor bare tillatt med slik prosessering dersom tre betingelser er tilfredsstilt, nemlig

1. forankring i lovverket
2. legitimt formål
3. proporsjonalitet og nødvendighet

Det er lite tvil om at DLD har grunnlag i skriftlig og allment tilgjengelig lovverk. Formålet, å bekjempe alvorlig kriminalitet, oppfattes også som legitimt. Det er det tredje prinsippet som skaper mest debatt. En vanlig tolkning av proporsjonalitet og nødvendighet er at det må finnes bevis for at handlingen faktisk fyller den oppgitte hensikten, og at det ikke finnes alternative måter å oppnå denne hensikten på som ville medført mindre inngrep i privatlivets fred.

Akademikerne er uenige. Bignami (Bignami 2007a) konkluderer med at DLD beskytter rettighetene som er gitt i EMK. Lukas Feiler (Feiler 2010) kommer frem til det motsatte, nemlig at DLD verken er et proporsjonalt eller nødvendig tiltak. Dette er den samme konklusjonen som Jon Wessel-Aas har kommet til (Wessel-Aas 2010). Han konkluderer med at det er lite sannsynlig at DLD ville blitt frikjent i en sak i EMD.

EDPS på sin side konkluderer i sin uttalelse med at direktivet ikke møter kravene til personvern og datasikkerhet, ettersom nødvendigheten av direktivet ikke er bevist, og fordi det finnes andre måter å regulere datalagring på som griper mindre inn i privatlivets fred (EDPS 2011, s. 9).

EU-domstolen vil snart bli nødt til å ta stilling til om DLD strider mot menneskerettighetene. EU er riktignok ikke direkte part i EMK. Men EUs charter om fundamentale rettigheter forutsettes å inneholde samme beskyttelse som EMK, og EU-domstolen bruker også praksis fra EMD som rettskilde for å tolke dette charteret. I saken som Digital Rights Ireland (DRI) har anlagt i irsk høyesterett, har spørsmålet om direktivets eventuelle konflikt med grunnleggende rettigheter blitt oversendt EU-domstolen, som dermed må ta stilling til dette spørsmålet.

DLD og nasjonal lovgivning

EU-direktiver er ikke automatisk gjeldende lov i medlemslandene. De er derimot forpliktelser på medlemslandene til å ha nasjonal lovgivning som oppfyller de substansielle kravene i direktivene (Fairhurst 2010, s. 65). De substansielle kravene i DLD innebærer i praksis obligatorisk lagring av datatypene listet i direktivets artikkel 5 i minst seks måneder.

Som beskrevet tidligere har den nasjonale lovgivningen som implementerer DLD blitt underkjent i flere land. De nasjonale domstolene har ikke myndighet til å underkjenne selve EU-direktivet; dette er EU-domstolens myndighet alene. Men det er allikevel interessant å se hvilke deler av direktivet som i praksis har blitt underkjent i de ulike landene.

I Romania og Tsjekkia er det selve den obligatoriske, universelle lagringen av data som har blitt kritisert. Denne kritikken går direkte til direktivets kjerne. Det er derfor vanskelig å se for seg hvordan DLD kan bli implementert i disse landene uten at grunnloven endres (EDRi 2011a).

I den ganske lange og kompliserte dommen fra den tyske, føderale forfatningsdomstolen, står det at lagringen av data i seg selv ikke *nødvendigvis* er i konflikt med den tyske forfatningen (Grundgesetz) (Bundesverfassungsgericht 2010). Forfatningsdomstolen har for øvrig en lang historie med å balansere mellom samarbeid og skepsis til europeisk integrasjon, og dommen må derfor sees i sammeheng med andre avgjørelser (Bäcker 2011). Den tyske avgjørelsen sies å være et mesterverk i å unngå direkte konflikt med EU.

Prinsipielle innvendinger

Uavhengig av hvorvidt DLD strider mot EMK eller nasjonal lovgivning har menneskerettighets-organisasjoner kommet med innvendinger mot direktivets inngripen i privatlivets fred. Striden står blant annet om hvorvidt direktivet bryter uskyldspresumpsjonen som er grunnleggende i en liberal rettsstat, hvorvidt borgerne mister bestemmelsesretten over sin private informasjon, om DLD vil medføre en såkalt chilling-effekt, og hvorvidt direktivet kan være en trussel mot ytringsfriheten.

Uskyldspresumpsjonen

DLD beskyldes for å bryte uskyldspresumpsjonen. Med DLD blir en svært stor mengde svært private data samlet om mennesker som ikke er beskyldt, eller engang mistenkt, for å ha gjort noe ulovlig. I følge motstanderne snus uskyldspresumpsjonen på hodet: Informasjon om din personlige kommunikasjon lagres i tilfelle du gjør, eller mistenkes for å gjøre, noe kriminelt i fremtiden.

Bestemmelsesrett over personlig informasjon

Tilhengere av DLD hevder at dersom du ikke har noe å skjule, har du ingenting å frykte. Det finnes imidlertid en rekke eksempler på informasjon som ikke har med lovbrudd å gjøre, men som man allikevel ønsker å skjule. Eksempler er seksuelle eller andre personlige preferanser, religiøs overbevisning eller helsetilstand. Ergo er det mange som både har noe å skjule og frykte, uten at de har brutt loven. Det er nettopp som en følge av dette at personvernslovgivning slår klart fast at du selv skal ha kontroll over personlig informasjon og hvem du ønsker å dele denne med.

Ikke noe system kan være perfekt. Det vil alltid eksistere en risiko for misbruk av informasjon. I tilfellet DLD kan dette enten skje ved uautorisert tilgang til data, eller at data brukes til andre formål enn hensikten. Det vil derfor alltid være slik at selv om man ikke har gjort noe ulovlig kan informasjonsinnhentingen som er ment for å beskytte deg bli brukt mot deg. Selv det man tror er helt sikre systemer kan være utsatt for risiko. Eksempler fra nyere tid som viser dette er for eksempel de mange Wikileaks-lekkasjene, eller hackingen av GSM-nettet i 2009.

Chilling-effekten

Det at man *tror* man blir eller kanskje blir overvåket kan i seg selv være en trussel mot det frie samfunnet. Den såkalte chilling-effekten gjør at personer endrer sin oppførsel når de opplever potensiell overvåkning. En studie utført i Tyskland viste at mer en halvparten av personene som visste hva DLD var, ville avstå fra å kontakte funksjoner som ekteskapsrådgivning eller psykologhjelp via fasttelefon, mobiltelefon eller e-post (Forsa 2008). Dette viser at selv om man er en lovlydig borger og ikke har noe å frykte, og selv om systemet i realiteten skulle være vanntett, vil personer endre sin oppførsel på en måte som er til skade for individet selv eller for samfunnet.

Ytringsfrihet
Journalister har klaget høylytt over at DLD setter ytringsfriheten i fare. DLD medfører at kommunikasjon med kilder via telefon eller e-post senere kan bli brukt i en etterforskning eller rettssak for å spore kilden. Dette kan gjøre undersøkende journalistikk vanskeligere, og potensielt være til hinder for å avdekke uønskede samfunnsforhold eller kriminalitet, ettersom kildenes anonymitet ikke lenger kan sikres.

Det finnes også mer direkte eksempler på at DLD truer ytringsfriheten. I Polen skal myndighetene ha vist spesiell interesse for trafikkdata lagret på grunn av DLD for journalister som dekker politisk sensitive hendelser (thenews.pl 2010).

Praktiske problemer ved innføring

Ettersom direktivet er et resultat av mange vanskelige kompromisser, mangler teksten definisjoner og spesifikasjoner av en rekke viktige konsepter. Dette fører til at det er nødvendig å tolke direktivet før det innføres, og ulike tolkninger fører til ulik nasjonal lovgivning.

Hva skal lagres?

I artikkel 5(2) i direktivet står det at ”ingen data som avslører innholdet i kommunikasjonen kan lagres som følge av dette direktivet”. Men dette er det umulig å tolke bokstavelig. Det finnes en rekke tilfeller hvor det å vite avsender og mottaker for kommunikasjonen langt på vei også kan avsløre innholdet. Direktivet må derfor tolkes som at ingen data som *direkte* avslører innholdet i kommunikasjonen kan lagres som følge av direktivet, ellers kunne man ikke ha lagret noe. Men i hvilken grad implementeringen kan tillate at innholdet *indirekte* blir avslørt sier direktivet ingenting om.

Videre er det problematisk at datatypene som skal lagres ikke er klart spesifisert i selve direktivet. I artikkel 2(1) i DLD referes det til det såkalte Framework Directive hvor noen videre definisjoner kan finnes. I tillegg må man når man tolker direktivet gå ut fra at det bygger på andre standarddefinisjoner i EU.

De konkrete begreper man må finne ut hva betyr omfatter spesielt ”internett-epost” og ”internettelefoni”. Om man følger europeiske standarddefinisjoner, utelater disse begrepene en lang rekke kommunikasjonsmetoder via internett fra direktivet (Feiler 2010). Noe av det som utelates er kommunikasjon via sosiale medier (Facebook, Twitter og lignende), direkte chat (MSN, IRC og lignende), diskusjoner på blogger og andre diskusjonsfora samt all http-trafikk generelt, inkludert webmail-tjenester som Google Mail og Hotmail.

Denne tolkningen deles ikke av alle som har innført direktivet. For eksempel lagres i Danmark alle internett-sesjoner operatører i mellom, og mellom operatør og bruker, ikke bare de sesjoner som omhandler e-post (Justisministeriet 2006).

Både tilhengere og motstandere av direktivet har kritisert inkonsistensen i typene kommunikasjon som dekkes av direktivet. Dersom trafikkdata for telefonsamtaler og e-post er essensielle (nødvendige) for å bekjempe alvorlig kriminalitet, hvorfor lagres ikke trafikkdata for chatting eller Facebook-diskusjoner? For stadig flere er nettopp denne typen alternativ kommunikasjon minst like viktig som telefon og vanlig e-post. Dermed er det også sannsynlig at trafikkdata fra disse kommunikasjonskanalene ville være minst like nyttig i kampen mot alvorlig kriminalitet.

Bruk og tilgang
DLD ble som tidligere beskrevet innført som et markedsharmoniserende tiltak. Det er derfor det mangler spesifikasjoner angående tilgang til og bruk av data. Ifølge rapporten fra WP29 varierer denne biten betraktelig mellom ulike land. Systemene for utveksling av data mellom teleoperatører og myndigheter fungerer svært ulikt, og med ulik grad av sikkerhet. I enkelte land har data blitt overført ukryptert og via usikre kanaler som vanlig e-post eller til og med telefax (Article 29 Data Protection Working Party 2010, s. 14).

Direktivets effektivitet

For å kunne undersøke effekten av DLD på bekjempelse av kriminalitet måtte man som et minimum kunne se på oppklaringsrater før og etter implementering, eller sammenligne land med og uten DLD. Slike undersøkelser finnes det svært få av, og kommisjonens egen evaluering (Kommisjonen 2011a) gjør ingen slike sammenligninger.

Statistikk versus anekdoter
Direktivet forplikter medlemslandene til å levere statistikk for antallet forespørsler etter data, men ikke for hvorvidt det faktisk bidrar til å oppdage, etterforske, oppklare eller påtale alvorlig kriminalitet. Den statistikken som foreligger så langt angående forespørsler er av dårlig kvalitet. Kun i enkelte tilfeller er det mulig å splitte de rapporterte forekomster på trafikkdataenes alder eller type kommunikasjon, og mange land har ikke levert statistikk i det hele tatt. Noen land, som Polen, rapporterer forespørsler som gjelder de samme data men ulike telekom-leverandører mange ganger, slik at det ikke er mulig å sammenligne eller aggregere dataene direkte. På grunn av dataenes dårlige kvalitet går det derfor ikke an å gjøre kvantitative analyser av direktivets effekt basert på de innsamlede dataene.

I Kommisjonens evaluering gis det en del eksempler på situasjoner hvor lagrede data har bidratt til å løse kriminalsaker. Dette gir lite annet enn anekdotiske bevis på at noen ganger kan det å ha kommunikasjonsdata være til hjelp for å oppklare kriminalitet.

Hvorvidt sakene kunne vært løst uten direktivet sier anekdotene ingenting om. Noen eksempler i rapporten er til og med fra land som ikke har implementert DLD. Langt mindre gir rapporten noe svar på om oppklaringen av saker ved hjelp av trafikkdata står i forhold til de økte kostnadene både for personvernet og rent økonomisk.

I et brev til Kommisjonen initiert av European Digital Rights (EDRi), datert 26. september 2011, krever 34 europeiske NGO'er, inkludert blant andre AKVorrat, Electronic Frontier Foundation, European Federation of Journalists, Privacy International og Statewatch bevis for at direktivet faktisk bidrar til å bekjempe kriminalitet (EDRi 2011b).

Enkelt å omgå direktivet
Det finnes en rekke teknikker for å unngå DLD, både for internettbruk og telefonbruk. For internett-bruk vil en VPN-tilkobling, et offentlig eller ikke-beskyttet trådløst nettverk eller en anonymiseringstjeneste som Tor (http://www.torproject.org) sørge for at trafikkdata ikke kan lagres, eller i det minste ikke kan spores tilbake til kilden. Som nevnt tidligere skal det også holde å benytte web-basert e-post eller chatte-tjenster for å unngå direktivet, men dette er avhengig av implementeringen i det enkelte land. For telefonbruk kan anonyme, forhåndsbetalte SIM-kort benyttes for å unngå at dataene kan spores direkte til brukeren. Disse kortene selges fremdeles i en rekke land i Europa, selv om forbud diskuteres.

I det store og det hele er det enkelt å unngå DLD, og svært enkelt for internett. Dette vil sannsynligvis redusere direktivets effekt mot kriminalitet. Tiltak for å unngå direktivet kan riktignok føre til noen ulemper for brukeren, så som noe lavere innlastingshastigheter, men få eller ingen funksjonelle begrensninger. Etter hvert som direktivet implementeres i stadig flere land er det også å vente at metodene for å omgå det vil bli enklere å utføre, bli bedre kjent og medføre færre ulemper for brukeren. Spesielt når det gjelder godt planlagt og alvorlig kriminalitet som terroristangrep er det forventet at de kriminelle vil ta forholdsregler angående sin kommunikasjon.

Mange vil da spørre seg hva som er vitsen med å lagre trafikk fra "gammeldags" e-posttrafikk (som er det som omfattes av EUs definisjon), all den tid det kun utgjør en liten andel av all den skriftlige kommunikasjonen som foregår på nett, og man lett kan bytte til andre kommunikasjonsmåter ved innføring av direktivet.

Økonomiske effekter

En annen svakhet ved direktivet er at det ikke ble (offentlig-) gjort noen kost/nytte-analyse før direktivet ble vedtatt. Ingen visste hva sikker lagring av data og sikre systemer for tilgang og overføring ville koste, og ingen felles politikk for tilbakebetaling av telekom-selskapenes kostnader ble utformet.

Tilbakebetaling av kostnader

I LIBE-komitéens rapport om det foreslåtte direktivet (LIBE 2005) ble behovet for komplett og harmonisert tilbakebetaling av kostnader understreket, på grunn av de potensielle skadevirkningene på rettferdig konkurranse dersom dette varierte fra land til land.

I rapporten fra WP29 pekes det på at den manglende felles politikken på dette området har ført til store forskjeller mellom land. I noen land tilbakebetaler myndighetene alle kostnader, i andre får leverandørene ingen kostnader dekket. Dette fører til en direkte motsetning mellom direktivet i praksis og dets markedsharmoniserende intensjon.

Små selskaper og sikkerhet

I land hvor kostnadene ikke dekkes (fullt ut), lider små teleselskaper under negative skalaeffekter. Dette kan føre til større inngangsbarrierer i bransjen. I tillegg har dette i følge WP29 ført til at noen av de små telekomleverandørene tar færre forholdsregler for de lagrede data, for å holde kostnadene nede (Article 29 Data Protection Working Party 2010).

Kommisjonen innrømmer i sin evaluering at ulike regimer for tilbakebetaling av kostnader er et problem, og vurderer å "sikre at leverandører får konsekvent tilbakebetaling for kostnader de pådrar seg" (Kommisjonen 2011a, s. 28).

Et felles regime for tilbakebetaling av kostnader ville flyttet kostnadene ved datalagring over på nasjonalbudsjettene. Dette ville jevne ut konkurransen, samt gjøre det mulig å vurdere kostnadene i forhold til den økte sikkerheten man oppnår.

UTFORDRINGER FOR DLD I NORGE

I Norge bør man ta inn over seg kritikken og problemene ved direktivet når man innfører den nasjonale lovgivningen. Det norske lovvedtaket lider stort sett av de samme mangler som det originale direktivet. For eksempel inneholder det ingen definisjon av de fem datatypene som skal lagres i det norske lovvedtaket, eller henvisning til slik definisjon, og kravene til sikkerhet er ikke spesifisert.

Følgende punkter kan oppsummere hva de norske myndigheter bør ta hensyn til i det videre arbeidet med forskrifter og praktisk implementering av DLD:

- Det norske vedtaket bør legge seg på minimumsløsningen, ikke bare for perioden data lagres hos leverandør, men også når det gjelder hvilke data som lagres. Norge bør også protestere dersom andre land pålegger telekomleverandørene lengre langringstid eller en utvidet forståelse av hvilke data som skal lagres.
- Norge må sørge for at kun state-of-the-art sikkerhetsløsninger benyttes for kommunikasjon mellom politimyndigheter og telekomleverandører. Selv om "full sikkerhet" aldri kan oppnås, må myndigheter og leverandører gjøre alt som står i sin makt for å sørge for sikkerhet når det gjelder forespørsel og overlevering av data. Norge bør snarest som et minimum vedta en forskrift om at all slik kommunikasjon skal være kryptert.
- Det må være klare og konsise retningslinjer for behandling, oppbevaring og sletting av data etter at de er overlevert politiet. Per i dag er det helt uvisst hva som skjer eller kan skje med data etter at de er utlevert.
- Både for telekomselskapenes og politiets bruk av data må det være streng adgangskontroll, samt logging av alle tilfeller hvor data er lest.
- Norske myndigheter må føre en nøyaktig, detaljert og informativ statistikk for bruk og nytte av lagrede data. Spesielt viktig er det å analysere hvilken effekt direktivet har, sammenlignet med reglene som gjaldt før direktivet. Det er derfor viktig å kartlegge nåsituasjonen slik at man senere kan sammenligne.
- Norske myndigheter bør dekke alle kostnader knyttet til implementering av direktivet hos telekomleverandørene. Dette er spesielt viktig for at små leverandører ikke skal oppleve en urettferdig ulempe, eller eventuelt fire på kravene til sikkerhet.
- På bakgrunn av de siste punkter bør norske myndigheter utføre grundige kost-/nytteanalyser for direktivet, og delta aktivt både med disse og andre erfaringer i EUs evalueringsprosess.
- Før innføring av den nye loven må det utarbeides en komplett og detaljert oversikt over hvilke data som lagres, når og hvordan. Denne oversikten må være teknisk nøyaktig, samtidig som den må være enkelt tilgjengelig for ikke-teknologer. Alle har krav på å vite nøyaktig hvilken informasjon som blir lagret om deres kommunikasjon.
- Sletteplikt må spesifiseres, også for data som er hentet ut av politimyndighetene.
- Det må gå klart frem hvordan man vil håndtere eventuelle utvidelser eller innstramninger i direktivet, for eksempel dersom EU går inn for endringer i direktivet. Dette må man ta høyde for når man utvikler de tekniske løsningene.
- Det må utføres en grundig vurdering av hvordan man skal bedømme kvaliteten på de lagrede data. Hvordan skal man luke ut data som er misvisende? Universitetet i Oslo trekker i sin høringsuttalelse om DLD frem Baneheia-saken: Ifølge trafikkdata fra den drapsdømtes mobil befant han seg ikke på åstedet, men hjemme, der han selv hevdet å ha vært. Retten så i dommen bort fra disse bevisene, altså ble mobildataene ansett som misvisende. Hvordan vil politiet sørge for at man ikke står overfor en tilsvarende situasjon som i Baneheia, og sjekker ut folk som faktisk kan ha noe med saken å gjøre?

Hvordan den norske løsningen forholder seg til disse punktene går ikke klart frem av lovforslaget. Regjeringen bør legge frem detaljene i god tid før lagring skal iverksettes.

Notatet er skrevet av prosjektmedarbeider i Civita, Anne Siri Koksrud. annesiri@civita.no

FORKORTELSER

DLD	Datalagringsdirektivet
EDRi	European Digital Rights
EDPS	The European Data Protection Supervisor (Det europeiske datasikkerhetstilsynet)
EF	Det Europeiske Fellesskap (fellesmarkedet)
EMD	Den Europeiske Menneskerettighetsdomstolen
EMK	Den Europeiske Menneskerettighetskonvensjonen
EØS	Det europeiske økonomiske samarbeidsområde
Kommisjonen	Europakommisjonen
LIBE	EU-parlamentets komité for borgerrettigheter og rettslige og indre anliggender (Civil Liberties, Justice and Home Affairs)
Parlamentet	Europaparlamentet (det europeiske parlament)
TFEU	Treaty on the Functioning of the European Union (tidligere Treaty Establishing the European Community, eller Roma-traktaten)
TEU	Treaty on European Union (Maastricht-traktaten)
HTTP	Hypertext transfer protocol
LIBE	The Committee on Civil Liberties, Justice and Home Affairs (komitéen for borgerrettigheter og rettslige og indre anliggender)
Rådet	Rådet for Den europeiske union (tidl. Ministerrådet)

OVERSETTELSER

Rammeavgjørelse	Framework Decision
Rettslige og indre anliggender	Justice and Home Affairs
Arbeidsgruppen for politisamarbeid	Working Party on Police Cooperation
Første behandling	First Reading
Rettsutvalget	Committee on Legal Affairs

LITTERATUR

Article 29 Data Protection Working Party. 2010. Report 01/2010 on the second joint enforcement action.

Bignami, Francesca. 2007a. Privacy and Law Enforcement in the European Union: The Data Retention Directive *Chicago Journal of International Law* 8.

———. 2007b. Protecting Privacy Against the Police in the European Union: The Data Retention Directive. *Duke Law School Research Paper* No. 13.

Bundesverfassungsgericht. 2010. Data Retention Case. *1 BvR 256/08, March 2nd 2010*. Available from http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html.

Bygrave, Lee A. 1998. Data protection pursuant to the right to privacy in human rights treaties. *International Journal of Law and Information Technology* 6 (3).

Bäcker, Matthias. 2011. Solange IIa oder Basta? Das Vorratsdaten-Urteil des Bundesverfassungsgerichts aus europarechtlicher Sicht. *Europarecht* 46 (1):103-120.

Clarke, Charles. 2005. Letter to Jean Marie Cavada MEP, Chairman, LIBE Committee, October 17th 2005.

Committee on Civil Liberties and Internal Affairs. 1999. Report on the draft Council Resolution on the lawful interception of telecommunications in relation to new technologies. *A4-0243/99, 23.04.1999*.

Council. 1996. Council Resolution of 17 January 1995 on the lawful interception of telecommunications. *Official Journal 96/C 329/01*.

EDPS. 2011. Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC). *OJ C 279, 23.9.2011, p. 1-10*.

EDRi. 2011. *EDRi-gram: Czech Constitutional Court rejects data retention legislation* 2011a [cited April 9th 2011]. Available from http://edri.org/edrigram/number9.7/czech-data-retention-decision.

———. 2011b. Letter to Commissioner Malmström. Available from http://www.statewatch.org/news/2011/sep/eu-mand-ret-ngo-letter-to-com.pdf.

EP. 2005. European Parliament legislative resolution on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC. *A6-0365/2005, 28.11.2005*.

Europa-Parlamentets og Rådets direktiv 2002/58/EF om behandling av personopplysninger og beskyttelse av privatlivets fred i den elektroniske kommunikasjonssektor (Direktiv om databeskyttelse innenfor elektronisk kommunikasjon).

Europa-Parlamentets og Rådets Direktiv 2006/24/EF av 15. mars om lagring av data fremkommet ved bruk av offentlig elektronisk kommunikasjonstjeneste eller offentlig elektronisk kommunikasjonsnett og om endring av direktiv 2002/58/EF.

Fairhurst, John. 2010. *Law of the European Union*. Harlow: Pearson/Longman.

Feiler, Lukas. 2010. The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection. *TTLF Working Paper* No. 7.

Forsa. 2008. Meinungen der Bundesbürger zur Vorratsdatenspeicherung.

Justisdepartementet. 2011. *Datalagring* 2011 [cited 11. juli 2011]. Available from http://www.regjeringen.no/nb/dep/jd/tema/kriminalitetsbekjempelse/datalagring.html?id=632963.

Justisministeriet. 2006. Vejledning til bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) In *VEJ nr 74 af 28/09/2006*.

Kommisjonen. 2011a. Evaluation report on the Data Retention Directive (Directive 2006/24/EC). *COM(2011) 225 final, 18.04.2011*.

———. 2011b. Press release: Data retention: Commission refers Sweden back to Court for failing to transpose EU legislation *IP/11/409, 6.4.2011*.

LIBE. 2005. Report on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC. *2005/0182(COD), 28.11.2005*.

Norton-Taylor, Richard, og Stuart Millar. 2011. *Privacy fear over plan to store email – EU wants data retained to help fight against crime*. The Guardian 2002 [cited April 23rd 2011]. Available from http://www.guardian.co.uk/uk/2002/aug/20/eu.digitalmedia/print.

Rådet. 1998. Interception of telecommunications – Draft Council Resolution on new technologies. *10951/1/98, 04.11.1998*.

———. 2001. Conclusions adopted by the Council (Justice and Home Affairs) Brussels, 20 September 2001. *SN 3926/6/01, 20.09.2001*.

———. 2004. Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism. *8958/04, 28.04.2004*.

———. 2005a. Note from Presidency to Coreper: Data Retention: Discussions with the European Parliament. *14023/05, 08.11.2005*.

———. 2005b. Note from Presidency to Coreper: Data retention: trialogue discussions with the European Parliament. *14328/05, 16.11.2005*.

———. 2005c. Note from Presidency to Council on Data Retention. *13036/05, 10.10.2005*.

———. 2005d. Note from Presidency to Delegations: Data Retention. *14935/05, 24.11.2005*.

Samferdselsdepartementet. *Høring - datalagring* 2010. Available from http://www.regjeringen.no/nn/dep/sd/dokument/hoyringar/Hoyringsdokument/2010/horing---datalagring/Horingsuttalelser.html?id=590002.

Spiegel Online. 2011. *EU drängt Deutschland zu Datensammelei* 2011a [cited June 24 2011]. Available from http://www.spiegel.de/netzwelt/netzpolitik/0,1518,769773,00.html.

———. 2011. *Justizministerin stellt sich gegen Innenminister* 2011b [cited June 24 2011]. Available from http://www.spiegel.de/netzwelt/netzpolitik/0,1518,769876,00.html.

Statewatch. 2011. *EU surveillance of telecommunications – Mystery of the missing minutes which surface nearly a year late* 2002 [cited April 25th 2011]. Available from http://www.statewatch.org/news/2002/apr/11enfo.htm.

———. 2011. *EU – Majority of governments introducing data retention of communications* 2003 [cited April 17th 2011]. Available from http://www.statewatch.org/news/2003/jan/12eudatret.htm.

Teknofil.no. *Datalagringsdirektivet: Aner ikke hva Stortinget har vedtatt* 2011. Available from http://www.teknofil.no/artikler/datalagringsdirektivet/93641.

thenews.pl. 2011. *Journalists' phones monitored in politically inspired investigation?* 2010 [cited April 24th 2011]. Available from http://www.thenews.pl/national/artykul141157_journalists-phones-monitored-in-politically-inspired-investigation.html.

Wessel-Aas, Jon. 2010. Datalagringsdirektivet – er dets krav om lagring av trafikkdata forenlig med Den europeiske menneskerettighetskonvensjonen? In *Overvåking i en rettsstat*, edited by D. W. Schartum. Bergen: Fagbokforlaget.