Høringsuttalelse

om

Datalagringsdirektivet

fra

Troms Nei til EU

Datalagringsdirektivet og EØS-relevans

Av Artikkel 1 i Datalagringsdirektivet framgår det hva som er formålet med direktivet:

> *"1. This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect of the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law."*

Formålet med direktivet er altså å harmonisere lovgivningen om lagring av data framkommet ved bruk av elektronisk kommunikasjon i den hensikt å sikre at data er tilgjengelige for etterforskning, oppklaring og rettsforfølging av alvorlig kriminalitet. EØS-avtalen omfatter ikke justisområdet innenfor EU-retten, så direktivet er derfor etter vårt syn ikke EØS-relevant.

Vi er kjent med EF-domstolens beslutning av 10. februar 2009, sak C-301/06, som sier at artikkel 95 i EF-traktaten er riktig hjemmel for direktivet. Der pekes det på at ulik praksis i medlemslandene når det gjelder krav til lagring gir ulike kostnader for tilbyderne, og dermed har direkte betydning for det indre marked.

Men også direktivet åpner for store forskjeller mellom land når det gjelder implementering. Lagringstiden kan variere fra 6 måneder til 2 år, landene kan selv bestemme om staten eller kundene må betale for lagringen, om lagringen skal skje sentralt eller hos den enkelte tilbyder, hvordan dataene skal være formatert, hvilke sikkerhetskrav som skal stilles til lagringen, krav til kryptering osv.

Alle disse forskjellene svekker troverdigheten av begrunnelsen for at det er et indre marked-direktiv. Svaret er nærliggende: Fordi daværende EU-rett tilsa enstemmighet på justisområdet, valgte man å legge artikkel 95 til grunn for å få direktivet vedtatt med kvalifisert flertall i stedet for ved enstemmighet som man visste ville bli nærmest umulig.

Med Lisboa-traktaten er søylene i EU-samarbeidet opphevet, og det er ikke lenger noe klart skille mellom de ulike sektorene innenfor EU-retten. I dag er det derfor ikke viktig om et direktiv er et indre marked-direktiv eller ikke. Det som er viktig for Norge, er om det er EØS-relevant eller ikke. Dette er ukjent terreng, som ganske sikkert vil føre til en rekke grenseganger for hva som ligger innenfor og utenfor EØS-avtalens virkeområde. Datalagringsdirektivet har ikke vært vurdert i forhold til den senere tids utvikling av EU-retten på dette området.

Troms Nei til EU mener at Datalagringsdirektivet ut fra direktivets formål tilhører justisområdet, og i den grad det berører konkurranseretten, gir det rom for så store kostnadsvariasjoner mellom land at konkurransenøytralitet ikke kan brukes som argument for at direktivet er EØS-relevant. På dette grunnlaget bør Datalagringsdirektivet avvises.

Skulle man likevel komme til at Datalagringsdirektivet er EØS-relevant, er det mange grunner for at reservasjonsretten i EØS-avtalen bør benyttes. Vi vil i det følgende begrunne dette nærmere.

Datalagringsdirektivet og Grunnloven

I Samferdselsdepartementets høringsdokument om Datalagringsdirektivet finnes det ingen problematisering av forholdet til Grunnloven. Dette må ansees som en stor mangel ved høringsdokumentet, da direktivet berører både § 100 og § 102 i Grunnloven. Disse paragrafene har følgende ordlyd:

> *§ 100.*
>
> *Ytringsfrihed bør finde Sted.*
>
> *Ingen kan holdes retslig ansvarlig for at have meddelt eller modtaget Oplysninger, Ideer eller Budskab, medmindre det lader sig forsvare holdt op imod Ytringsfrihedens Begrundelse i Sandhedssøgen, Demokrati og Individets frie Meningsdannelse. Det retslige Ansvar bør være foreskrevet i Lov.*
>
> *Frimodige Ytringer om Statsstyrelsen og hvilkensomhelst anden Gjenstand ere Enhver tilladte. Der kan kun sættes slige klarlig definerede Grændser for denne Ret, hvor særlig tungtveiende Hensyn gjøre det forsvarligt holdt op imod Ytringsfrihedens Begrundelser.*
>
> *Forhaandscensur og andre forebyggende Forholdsregler kunne ikke benyttes, medmindre det er nødvendigt for at beskytte Børn og Unge imod skadelig Paavirkning fra levende Billeder. Brevcensur kan ei sættes i Værk uden i Anstalter.*
>
> *Enhver har Ret til Indsyn i Statens og Kommunernes Akter og til at følge Forhandlingerne i Retsmøder og folkevalgte Organer. Det kan i Lov fastsættes Begrænsninger i denne Ret ud fra Hensyn til Personvern og af andre tungtveiende Grunde.*
>
> *Det paaligger Statens Myndigheder at lægge Forholdene til Rette for en aaben og oplyst offentlig Samtale.*
>
> *§ 102.*
>
> *Hus-Inkvisitioner maa ikke finde Sted, uden i kriminelle Tilfælde.*

Ytringsfriheten

Ytringsfriheten er en grunnleggende forutsetning for en opplyst allmennhet og dermed også for et demokratisk styresett. Grunnloven er forbilledlig klar på dette punktet, men ble til i en tid da man ikke hadde noen mulighet til å forestille seg utarbeidelse av kontakt- og adferdsprofiler med bakgrunn i telekommunikasjonsadferd. Det er derfor en for snever tolkning av Grunnlovens forbud mot brevsensur å hevde at fordi man ikke lagrer innholdet i kommunikasjonen, bryter man heller ikke Grunnlovens forbud. Mest sannsynlig vil en profilanalyse av samtlige telekommunikasjonsmidler en person benytter i et halvt år være et langt sterkere inngrep i hans private sfære enn at et brev blir lest av uvedkommende.

Det at man vet seg overvåket, kan i seg selv føre til at man er mer forsiktig med hvem man tar kontakt med. Fra vår nære fortid vet vi at mange var redde for å bli sett sammen med kommunister fordi de visste at disse ble overvåket. I dag er det tenkbart at en lignende frykt kan holde folk tilbake i deres telekommunikasjon med for eksempel muslimer. Ytringsfriheten må altså ikke bare innbefatte en rett til offentlig skrift og tale, men også til uten frykt for framtidige konsekvenser å kunne ha kontakt med hvem som helst, så lenge denne kontakten ikke skjer i forbrytersk hensikt.

Kildevernet

Det påligger altså "Statens Myndigheder" å legge forholdene til rette for en åpen og opplyst offentlig samtale. En av de viktigste forutsetningene for dette er en fri og uavhengig presse. Pressen er helt avhengig av skjulte informanter for å kunne avdekke kritikkverdige forhold i samfunnet. Pressen er derfor fritatt fra vitneplikt, jfr. Straffeprosesslovens § 125, og beslag av data i pressens besittelse er som hovedregel utelukket, jfr. Straffeprosesslovens § 210. Innføring av Datalagringsdirektivet vil uthule prinsippet om kildevern, da informanter som vet at alle trafikkdata blir lagret, vil vegre seg for å ta kontakt med pressen, ettersom de står i fare for å bli avslørt. Slik kan kritikkverdige forhold i samfunnet forbli skjulte, uten at hvite felter i avisene viser at sensur har funnet sted.

Ransaking

Argumentasjonen om at bestemmelsen i Grunnloven om brevsensur må sees i forhold til de inngrep i den enkeltes frihet Eidsvollsmennene kunne se for seg, må også gjelde for bestemmelsen om husundersøkelser. Også her er forholdet at en kontakt- og adferdsprofil ut fra telekommunikasjon som regel er et større inngrep i privatlivets fred enn hva en husundersøkelse er. At inngrepet kanskje ikke oppleves så krenkende fordi det skjer i det skjulte, er ingen formildende omstendighet, snarere tvert imot. Det å vite hvilke data om deg som lagres, er i seg selv en viktig rettighet i en rettsstat, og ble da også en del av resultatet etter at Lund-kommisjonen hadde lagt fram sin innstilling.

Datalagringsdirektivet og Den europeiske menneskerettighetskonvensjonen

Den europeiske menneskerettighetskonvensjonen trådte i kraft i 1953 etter at tilstrekkelig mange land hadde ratifisert den. Konvensjonen har som formål å beskytte menneskerettighetene og de grunnleggende friheter. Ratifikasjon av konvensjonen er ett av kriteriene for å bli medlem av Europarådet. Konvensjonens artikkel 8 er gjengitt nedenfor.

> ***Artikkel 8:***
>
> 1. *Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.*
>
> 2. *Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale*

sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.

Artikkel 8.1 er veldig tydelig, så det skulle ikke være behov for ytterligere tolkninger. Så er det i samme artikkels andre ledd tatt en rekke forbehold, men det er verd å merke seg at den frie konkurransen i EUs indre marked ikke er en gyldig grunn til å fravike hovedregelen om at "Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse". Så hvis Datalagringsdirektivet er et indre marked-direktiv, er det i strid med Den europeiske menneskerettighetskonvensjonen, hvis det er et justisdirektiv, er det ikke EØS-relevant. Norge er pliktig til å følge bestemmelsene i Den europeiske menneskerettighetskonvensjonen, ikke til å implementere EUs datalagringsdirektiv.

Mer overvåking

I rettspleien er det et bærende prinsipp at enhver er uskyldig til det motsatte er bevist. For at politiet i dag skal kunne foreta teknisk sporing, må det foreligge skjellig grunn til mistanke om handling med strafferamme på minst 5 år, jfr. Straffeprosesslovens § 202b. For å plassere teknisk peileutstyr i klær, kreves en strafferamme på 10 år og foreligge skjellig grunn til mistanke, jfr. Straffeprosesslovens § 202c.

Av høringsdokumentet framgår det at blant de data som skal lagres ved mobiltelefoni er "lokaliseringsinformasjon ved start og avslutning av kommunikasjon". Direktivteksten i Artikkel 5.1, litra f er imidlertid som følger:

> *"(f) data necessary to identify the location of mobile communication equipment:*
>
> *(1) the location label (Cell ID) at the start of the communication;*
>
> (2) *data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period of which communication data are retained."*

Siste ledd kan vanskelig tolkes annerledes enn at mobiltelefonens posisjoner skal registreres "i den perioden kommunikasjonsdata blir oppbevart", altså ikke begrenset til registrering av posisjon ved start og avslutning av samtaler, men bare av om mobiltelefonen er innenfor dekningsområde. Særlig i tettbygde strøk vil dette gi en meget presis beskrivelse av den enkeltes bevegelser over lang tid. Telenors ekspert Erlend Bjørtvedt bekreftet i en debatt under Nei til EUs landskonferanse 12. mars i år denne forståelsen av direktivteksten.

Med datalagringsdirektivet kan slike og andre data samles inn uten skjellig grunn til mistanke, og slik direktivet foreslås implementert, kan disse dataene overlates til politiet om strafferammen for forbrytelsen er minst 3 år. I tillegg er det listet opp mange unntak fra 3-årsgrensen. Dette er en klar liberalisering av dagens regelverk, ikke en innstramming som det er blitt hevdet.

Faren for kompromittering

Samling av store mengder personopplysninger på ett sted er blitt karakterisert som en honningkrukke for kriminelle. Dataregistre som har til hensikt å bekjempe kriminalitet, kan tvert imot bli en kilde til kriminalitet. I høringsdokumentet går man da heller ikke inn for at

alle data skal lagres i en database. Det blir sett på som sikrere at den enkelte tjenestetilbyder lagrer sine data. Dette reiser imidlertid andre problemstillinger.

Ved desentralisert lagring er det vanskelig å se for seg at data blir kryptert. Det er også grunn til å tro at mindre tilbydere ikke har de samme muligheter til å beskytte data mot inntrenging som de store telekomselskapene har. Siden man må regne med at det er kundene som må betale for lagringen, vil tilbyderne i markedet av konkurransehensyn ha interesse av så lave lagringskostnader som mulig. Det betyr i praksis lav sikkerhet, og lagring utenfor landets grenser.

Like før påske var det medieoppslag om kompromittering av bankdata fra Sparebanken Øst, som hadde overlatt IT-virksomheten til EDB Business Partner som igjen hadde overlatt jobben til et datterselskap i Ukraina. Det er ikke utenkelig at slikt også kan skje med lagrede trafikkdata. Israel er alt godkjent av EU som lagringssted for personopplysninger, og med Mossads ID-tyverier i forbindelse med drapet på Hamas-lederen Mahmoud al-Mabhouh i Dubai tidligere i år i friskt minne, er Israel som lagringssted et skrekkscenario.

I jula 2009 ble Google utsatt for et massivt cyber-angrep der kinesiske hackere som disponerte superdatamaskiner prøvde å skaffe seg oversikt over hvem kinesiske menneskerettsaktivister kommuniserte med via g-mail. Dette viser at trafikkdata kan være av vel så stor interesse i politisk som i kriminalitetsforebyggende sammenheng, og når de illegitime interessene er sterke nok, skal det mye til for å hindre kompromittering.

Men faren er nok større for at utro tjenere vil skaffe fram opplysninger som de kan selge til skandalepressen, andre kommersielle aktører, konkurrenter eller kriminelle. Tatt i betraktning de forhold som ble avdekket av Lund-kommisjonen, bør man også være oppmerksom på muligheten for myndighetsmisbruk i form av ulovlig overvåking og kontroll av meningsmotstandere. Og selv om vi i dag lever i et demokratisk samfunn, skal vi alltid ha i bakhodet hva registre kan brukes til av illegitime regimer. Det er i den forbindelse nok å minne om hva jøderegistrene ble brukt til da nazistene iverksatte sin djevelske plan om "Endlösung des Jüdenproblemes".

Datalagringsdirektivet og alvorlig kriminalitet

Det er grunn til å anta at terrorister og kriminelle organisasjoner i god tid har tatt sine forholdsregler slik at deres aktivitet ikke fanges opp av tiltak iverksatt som en følge av Datalagringsdirektivet. Det er en kjent sak at miljøer den amerikanske etterretningsorganisasjonen NSA ønsker å kikke i kortene, har tatt i bruk så tung kryptering at selv verdens kraftigste superdatamaskiner ikke greier å forsere krypteringen. Det vil derfor være naivt å tro at ikke de som bedriver alvorlig kriminalitet også vil være i stand til å skjule sine elektroniske spor.

Hvis man googler frasen "Hide my IP", får man opp 4,7 millioner treff. Her kan man velge og vrake mellom gratis eller betalte løsninger for skjuling av IP-adresse. Dersom de som har kontakt med hverandre begge bruker slikt verktøy, der IP-adressen endres med sekunders mellomrom og hopper fra land til land, vil det være en vanskelig oppgave for en overvåker å holde oversikten selv i sanntid, og en umulig oppgave lang tid etterpå.

Datalagringsdirektivet omfatter ikke kommunikasjon der lagring av trafikkdata kompromitterer innholdet. Skype, MSN, Yahoo Messenger, Google Talk og andre lignende tjenester faller derfor utenfor direktivets rammer. Denne teknologien er i rivende utvikling, eksempelvis har Skype-telefonen vært på markedet en god stund nå.

Andre måter å unngå Datalagringsdirektivet på er å kommunisere via chat, nyhetsgrupper, fildelingsnettverk og andre nettfora. EU har tydeligvis sett denne svakheten, så man har startet et prosjekt kalt Indect med mål å overvåke også slike tjenester. Dette viser at Datalagringsdirektivet bare er første skritt på veien mot overvåkningssamfunnet.

Men for dem direktivet er ment å ramme, blir virkningen slik som beskrevet av EuroCOP-sjefen Heinz Kiefer: "Resultatet blir at store anstrengelser gjøres med knapt større virkning på kriminelle og terrorister enn litt irritasjon."

Konklusjon

Troms Nei til EU mener at Datalagringsdirektivet ikke er relevant i forhold til EØS-avtalen, og at det må avvises på dette grunnlag.

Dersom man likevel skulle konkludere med at direktivet er EØS-relevant, må det foretas en vurdering av direktivet i forhold til Grunnlovens bokstav og ånd. Vi mener at bruddene her er klare nok til at dette er et selvstendig grunnlag for å bruke reservasjonsretten i EØS-avtalen.

Videre bryter direktivet klart med Den europeiske menneskerettighetskonvensjonens artikkel 8 som Norge er forpliktet til å overholde. Datalagringsdirektivet fører til mer overvåking uten at det er sannsynliggjort at dette sikrer oss mot terrorisme og alvorlig kriminalitet. Og direktivet skaper ny risiko for kompromittering av sensitiv informasjon.

Alt dette tilsier at Norge bruker reservasjonsretten i EØS-avtalen for første gang.