

Datalagringsdirektivet – mer enn et spørsmål om lagringstid

av Eva I. E. Jarbekk



Innledning

EU/EØS har pålagt medlemsstatene å implementere direktiv 2006/24/EF som er meget omstridt. Lesere av *Lov&Data* vil antakelig være godt kjent med dette. Det har vært rikelig pågang i media av folk med mer eller mindre forståelse for hvilke regler direktivet innebærer. Noen har forsøkt å forsvare direktivet, men media har viet dem mindre oppmerksomhet. De fleste som har fått medias oppmerksomhet er kritiske. Det er ikke hverdagskost at det dannes interessegrupper på Internett, Facebook og e-post-kampanjer mot direktiver. Den tyske stat er saksøkt av borgerrettsgrupper for innføringen av direktivet. Hva er bakgrunnen for dette engasjementet? Jeg kommer tilbake til det avslutningsvis.

Hvordan vil direktivet bli implementert i Norge?

Det er det ingen som vet. Direktivet skal implementeres senest i mars 2009. Det norske lovforslaget vil

antagelig komme på høring før sommeren 2008, men direktivets regler gir jo en mer enn omtrentlig pekepinn på hva vi kan vente.

Direktivet fastslår at medlemsstatene skal lagre bestemte kommunikasjonsdata i en viss tidsperiode. Lagringstiden kan bli fra seks måneder til to år. Hva myndighetene vil velge, vites ikke.

Viktigere enn lagringstid, men ofte omtalt med langt mindre presisjon i media, er hvilke typer opplysninger som skal lagres. Her må det umiddelbart understrekes at det ikke skal lagres informasjon om «innholdet» av kommunikasjonen. Akkurat dette har nok vært misforstått av mange i pressen. Men det er likevel ganske mye annet som skal lagres.

Det skal lagres opplysninger om brukerne av telefoni, internett, e-post og ip-telefoni. Dette er bl.a. A- og B-nummer for vanlig telefoni, brukeridentitet for e-post, dato og klokkeslett for kommunikasjonen og mye mer. Noen av disse opplysningene gir en ganske sikker personidentifikasjon av hvem som har forestått kommunikasjonen, for eksempel et A-nummer i en husholdning med en person. For IP-numre i store bedrifter vil en slik personidentifikasjon være mer usikker, men man vil nok kunne avgjøre fra hvilket firma (juridisk person) en kommunikasjon kommer.

Det er dessuten særlig angitt at man skal lagre lokaliseringsdata for mobiltelefoner slik at man kan fastslå hvor mobiltelefonen befant seg da kommunikasjonen ble startet. EU/EØS har dessverre ikke åpnet for at medlemsstatene kan velge å ikke lagre de opplysningene direktivet angir.

Opplysningene skal ligge passivt hos teleoperatørene inntil myndighetene har hjemmel for å innhente og bruke opplysningene. Det er såle-

des den enkelte leverandør som skal forstå lagringen av disse opplysningene. Hvilke myndigheter som kan kreve innsyn er ikke bestemt. Det vil nok bli politiet, men kanskje også myndigheter som Kredittilsynet, Skatteetaten og Konkurransetilsynet. De nærmere vilkårene for å få tilgang til opplysningene er ikke fastlagt, men det ligger en føring i at opplysningene kun skal brukes til oppklaring av grov kriminalitet. Definisjonen av hva som er grov kriminalitet er opp til det enkelte land.

Et forhold som ikke har vært mye fremhevet i media, er at direktivet ikke bare gjelder for privatpersoner. Det gjelder også for kommunikasjon mellom bedrifter. Også bedrifter kan begå grov kriminalitet som for eksempel korrupsjon og skattekriminalitet.

Formålet med direktivet er primært å bedre mulighetene for å etterforske og oppklare grov kriminalitet. De store terrorangrepene i bl.a. London er noe av bakteppet for direktivet. Et av målene er å hindre organisert kriminalitet. Forebygging er også nevnt.

Fare for utglidning og misbruk?

Direktivets hensikt er edel, men mange er redde for at reglene kan bli misbrukt. Denne frykten for misbruk er berettiget og misbruk kan skje på mange måter. De aktuelle opplysningene *kan* brukes til å gi en ganske god oversikt over hvem som har kontakt med hvem i vårt samfunn. Noen av opplysningene kan også brukes til å lokalisere personer. De fleste vil forstå at dette er opplysninger som kan tenkes å ha interesse i mer enn kriminalrettslig forstand. Det er sannsynlig at slik informasjon også representerer en økonomisk verdi.

Det er i første rekke myndighetene som bestemmer hvordan opp-

lysningene skal bli brukt. Etter dagens direktiv vil opplysningene som nevnt kun bli brukt til å oppklare grov kriminalitet. Men hva hvis vi skulle få et annet politisk regime? Hvordan vil et totalitært regimes definisjon av grov kriminalitet være? For totalitære regimer vil denne type opplysninger være ypperlige til å identifisere motstandere og deres nettverk. Hvem tør si at dette ikke kan skje hos oss?

Det er også ofte slik at det nesten er en naturlov i det at informasjon som eksisterer, vil bli brukt. Når opplysningen først er lagret er det mange som vil ha innsyn og intensjonen bak er alltid god. Ofte blir opplysninger derfor brukt i en helt annen sammenheng enn hva man opprinnelig tenkte seg. Man trenger ikke et totalitært regime for at dette skal skje. Derfor må man tørre å se på direktivets konsekvenser i en større sammenheng enn hva direktivet selv oppsetter. Kritikerne av direktivet frykter at politikerne vil finne stadig nye måter å bruke opplysningene på slik at personvernet skrumpes ytterligere inn.

Dette har jo også en økonomisk side. Informasjon om hvem en person ringer eller sender e-post til kan være interessant for mange. Det er teleoperatørene som skal lagre opplysningene. Lagring koster penger. Lagringen skal teleoperatørene naturligvis gjøre på en sikker måte, slik at opplysningene ikke lekker ut. Men dette er private aktører som er drevet av krav til bunnlinje. Har de råd til sikre nok systemer? Hvem skal kontrollere dette? Det blir antakelig Datatilsynet, men har Datatilsynet nok ressurser? Datatilsynet har i media uttalt at mange av de aktørene som skal oppbevare opplysningene sliter med forsvarlig sikring av data. Det er ikke betryggende.

Over tid vil det ganske sikkert skje tilfeldige lekkasjer fra slike registre. I pressen har mange også nevnt faren for at ansatte hos teleoperatøren kan «snoke» i opplysningene. Det er heller ikke utenkelig at slike opplysninger kan tenkes å bli

«kjøpt ut» hvis de representerer en stor verdi. Over tid er det uansett sannsynlig at det vil skje lekkasjer av informasjonen.

Hva oppnår man?

For artikkelforfatteren er det vanskelig å tenke seg at grov og organisert kriminalitet vil bli forebygget ved dette direktivet. Pressen har allerede vært full av gode råd til de som vil unngå å etterlate spor. Det er ikke slik at mobiltelefon og e-post er eneste kommunikasjonsform som kan brukes. Andre metoder kan brukes uten å etterlate klare spor; ikke bare post. Teknologien på dette vil nok utvikle seg videre. Det er all grunn til å tro at organisert kriminalitet vil benytte andre muligheter enn de direktivet vil skal overvåkes.

Da står man igjen med at direktivet åpner for enklere oppklaring av tilfeller av mer tilfeldig og ikke-planlagt grov kriminalitet. Slik kriminalitet forebygges sjelden ved at oppklaringsmulighetene er gode. Det er naturligvis prisverdig å forenkle og øke oppklaringsmulighetene for slik kriminalitet, men det bør ikke markedsføres politisk som oppklaring av organisert kriminalitet.

Overvåking av uskyldige?

Mange mener at direktivet innfører et nytt prinsipp, nemlig overvåking av personer som ikke er mistenkt for et straffbart forhold eller noe lovbrudd overhode. Forstått slik, er det ikke rart at folk reagerer og at interessegrupper mot direktivet dannes. Det er faktisk et sunnhetstegn. Andre har ment at direktivet ikke innfører noen overvåking; at det kun åpner for lagring av opplysninger og at disse kun skal brukes til et snevert – og ærverdig – formål. Det blir en teoretisk diskusjon om man skal kalle dette overvåking eller ikke. Uansett medfører direktivet at det lagres vesentlig mye mer informasjon om oss enn tidligere.

Hvis man tror at informasjonen aldri vil bli brukt til noe annet enn hva direktivet angir, så kan man kanskje forsvare direktivet. Hvis ikke, er

det mye mer komplisert. Mange tror at bruken av opplysningene ikke vil være begrenset til dette direktivets regler. Det har lenge vært et personvernmessig prinsipp at individene skal ha kontroll med informasjon som omhandler dem selv. Dersom stadig mer informasjon om oss registreres og brukes av myndighetene, uthules dette prinsippet. Jeg tror dette er bakgrunnen for det engasjement man har sett om direktivet i media. Mange er redde for at direktivet varsler et vesentlig endret samfunn der vi alle er mer enn langt kartlagt av myndighetene – og kanskje av andre enn myndighetene.

Har Norge noe valg?

Både ja og nei. Det skal svært meget til for at Norge skal velge å ikke implementere et direktiv. Men dette er et meget omstridt direktiv, også i Europa. Og nettopp det at motstanden mot direktivet er så stor i Europa, kan medføre at de politiske virkningene av å ikke implementere direktivet kan bli akseptable.

I pressen har det vært fremhevet at det kan være personvernmessig lettere å få gjennomslag for lagring i seks måneder enn to år. Jeg tror at det er en grov personvernmessig avsporing. Den viktige personvernmessige diskusjonen går på om vi overhodet synes det er forsvarlig med slik lagring hos teleoperatørene.

Eva I. E. Jarbekk
er partner i Brækhus Dege
og leder for advokatforeningens
lovutvalg for ikt og personvern.