Fra rådet til tinget

Datalagringsdirektivet

Teknologirådet

Fra rådet til tinget nr. 26, april 2010

Sammendrag

Etter terrorangrepene i Madrid og London har flere land ønsket å lagre kommunikasjonsdata fra telefoni, mobiltelefoni og internett, også utover de data operatørene trenger for driftsformål. Gjennom data-lagringsdirektivet søker EU å sikre like vilkår for lagring av slike data i hele EØS-området. Dataene skal lagres i minimum 6 måneder og maksimum 2 år.

Kortest mulig lagringstid
En lagringstid på 6 måneder vil for mye av teletrafikkdataene innebære en betydelig utvidelse i forhold til dagens situasjon. Det vil være rimelig at effekten av en slik økning evalueres før man eventuelt vurderer mer drastiske tiltak. Vi vet at det er enklere å innføre nye tiltak enn å fjerne tiltak som allerede er innført.

Desentral lagring det beste
Trafikkdata bør av personvernhensyn lagres desentralisert hos den enkelte operatør som i dag, framfor i en sentral database. Kun politiet bør få tilgang, og da etter en rettskjennelse. Sentrale databaser har en del personvernutfordringer, slik som sikkerhet mot datainnbrudd og -lekkasjer, dobbeltlagring, formåls-utglidning og sammenstilling av data fra ulike kilder. Det må utvikles klare krav til hvordan sikkerheten for de lagrede dataene skal ivaretas, og til rutiner for sletting eller anonymisering av data.

Effekten må evalueres, og direktivet ses i sammenheng med andre overvåkingstiltak
Teknologiutviklingen de siste årene har medført en økning i elektroniske spor, og dermed en økt mulighet til å overvåke og spore innbyggerne i Norge. Dersom direktivet innføres, er det viktig at det gjennomføres en evaluering i etterkant, og at datalagringsdirektivet ses i sammenheng med andre sikkerhets- og overvåkingstiltak i samfunnet, blant annet valutaregisterloven.

Bakgrunn

Europaparlamentets- og rådsdirektiv 2006/24/EF av 15. mars 2006 omhandler lagring av data som fremkommer ved bruk av offentlig elektronisk kommunikasjon, slik som telefoni, mobiltelefoni og internett. Bakgrunnen for direktivet er terrorangrepene i Madrid og London. Disse angrepene har ført til lokale datalagringsinitiativ, og direktivet tar sikte på å harmonisere denne praksisen.

I tillegg er forretningsmodellene for kommunikasjonstjenester i endring: For internett har vi gått fra modem og oppringte linjer, til faste månedspriser for å være "alltid på". Dette er også en utvikling vi ser for mobiltelefoni. Fordi lovverket bare tillater lagring av data som er nødvendige for driftsformål, har dette medført at færre data lagres, noe blant annet politiet opplever som et problem.

Direktivet har vært omstridt innenfor EU, og flere land har ennå ikke innført direktivet, til tross for at implementeringsfristen er gått ut. Det har blant annet vært debatt om hvorvidt direktivet skal kobles til det indre markedet, eller om det utelukkende er relevant for politi- og strafferettssamarbeidet. I 2009 slo EF-domstolen fast at direktivet angår det indre markedet, og dermed også er EØS-relevant.

Dette *Fra rådet til tinget* tar ikke stilling til hvorvidt datalagringsdirektivet bør innføres,

men vurderer viktige forhold rundt den eventuelle implementeringen. Direktivet settes også i sammenheng med andre, lignende tiltak, og det tas opp hvordan direktivet påvirker det totale overvåkingsnivået i det norske samfunnet.

Hva innebærer direktivet?

Datalagringsdirektivet er formulert slik at de enkelte land har ganske stor frihet i hvordan det gjennomføres i praksis. Enkelte ting ligger imidlertid fast, blant annet hvilke data som *må lagres*:

- Data som er nødvendige for å spore og identifisere de som kommuniserer, både for fasttelefoni, mobiltelefoni, internettadgang, e-post og IP-telefoni
- Dato, klokkeslett og varighet for telefonsamtaler, inn- og utloggingstidspunkt, IP-adresser og bruker-ID for internettadgang
- Telefonnummer, ID-numre for mobiltelefon, telefon-eller DSL-linje for data
- Data som viser hvilken basestasjon (celle ID) samtalen ble koblet opp fra

Innholdet i kommunikasjonen *lagres ikke* – og heller ikke adressene til nettsidene man besøker.

De enkelte landene kan selv bestemme varighet av lagringen innenfor et intervall på minimum 6 måneder og maksimum 2 år, hvordan lagringen skal organiseres og hvem som skal få tilgang til dataene og under hvilke betingelser.

Annen datalagring i Norge

I Norge har vi allerede eksempler på lovgivning hvor data lagres med kriminalitetsbekjempelse som begrunnelse. Den mest omfattende av disse er valutaregisterloven.

Formålet med valutaregisterloven er å forebygge og bekjempe kriminalitet og å bidra til riktig skatte- og avgiftsbetaling, ved at kontroll- og etterforskningsorganene får tilgang til opplysninger om valutavekslinger og fysisk eller elektronisk overføring av betalingsmidler inn og ut av Norge. I praksis betyr det at svært detaljert informasjon om for eksempel innkjøp gjort i utlandet registreres og lagres i et register som en rekke etater har tilgang til, blant annet: Politiet, skatteetaten, toll- og avgiftsetaten, Arbeids- og velferdsdirektoratet, Finanstilsynet og Norges Bank. Opplysninger i registeret skal slettes senest fem år etter utløpet av registreringsåret.

Et annet eksempel er forbudet mot anonyme kontantkort fra 2004. Ved kjøp av forhåndsbetalte kontantkort bortfalt teleoperatørens behov for registrering, ettersom ingen informasjon var nødvendig for fakturering. Et kontantkort muliggjorde dermed kommunikasjon som ikke kunne spores tilbake til opprinnelsesperson. Gjennom å forby anonyme kontantkort ønsket Stortinget å sikre at det i forbindelse med etterforskning av kriminelle forhold skulle være mulig å spore samtaler også fra telefoner med denne formen for avtale. Dette var i praksis en form for lagringsplikt som gikk utover operatørens forretningsmessige behov.

Bankene lagrer i dag informasjon både om kontoinnehavere og transaksjoner. Dette er begrunnet i flere lover, blant annet lignningsloven som sier at skattesaker ikke er foreldet før etter 10 år, og hvitvaskingsloven som angir at mistenkelige transaksjoner skal lagres i 5 år. Dette er data hvor detaljeringsnivået har endret seg betydelig de siste 10 årene, i takt med økningen i bruk av kort som betalingsmiddel.

Hvor bør dataene lagres?

I dag lagrer de enkelte teleoperatørene dataene i sine egne systemer, og politiet kan få tilgang til disse etter at Post- og teletilsynet har opphevet operatørens taushetsplikt. Enkelte internettleverandører og mindre teleoperatører har i dag ikke de systemene som kreves, og vil måtte gjøre en investering for å få dette på plass. Vi

mener likevel dette er en løsning som er langt å foretrekke framfor en sentral løsning, lagt til for eksempel politiet.

Dette skyldes ikke minst at det er en del personvernutfordringer knyttet til store, sentrale databaser.

Sikkerhet
En viktig personvernutfordring ved sentrale databaser er sikkerhet. Dersom det skjer et datainnbrudd, eller data lekker ut ved en feiltakelse, vil omfanget være mye større enn med en desentralisert struktur.

Dobbeltlagring
Et relatert argument er at store deler av datamengden uansett må lagres av den enkelte operatør i forbindelse med forretningsdriften. Selv om operatørene ikke har behov for å lagre dataene like lenge som direktivet krever, ville dette medføre en stor grad av dobbeltlagring, noe som igjen medfører en økt sikkerhetsrisiko.

Formålsutglidning
Det viktigste argumentet mot sentral lagring er likevel faren for formålsutglidning. Dersom man samler alle kommunikasjonsdata for telefoni og internett i én sentral database som forvaltes av politiet, blir terskelen lavere for å ta dataene i bruk for andre formål.

Vi har tidligere sett eksempler på dette i Norge: I 2003 ble det vedtatt å gi politiet tilgang til å sjekke fingeravtrykk fra kriminalsaker opp mot fingeravtrykk i utlendingsregisteret. Dette skjedde til tross for at det ved opprettelsen av registeret eksplisitt ble nedfelt i utlendingsforskriften at søk i registeret ikke skulle finne sted i forbindelse med etterforskning av straffbare handlinger begått i Norge.

Sammenstilling av data fra ulike kilder
Den tyske forfatningsdomstolen besluttet i mars 2010 at den tyske implementeringen av datalagringsdirektivet er i strid med grunnloven. I sin begrunnelse går retten igjennom hvilke kriterier som må være til stede for at datalagring skal kunne aksepteres. En av faktorene som trekkes fram er nettopp viktigheten av at lagringen foretas av operatørene og ikke direkte av myndighetene. Dette betyr at dataene ikke er koblet sammen allerede gjennom lagringen (for eksempel ved ulike kundeforhold for mobiltelefoni, fasttelefoni og internett), og medfører i mindre grad at lagringen kan oppleves som en totalkartlegging av alle borgernes kommunikasjonsaktiviteter.

Krav til sikkerhet og rutiner for sletting
Fra sentralt hold må det utvikles klare krav til hvordan sikkerheten for de lagrede dataene skal ivaretas, og til rutiner for sletting eller anonymisering av data etter endt lagringsperiode. Datatilsynet bør få tilstrekkelig ressurser til å føre tilsyn med operatørene, og brudd på sikkerhets- og sletterutiner må medføre sanksjoner.

Hvem skal få tilgang til dataene og når?

Det er kun politiet som bør få tilgang til dataene, og da kun etter en rettslig kjennelse.

Kjennelse viktig for opplevelse av rettssikkerhet
I 2007 gjennomførte Teknologirådet sammen med flere europeiske partnere fokusgruppeundersøkelser i seks land. Undersøkelsene tok for seg ulike typer teknologi for samfunnssikkerhet og overvåkning. Deltakerne diskuterte blant annet hvilke trusler som kan rettferdiggjøre økt overvåkingsnivå, og hvilke typer teknologi og inngrep de kunne akseptere. Rettskjennelser ble trukket fram som svært viktig for å kunne akseptere inngrep i privatlivet.

Proporsjonalitet
Tiltak som datalagringsdirektivet medfører alltid en avveining mot hensynet til personvern. Slike avveininger står sentralt i den europeiske menneskerettighetskonvensjonen (EMK) og omtales gjerne som *proporsjonalitetsprinsippet*.

I sin høringsuttalelse om datalagringsdirektivet påpeker Datatilsynet at trafikkdata fra internett- og telekommunikasjon blir stadig mer omfattende. Den økende trenden med smarttelefoner, kombinert med stadig større datahastigheter medfører at folk bruker telefonene sine annerledes enn tidligere. I mange tilfeller (for eksempel ved funksjonalitet som sjekker epost kontinuerlig, såkalt *push mail*) medfører

dette at mobiltelefonen kobles av og på nettverket hele tiden. Dette bidrar til mye data som blant annet avslører brukerens lokasjon nærmest kontinuerlig.

Når dataene er av så omfattende karakter, og potensielt kan gi mye informasjon utover det man tradisjonelt har forbundet med trafikkdata, er det viktig at kravene til innsyn står i forhold til dette. Det er derfor positivt at departementet i sitt høringsnotat foreslår at det skal foreligge skjellig grunn til mistanke om alvorlig kriminalitet for at det skal kunne gis innsyn i dataene.

Dersom Stortinget velger å ikke innføre datalagringsdirektivet bør det uansett gjennomføres en slik opprydding i praksis for tilgang til teletrafikkdata.

Krav til transparens

Det er et viktig personvernprinsipp at innsamling og bruk av persondata skjer åpent, slik at den enkelte vet hvilke data som er samlet inn om ham/henne, og hvem som har tilgang til dem. Dersom politiet etter en rettskjennelse har fått tilgang til en persons teletrafikkdata, skal personen underrettes. Dersom det vil skade etterforskningen å underrette i forkant, skal retten i sin kjennelse ta stilling til om innsynet kan unndras den som er under mistanke i et fastsatt tidsrom.

Lagringstid

I dag lagres trafikkdata i 3 eller 5 måneder, avhengig av hvor ofte kunden faktureres. En lagringstid på 6 måneder, som er minstekravet innenfor rammen av direktivet, vil med andre ord medføre en dobling av lagringstiden for en stor del av kundene. Internettrafikk kan i dag lagres i 3 uker. 6 måneder lagringstid vil være en betydelig utvidelse.

Det vil være rimelig at effekten av en slik økning evalueres før man eventuelt vurderer mer drastiske tiltak. Vi vet av erfaring at det er enklere å innføre nye eller skjerpede tiltak enn å fjerne tiltak som allerede er innført.

Det foreligger i dag ingen statistikk over hvor gamle data politiet har etterspurt til nå. I sin evaluering av bruken av skjulte tvangsmidler peker Metodekontrollutvalget på at det er vanskelig å finne informasjon i systematisert form om bruken av de ulike metodene og utfallet i sakene hvor de er blitt brukt. Slik informasjon er viktig også i forhold til utlevering av teletrafikkdata dersom det skal kunne gjennomføres en reell evaluering.

Hva slags overvåkningssamfunn vil vi ha?

Teknologiutviklingen de siste årene har medført en økning i elektroniske spor, og dermed en økt mulighet til å overvåke og spore individer. Det er slik sett et paradoks at når forretningsmodellene knyttet til internett og telefoni innebærer en *reduksjon* i denne typen spor, så finner myndighetene det nødvendig å kompensere for dette med et eget regelverk.

Dersom man ikke ønsker et samfunn med stadig mer overvåking, må det også være en vilje til å stramme inn på eksisterende ordninger. Direktivet bør evalueres en tid etter eventuell innføring, og dette bør skje i sammenheng med en evaluering av andre former for datalagring, slik som valutaregisteret og bankenes transaksjonsdata. Formålet må være å sikre at ikke proporsjonaliteten mellom kriminalitetsbekjempelse og personvern forskyves ytterligere.

Teknologirådet er et uavhengig, rådgivende organ for teknologivurdering. Det ble opprettet ved kgl. res. 30.april 1999 etter initiativ fra Stortinget. "Fra rådet til tinget" utgis av Teknologirådets sekretariat.

Dette dokumentet er basert på Teknologirådets høringsinnspill om datalagringsdirektivet, oversendt 12.4.2010.

Redaksjon
Christine Hafskjold, Tore Tennøe

Abonnement
post@teknologiradet.no
Alle utgaver av *Fra rådet til tinget* kan leses på
www.teknologiradet.no