Samferdselsdepartementet
Att: Heidi Karlsen

Teknologirådet

Pb. 522 Sentrum
0105 Oslo

Prinsensgate 18
Norway

T: +47 23 31 83 00
F: +47 23 31 83 01

www.teknologiradet.no
post@teknologiradet.no

Vår ref.: 20.10
Deres Ref.: 09/585-HK
Dato: 12.04.2010

## Høringsuttalelse om datalagringsdirektivet

I sitt høringsnotat ber departementene om tilbakemelding på de synspunktene som fremmes i notatet. I dette høringsinnspillet tar Teknologirådet derfor ikke stilling til hvorvidt datalagringsdirektivet bør innføres, men vurderer viktige forhold rundt den eventuelle implementeringen av direktivet.

Det er også relevant å sette direktivet i sammenheng med andre, lignende tiltak, og ta opp hvordan direktivet påvirker det totale overvåkingsnivået i det norske samfunnet.

**Direktivet som del av en større kontekst**
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, Norges bank og Utenriksdepartementet. 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 ligningsloven 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 ved en sentral database 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 relatert til 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 registrert 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.

*Sentral lagring medfører 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*
Selv om man velger en desentralisert løsning, hvor dataene lagres hos den enkelte tilbyder, må det fra sentralt hold 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. Her støtter vi det forslaget departementene har framsatt i høringsnotatet.

*Rettskjennelse viktig for folks opplevelse av rettsikkerhet*
I 2007 gjennomførte Teknologirådet sammen med flere europeiske partnere en serie fokusgruppeundersøkelser i seks land. Undersøkelsen tok for seg ulike typer teknologi knyttet til samfunnssikkerhet og overvåkning. Deltakerne diskuterte blant annet hvilke trusler som kan rettferdiggjøre økt overvåkningsnivå, og hvilke typer teknologier og inngrep de kunne akseptere. Det var generell enighet om at den type sikkerhetsmekanisme som en rettskjennelse utgjør er viktig for å kunne akseptere inngrep i privatlivet i forbindelse med bekjempelse av kriminalitet.

*Kravene til innsyn må stå i forhold til hvor omfattende inngrepet er*
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 e-post kontinuerlig, såkalt *push mail*) medfører dette at mobiltelefonen kobles av og på nettverket hele tiden. Dette bidrar til store mengder data som blant annet avslører brukerens lokasjon nærmest kontinuerlig.

Når dataene er av så omfattende karakter, og potensielt kan gi svært 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 man har kjennskap til hvilke data som er samlet inn om en selv, 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 være av skade til etterforskningen å underrette i forkant, skal retten i sin kjennelse ta stilling til om politiets innsyn kan unndras den som er under mistanke i et fastsatt tidsrom.

**Lagringstid**
I dag lagres trafikkdata i mellom 3 og 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. For internettrafikk, som det i dag bare er anledning til å lagre i 3 uker, vil 6 måneder være en betydelig utvidelse av lagringstiden.

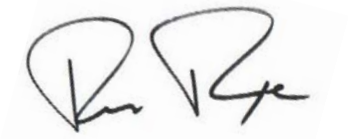
Det vil være rimelig at effekten av en slik økning evalueres før man eventuelt vurderer mer drastiske tiltak. Vi vet av erfaring at det er enklere å innføre nye eller skjerpede tiltak enn å fjerne tiltak som allerede er innført.

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.

**Avsluttende merknader**
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. Det er derfor viktig at en evaluering av datalagringsdirektivet ses i sammenheng med andre former for datalagring, så vel som sikkerhets- og overvåkingstiltak som er innført de senere årene. Dette er viktig for å forhindre at proporsjonaliteten mellom kriminalitetsbekjempelse og personvern forskyves ytterligere, og for å sikre at vi ikke får en uholdbarøkning i det generelle overvåkingsnivået.

Med vennlig hilsen



Tore Tennøe
Direktør

Christine Hafskjold
Prosjektleder

Teknologirådet
www.teknologiradet.no