Datalagringsdirektivet: Nei til EUs styremøte.

Gisle Hannemyr

22. august 2009

Datalagringsdirektivet

- Europaparlaments- og rådsdirektiv 2006/24/EF av 15. mars 2006, samt endring i europaparlaments- og rådsdirektiv 2002/58/EF.
- Omhandler lagring av trafikkdata som framkommer ved bruk av offentlig elektronisk kommunikasjon: (dvs. telefoni, mobiltelefoni og bruk av internett).
- Grunngitt med behovet for å bekjempe alvorlig kriminalitet (*detection and prosecution of serious crime, as defined by each Member State in its national law*).
- http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML

Kort om innholdet

- Pålegg om å lagre *trafikkdata* (i 6-24 måneder).
- Retter seg til *teleoperatørene*.
- *Myndighetene* vil få tilgang til lagrede data (etter rettslig begjæring).

Innholds- og trafikkdata

- **Innholdsdata**, dvs. innhold i kommunikasjonen skal ikke lagres.
- **Trafikkdata**: Hvem som ringer til hvem, hvem som sender epost til hvem. Tid, sted og varighet for kommunikasjonen.
- Datalagringsdirektivets artikkel 5 presiserer hvilke hovedkategorier av data som skal lagres.

Hva skal lagres (artikkel 5)

1. Data som er nødvendige for å spore og identifisere *opprinnelsen* til en kommunikasjon.
2. Data som er nødvendige for å identifisere *destinasjonen* til en kommunikasjon mellom individer.
3. Data nødvendige for å identifisere *dato, tid og varighet* av en kommunikasjon.
4. Data nødvendige for å identifisere *typen* kommunikasjon.
5. Data nødvendige for å identifisere *brukernes kommunikasjonsutstyr* eller hva som går for å være deres utstyr.
6. Data nødvendige for å identifisere *lokaliseringen* av mobilt kommunikasjonsutstyr.

Hva skal lagres (artikkel 5)

- Alle disse seks hovedpunkter har til sammen et tjue-talls presiserte underpunkter over data som anses nødvendige å lagre.
- Hele «kart» kan med utgangspunkt i slike data utarbeides over borgernes telekommunikasjonsvaner, kontaktnett og forbindelser.
- Endringer i forhold til dagens praksis (lagring for fakturering):
  - *Lengre lagringstid* for de data som i dag lagres for faktureringsformål.
  - Markant *utvidelse* av hva som lagres, som for eksempel lokaliserings-data og epost-logger.
  - Direktivet vil omfatte *langt flere organisasjoner*, blant annet ISPer, som i dag ikke har tradisjon for å lagre.
  - Nytt *normativt grunnlag* for lagring: Fra dagens *rett* til å lagre visse opplysninger for et forretningsmessig formål, og til en *plikt* til å lagre for politiformål.

Teleoperatørene skal lagre

- Datalagringsdirektivet innebærer at flere hundre internettleverandører (ISPere) vil måtte begynne å lagre personopplysninger som de ikke har tradisjon for å lagre.
- De vil heller ikke ha en selvstendig egeninteresse av å bruke særlig med ressurser for å sikre disse opplysningene.
  - Flere eksempler: Tele2-saken (2007). Tap av ukrypterte disker med PO om samtlige barnefamilier i UK (2007). Deutsche Telekoms ulovlige analyse av egne trafikkdata (2008).

Formålet er å bekjempe «alvorlig kriminalitet»

- Definisjonen overlates til medlemsstatene. Det betyr at ulike land kan definere (og redefinere) formålet som de ønsker.
  - Terrorisme?
  - Opptøyer?
  - Politiske demonstrasjoner?
  - Hva med strategisk informasjonsanalyse?
- Funksjonsutglidning.

Tilgang til data (artikkel 4)

- “Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law.”
- Hvem? Politet (selvsagt). Men hva med:
  - Tollvesenet?
  - Skatteetaten?
  - Kredittilsynet?
  - Konkurransetilsynet?
  - Helsevesenet?
  - Nød- og redningsetater?

Direktivet og menneskerettighetene

- Datalagringsdirektivet setter *både* personvernet og ytringsfriheten på prøve.
- Dette vil gjelde selv om lagring av trafikkdata i henhold til direktivet ikke anses som kontinuerlig eller regelmessig overvåkning av borgerne. Verdien av lagring må nemlig også veies opp mot effekter på frimodighet. Dette gjelder selv om formelle friheter ikke berøres, og selv om de registrerte data kun skal være tilgjengelige for politiet under regulerte forhold.
- Vissheten av at noen *kan lete seg fram til dine kontakter og dine bevegelser, både i det* virkelige rommet og på Internett, kan være nok til å hemme borgere i utøvelsen av sine friheter til å samles, til å ytre seg og til å søke opplysninger.

Direktivet og menneskerettighetene

- EMK artikkel 8 annet ledd åpner for at det kan gjøres inngrep i personvernet.
- Men for at et slikt inngrep skal være forsvarlig må det blant annet være *nødvendig* i et demokratisk samfunn. I dette ligger det etter Den Europeiske menneskerettighetsdomstolens (EMD) praksis at det må være en «pressing social need» for å gripe inn i personvernet. Det holder ikke at det er hensiktsmessig, rimelig eller ønskelig.
- Inngrepet som gjøres må dessuten være *proporsjonalt* i forhold til formålet som ønskes oppnådd.
- Den omfattende lagringsplikten som følger av direktivet er problematisk i forhold til *nødvendighetsprinsippet* og *proporsjonalitetsprinsippet*.