



JUSTIS- OG POLITIDEPARTEMENTET

Noen betragtninger om datalagringsdirektivet

Av

Lovrådgiver Gry Steen Hvidsten

Hva skal lagres?

- Skal lagre visse typer trafikkdata, lokasjonsdata og abonnements-/brukerdata som fremkommer ved:
 - fasttelefoni
 - mobiltelefoni
 - internettbruk
- Det skal **ikke** lagres:
 - innholdsdata
 - bevegelsesmønster på Internett

Dagens plikter for tilbydere

- Ingen lovbestemt plikt
- Lagring er en *rett* tilbyderne har av forretningsmessige hensyn
- Trafikkdata skal slettes eller anonymiseres så snart de ikke lenger er nødvendige
- Etter ekomloven har tilbyderne en **plikt til å tilrettelegge** slik at politiet får tilgang til informasjon i forbindelse med etterforskning av kriminalitet

Dagens lagringspraksis hos tilbyderne – del I

- De ansvarlige departementer har innhentet informasjon fra tilbyderne om dagens lagringspraksis
- Vår oppfatning av forholdet mellom *direktivets krav* til hva som skal lagres og *dagens lagringspraksis* kan oppsummeres på følgende måte:
 - For **fasttelefon** og **mobiltelefon** er det ikke store endringer
 - Nesten alle tilbyderne av fasttelefoni lagrer data som direktivet omfatter
 - De fleste tilbydere av mobiltelefonitjenester gjør det samme

Dagens lagringspraksis hos tilbyderne – del II

- For data knyttet til bruk av *Internett* ser bildet noe annerledes ut
- For ***internettaksess*** er det trolig riktig å si at de fleste tilbyderne lagrer navn på den abonnenten som foretar tilkoblingen og dennes IP-adresse, men at bare halvparten lagrer de resterende data som etterspørres i direktivet
- Mht ***IP-telefoni*** er det trolig riktig å si at de fleste tilbyderne lagrer A og B nummer samt dato og klokkeslett for oppkobling, men at de i mindre grad lagrer navn og adresse til abonnent som mottar samtalen

Dagens lagringspraksis hos tilbyderne – del III

- Når det gjelder **e-post** er det så langt vi kjenner til under halvparten av tilbyderne som lagrer de data som etterspørres i direktivet
- Trolig er det her forskjellen mellom dagens lagringspraksis og direktivet er størst
- På denne bakgrunn er det neppe grunnlag for å si at en gjennomføring av direktivet vil medføre noen dramatisk utvidelse ift hvilke data som skal lagres
- Lagringstiden vil kunne bli lenger enn dagens praksis

Lagringstid

- Direktivet fastsetter en lagringstid mellom 6 og 24 måneder
- I dag lagres data for fakturering som hovedregel i 3-5 måneder
- Hvor lenge data lagres for andre formål har ikke vi noe kunnskap om
- Behovet for å oppklare kriminalitet bør tillegges vekt ved valg av lagringstid
- Spørsmålet om lagringstid må avgjøres politisk
- Vi er ikke kjent med at andre land har valgt lavere lagringstid enn 12 måneder

Informasjonssikkerhet – del I

- **Informasjonssikkerheten** hos tilbyderne er avgjørende for ditt og mitt personvern
- Faren er ikke i de saker der politiet rettmessig får innsyn i lagrede data i forbindelse med en straffesak
- Derimot er det en fare for at uvedkommende skal få innsyn i informasjon om oss
- Tilbyderne har tilgang der det er nødvendig i egen forretningsvirksomhet
- I forbindelse med uthenting av informasjon til politiet skal bare særlig autorisert personell kunne bistå

Informasjonssikkerhet – del II

- Direktivet oppstilles visse krav til informasjonssikkerhet hos tilbyderne
- Disse kravene er i stor grad allerede oppfylt i norsk rett
- Kravene innebærer at de aktuelle dataene skal sikres av tilbyderne med hensyn til *konfidensialitet*, *integritet* og *tilgjengelighet*
- Urettmessig innsyn er sanksjonert med en rekke bestemmelser bl.a. i personopplysningsloven, ekomloven og straffeloven
- På lovsiden er **personvernet** godt ivaretatt

Personvernet – noen utfordringer

- Utfordringen består i å få personvernet gjennomført i praksis
- Her har tilsynsmyndighetene Post- og teletilsynet og Datatilsynet en svært viktig oppgave
- De ansvarlige departementene må tenke over hva vi kan bidra med for å legge til rette for den viktige jobben tilsynene her skal gjøre

Politiets tilgang – del I

- Ikke snakk om at alle vil bli omfattet, men kun de få som kommer i politiets søkelys i forbindelse med etterforskning av straffbare forhold av et visst alvor
- *Personvernet og rettssikkerheten* til den som kommer i politiets søkelys vil bli ivaretatt av ***straffeprosesslovens*** bestemmelser
- Denne loven er bygget opp nettopp med tanke på at man skal sikre en forsvarlig og forholdsmessig behandling av straffesaker
- Dette innebærer at også den mistenkte er sikret visse grunnleggende rettigheter som selvfølgelig skal gjelde også for datalagringsdirektivet

Politiets tilgang – del II

- Viktig å merke seg at det er ikke politiet som skal lagre data
- Lagringen skal foregå i tilbydernes systemer og verken tilbyder eller politi skal ha fri tilgang til informasjonen
- For politiet gjelder det krav om mistanke *før* tilgang
- Neppe særlig treffende å si at vi alle blir å anse som mistenkte eller at vi alle skal overvåkes

Overvåking eller mistenkeliggjøring?

- Justismyndighetene har ikke noe ønske om å legge til rette for eller gjennomføre noen form for mistenkeliggjøring og overvåking av befolkningen
- Det finnes visse skranker for hva myndighetene kan foreta seg – både lovgiver og politi
- Disse grunnleggende sidene ved vår samfunnsordning skal fortsette å gjelde selv om datalagringsdirektivet blir gjennomført
- Er man tjent med at det nærmest settes likhetstegn mellom datalagringsdirektivet og overvåking?

Skjerping av straffeprosessloven

- Direktivet medfører ingen utvidelse av politiets tilgang
- Direktivet overlater til nasjonal myndigheter å fastsette vilkår og prosedyrer
- Direktivet stiller krav om at en gjennomføring skal være i overensstemmelse med EMK artikkel 8
- Justisdepartementet legger opp til en *skjerping* av straffeprosesslovens regler om politiets tilgang, slik at rettssikkerheten til den enkelte skal bli enda bedre ivaretatt

Elektroniske spor i samfunnet

- Fra vi står opp til vi legger oss etterlater vi store mengder elektroniske spor gjennom dagligdagse aktiviteter, som bruk av:
 - Mobiltelefon
 - Internett
 - Betalingstjenester
 - Elektroniske brikker i automatiske bomstasjoner
- Videreføring og styrking av demokratiet og rettsstaten
- En slik samfunnsordning krever blant annet at behandling av personopplysninger skal være forholdsmessig og ha hjemmel i lov
- Den mistenkte garanteres visse straffeprosessuelle rettigheter

Kriminalitetsbekjempelse – politiets behov

- Direktivet er begrunnet i hensynet til kriminalitetsbekjempelse
- Nødvendig å klargjøre politiets behov
- Trafikkdata har hatt betydning for oppklaring av saker som:
 - Baneheia
 - Munch
 - NOKAS
- Hensynet til kriminalitetsbekjempelse og hensynet til personvernet må avveies

**Takk
for
oppmerksomheten!**

Spørsmål?