

Noen betraktninger om datalagringsdirektivet

Stortinget, torsdag 13. mars 2008, kl. 13.30

Av lovrådgiver Gry Steen Hvidsten

Bakgrunn

Som mange av dere sikkert er kjent med er spørsmålet om en gjennomføring av datalagringsdirektivet for tiden til behandling i de ansvarlige departementene. Det er derfor per i dag vanskelig for de ansvarlige myndigheter å delta i en debatt om direktivet, fordi man ikke har de nødvendige politiske avklaringer på plass. Når det er sagt er det klart at departementene både kan og vil bidra til å belyse hva denne saken dreier seg om, og forhåpentligvis kan vi bidra til å klargjøre de sentrale problemstillingene noe nærmere.

Selve foredraget

Jeg vil i denne presentasjonen si noe om hvordan Justisdepartementet oppfatter direktivets innhold. Jeg skal si litt om gjeldende rett og litt om hva som er nytt med direktivet. Jeg vil så godt det lar seg gjøre forsøke å skille mellom det som gjelder lagringen – som foregår hos tilbyderne – og den senere utleveringen av informasjon fra tilbyderne til politiet – det som gjelder reglene om politiets rett til innsyn.

Det som ifølge direktivet skal lagres er visse typer trafikkdata, lokasjonsdata og abonnements-/brukerdata som fremkommer ved bruk av fasttelefon, mobiltelefon og Internett. For eksempel skal man lagre at telefonnummer A har ringt til telefonnummer B samt tidspunktet og varigheten for samtalen. Innholdsdata skal ikke lagres. Direktivet sier klart at tilbyderne bare skal lagre informasjon som de allerede har i sine systemer som en følge av tjenestene de leverer (fortalen punkt 23). Informasjonen som skal lagres finnes altså hos tilbyderne i en viss periode helt uavhengig om de får en lagringsplikt eller ikke.

I dag er det ingen lovbestemt plikt for tilbyder til å lagre. Lagring er en rett tilbyderne har av hensyn til fakturering og andre forretningsmessige formål. Trafikkdata hos tilbyderne skal slettes eller anonymiseres så snart de ikke lenger er nødvendige for kommunikasjons- eller faktureringsformål. Etter ekomloven har tilbyderne allerede i dag en plikt til å tilrettelegge slik at politiet får tilgang til informasjon i forbindelse med etterforskning av kriminalitet. Det nye med direktivet er at tilbyderne blir pålagt å lagre data av hensyn til kriminalitetsbekjempelse.

Som ledd i arbeidet med denne saken har de ansvarlige departementer innhentet informasjon fra tilbyderne om dagens lagringspraksis. Vår oppfatning av forholdet mellom direktivets krav til hva som skal lagres og dagens lagringspraksis kan kort oppsummeres på følgende måte:

Når det gjelder fasttelefon og mobiltelefon så er det ikke store endringer det er tale om. Nesten alle tilbyderne av fasttelefoni lagrer de data som direktivet omfatter. Det er også slik at de fleste tilbydere av mobiltelefonitjenester gjør det samme.

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.

Når det gjelder e-post er det så langt vi kjenner til under halvparten av tilbyderne som lagrer de data som etterspørres i direktivet. Det er derfor trolig 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.

En annen sak er selvfølgelig at lagringstiden vil bli forlenget. Direktivet overlater som kjent til de nasjonale myndigheter å fastsette en lagringstid mellom 6 og 24 måneder. I dag lagres data for fakturering som hovedregel i 3-5 måneder. Departementet har ikke kunnskap om hvor lenge data lagres for andre formål.

Justisdepartementet mener at samfunnets behov for å oppklare kriminalitet bør tillegges vekt ved valget av lagringstid. Spesielt i saker om alvorlig organisert kriminalitet strekker etterforskningen seg over en lengre tidsperiode. I disse sakene kan det blant annet ta lang tid til å få oversikt over alle de involverte. Dersom data først er slettet, er det ikke mulig for politiet å få tak i bevisene. Politiet vil heller ikke kunne gjøre seg noen nytte av frys-reglene i straffeprosessloven dersom de ikke har noen konkret mistenkt å knytte saken til. Også etterforskningen av såkalte seriesaker krever betydelige ressurser og det kan ta lang tid før politiet ser sammenhengen mellom flere straffbare handlinger, jf. Lommemann-saken. Etter det vi har fått opplyst fra politiet er det også mange eksempler på saker der eldre trafikkdata ville medvirket til mer oppklaring og raskere oppklaring dersom slike data hadde vært tilgjengelig. Spørsmålet om lagringstid må avgjøres politisk. Så langt kan vi bare si at andre land ser ut til å velge minimum 12 måneders lagring.

Etter departementets oppfatning er det i stor grad informasjonssikkerheten hos tilbyderne som er avgjørende for ditt og mitt personvern. Da tenker jeg ikke på saker der politiet rettmessig får innsyn i lagrede data i forbindelse med en straffesak, men faren for at uvedkommende skal få innsyn i informasjon om oss.

Tilbyderne selv skal kun ha adgang til data i den grad dette er nødvendig av hensyn til egen forretningsvirksomhet. I forbindelse med uthenting av informasjon til politiet skal bare særlig autorisert personell kunne bistå. Det hører også med til dette bildet at data som lagres hos tilbyderne, har karakter av råmateriale i ulike dataformater, og at en viss teknisk bearbeiding er nødvendig før de har en egentlig informasjonsverdi. Slik bearbeiding vil bare skje der det foreligger hjemmel for innsyn.

Direktivet oppstilles visse krav til informasjonssikkerheten 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 og ekomloven men også i straffeloven, for eksempel hvis det er utenforstående som ved datainnbrudd skaffer seg tilgang til tilbydernes systemer. På lovsiden er personvernet således nokså godt ivaretatt. Utfordringen består i å få dette personvernet gjennomført i praksis. Her har tilsynsmyndighetene – Post- og teletilsynet og kanskje særlig Datatilsynet – en svært viktig oppgave. Også de ansvarlige departementene må tenke over hva vi kan bidra med for å legge til rette for den viktige jobben tilsynene her skal gjøre.

Det som så langt er sagt gjelder i hovedsak lagringen hos tilbyderne. Lagringen skal – på samme måte som den lagringen tilbyderne foretar i dag – omfatte oss alle. Som jeg har vært inne vil personvernet her ivaretas av de krav til informasjonssikkerhet som skal gjelde.

For politiets rett til innsyn, blir bildet et annet. Her er det ikke lenger 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. Eksemplet som har vært brukt med at en gjennomføring av direktivet vil være som å si ja til at det i alle tilfeller skal stå en betjent fra politiet og notere seg navnet på hvem som sender brev til hverandre er etter departementets syn en lite treffende beskrivelse av situasjonen. Det er ikke politiet som skal samle inn eller lagre data. Lagringen skal foregå i tilbydernes systemer og verken tilbyder eller politi skal ha fri tilgang til informasjonen. For politiets del vil det gjelde et krav om at det før innsyn foretas må foreligge en konkret mistanke. Det er derfor neppe særlig treffende å si at vi alle blir å anse som mistenkte eller at vi alle skal overvåkes. I alle fall det siste blir positivt galt.

Direktivets artikkel 4 om adgang til data, medfører i seg selv ingen utvidelse av politiets rett til innsyn. Tvert imot overlater bestemmelsen til nasjonale myndigheter å fastsette de vilkår og prosedyrer som skal gjelde. Direktivet stiller imidlertid krav om at utlevering kun skal skje til de rette myndigheter og med hjemmel i lov. Her ser man at direktivet selv legger opp til at de nasjonale myndigheter i sin gjennomføring skal og må ta høyde for de krav som følger av menneskerettighetslovgivningen og da særlig Den europeiske menneskerettighetskonvensjon (EMK) artikkel 8 om beskyttelse av privatliv og familieliv.

EMK artikkel 8 angir på sin side at inngrep i personvernet kan aksepteres dersom dette fastsettes i lov og inngrepet anses nødvendig for å forebygge kriminalitet eller for å beskytte andres rettigheter eller friheter. Selv om direktivet medfører at lagring av trafikkdata skal skje for et nytt formål, er det altså rettslig sett fullt lovlig å fastsette en slik plikt så lenge man holder seg innenfor de rammer som følger av EMK artikkel 8. Dette vil selvfølgelig norske myndigheter også forholde seg til.

Justisdepartementet legger opp til en skjerping av straffeprosesslovens regler om politiets rett til innsyn, slik at rettssikkerheten til den enkelte skal bli enda bedre ivaretatt. I dag er det nemlig slik at tilbyderne i stor grad kan velge om de vil utlevere trafikkdata til politiet som ledd i en frivillig vitneforklaring eller om de vil kreve at politiet fremlegger en beslagsbeslutning. Forskjellen på disse to alternativene er at tilbyder gjennom sitt valg påvirker rettssikkerheten til den informasjonen gjelder, nemlig den som har ringt eller sendt en e-post. Dersom utlevering skjer som en frivillig vitneforklaring gjelder ikke de samme prosessuelle krav og rettssikkerhetsgarantier som i de tilfeller der politiet må anvende tvang for å få tilgang til et bevis. Det er Justisdepartementets klare oppfatning at disse sakene for fremtiden bør følge tvangsmiddelsporet.

Mange har tatt sterke ord i bruk i sin beskrivelse av direktivet. Det er blant annet uttalt at direktivet innebærer en form for totalitært svermeri.

Antydningen om at de ansvarlige myndigheter skulle være tilhengere av totalitære regimer eller at vi i beste fall ikke helt forstår alvoret i saken vi selv holder på med, synes vi nok imidlertid er å gå noe langt. Og man kan spørre om personverndebatten som vi i høyeste grad skal ta på alvor, er tjent med en slik ordbruk.

Justismyndighetene har ikke noe ønske om å legge til rette for eller gjennomføre noen form for mistenkeliggjøring og overvåking av befolkningen på generelt grunnlag. Det fremgår av det som er sagt at dette heller ikke er mulig så lenge vi lever i en demokratisk rettsstat som baserer seg på grunnleggende rettssikkerhetsgarantier og menneskerettigheter for alle borgere. Det finnes visse skranker for hva myndighetene kan foreta seg – både lovgiver og politi. Jeg antar vi alle må være enige om at disse grunnleggende sidene ved vår samfunnsordning skal fortsette å gjelde selv om datalagringsdirektivet blir gjennomført.

Man kan også spørre om den mer overordnede debatten om ”overvåkingssamfunnet” er tjent med at det nærmest settes likhetstegn mellom datalagringsdirektivet og overvåking. Det er jo ikke slik at et ”ja” eller ”nei” til datalagringsdirektivet er et ”ja” eller ”nei” til overvåkingssamfunnet. Fra vi står opp til vi legger oss etterlater vi store mengder elektroniske spor gjennom dagligdagse aktiviteter, som bruk av mobiltelefon, Internett, betalingstjenester og passeringbrikker i automatiske bomstasjoner. Elektroniske spor er en realitet i dagens samfunn enten vi liker det eller ikke. Og i kampen for å sikre at personvernet også for fremtiden skal være en verdi som verdsettes på linje med andre grunnleggende interesser og verdier, er en videreføring og styrking av demokratiet og av rettsstaten trolig veien å gå. En slik samfunnsordning krever blant annet at behandling av personopplysninger skal være forholdsmessig og ha hjemmel i lov. Den krever også at den som mistenkes garanteres visse straffeprosessuelle rettigheter. Personvernet vil imidlertid ikke kunne være det eneste hensynet som kan tillegges vekt i vurderingen av en sak. Det må også være legitimt for ansvarlige myndigheter å vektlegge andre hensyn, herunder kriminalitetsbekjempelse.

Dette bringer meg over i det siste og avsluttende poenget, nemlig spørsmålet om hvilken betydning denne typen bevis har for oppklaringen av kriminalitet. Dette har ikke departementet særlige forutsetninger for å mene så mye om. Vi er imidlertid kjent med at trafikkdata har hatt betydning for oppklaringen av blant annet Baneheia-saken, ranet på Munch-museet og NOKAS-saken. Det er nok departementets syn at politiets behov har blitt for dårlig belyst i debatten så langt. Jeg antar at det senere innlegget fra politiet vil bidra til å rette opp noe i så måte. Det er ikke til å komme bort fra at betydningen denne typen bevis har for oppklaring av alvorlig kriminalitet, er et sentralt moment ved vurderingen av saken. Det er tross alt hensynet til kriminalitetsbekjempelse som begrunner hele direktivet. Vi kan derfor ikke diskutere datalagring uten å være villige til å høre på hva politiet har å si, og så får vi vurdere om dette kan forsvare innføringen av en lagringsplikt. I denne vurderingen vil selvfølgelig også personvernet inngå som en viktig del.

Takk for oppmerksomheten !