NORGES JURISTFORBUND
PRIVAT

Samferdselsdepartementet
Postboks 8010 Dep
0030 OSLO

Også sendt som e-post til
postmottak@sd.dep.no

Dato: 26. mars 2010

Høringsuttalelse fra NJ-Privat vedrørende datalagringsdirektivet

Innledning

Det vises til departementets høringsbrev av 8. januar 2010.

Denne høringsuttalelsen avgis på vegne av NJ-Privat, som er en av fem seksjoner i Norges Juristforbund. NJ-Privat består av ansatte og selvstendig næringsdrivende jurister, advokatfullmektiger og advokater i privat sektor. Seksjonen representerer omkring 6 000 av Norges Juristforbund 16 000 medlemmer.

Formålet med direktivet

Formålet med direktivet er primært å bedre mulighetene for å etterforske og oppklare grov kriminalitet. De store terrorangrepene i bl.a. London er noe av bakteppet for direktivet. Et av målene er å hindre organisert kriminalitet.

Om typer informasjon som skal lagres

Det skal lagres opplysninger om brukerne av telefoni, internett, e-post og IP-telefoni. Dette er bl.a. A-og B-nummer for vanlig telefoni, brukeridentitet for e-post, dato og klokkeslett for kommunikasjonen og mye mer. Noen av disse opplysningene gir en ganske sikker person-identifikasjon av hvem som har forestått kommunikasjonen, for eksempel et A-nummer i en husholdning med en person. For IP-numre i store bedrifter vil en slik personidentifikasjon være mer usikker, mens man nok ofte vil kunne se fra hvilket firma en kommunikasjon kommer.

Det er dessuten særlig angitt at man skal lagre lokaliseringsdata for mobiltelefoner, slik at man kan fastslå hvor mobiltelefonen befant seg da kommunikasjonen ble startet. EU/EØS har dessverre ikke åpnet for at medlemsstatene kan velge ikke å lagre de opplysningene direktivet angir.

Det er hevet over tvil at det nå vil lagres typer informasjon som man ikke har lagret tidligere. Dessuten er omfanget av opplysninger som skal lagres svært stort.

Fra et personvernmessig standpunkt er det åpenbart at de typer av data som direktivet angir er svært omfattende. En slik gjennomgripende registrering er uheldig.

Særlig om satellittelefoni

Satellittelefoni er ikke eksplisitt nevnt i direktivet og det er derfor uklart om det omfattes.

Samferdselsdepartementet har tidligere opplyst at satellittelefoni omfattes av direktivet, og bygger dette på en tolkning av direktivet og ekom-loven. Departementets synspunkt er at satellittelefoni er en offentlig elektronisk kommunikasjonstjeneste og at operatører som tilbyr slike tjenester er tilbydere og derfor omfattet av direktivet.

Denne tolkningen er rettslig sett tvilsom, ettersom direktivet lister klart opp hvilke kommunikasjons-former som er omfattet. Satellittelefoni nevnes ikke. En slik lovgivningsteknikk som spesifikt lister opp hva som er omfattet, tolkes normalt slik at det som ikke er tatt med heller ikke er omfattet.

Det kan derfor anføres at direktivet faktisk ikke kommer til anvendelse på satellittelefoni. Det er da uheldig at høringsnotatet ikke utdyper problemstillingen. Lovgiver står selvsagt fritt til å utvide og dermed inkludere satellittelefoni i den norske reguleringen.

Men også dersom satelittelefoni er omfattet av direktivet, oppstår et sentralt spørsmål. Nemlig om man med det har stengt også denne kommunikasjonskanalen for terrorister. Sannsynligvis ikke. Sannsynligvis vil de bare velge sin leverandør av satellitt-tjenester med omhu. Noe av problemet er jo at satellitter ikke tilhører en enkelt nasjon. Direktivets lagringsregler vil kun gjelde for satellitter/operatører innenfor EU/EØS-området.

Hvis man ønsker det kan man derfor enkelt unngå at data blir lagret. Det er ikke vanskelig eller særlig dyrt heller. Dette koster noe og krever en viss planlegging, men man kan sitte i London eller Oslo og prate med folk i Afghanistan uten at opplysningene lagres. Enkelte satelittelefoner kan også benyttes for internettaksess, enten fra telefonen eller tilkoplet datautstyr. Slik kan man enkelt kommunisere også over internett via satelittelefon uten at trafikkdata lagres.

Det vurderes derfor som meget uheldig at satelittelefoni ikke er problematisert i høringsnotatet.

Særlig om anonymitet, omgåelse og konvergens
Konvergens, anonymitet og mulighetene for omgåelse er heller ikke tilstrekkelig problematisert i høringsnotatet, og dette er etter vår mening svært beklagelig.

Ved bruk av anonyme proxyservere eller programvare designet for å hindre sporbarhet og sikre anonymitet, f.eks. The Onion Ring (www.torproject.org) eller Dold (www.dold.se) kan den som ønsker det unngå lagring av detaljerte trafikkdata. Ved å benytte krypterte trafikkanaler og webbaserte e-posttjenester, kan den som ønsker det enkelt kommunisere uten å legge igjen slik informasjon som man med direktivet ønsker å fange opp.

Videre eksisterer det allerede en rekke selskaper som tilbyr anonyme VPN-tjenester med krypterte linjer ut av datalagringsdirektivets virkeområde. Et eksempel er Panama-baserte ShadowVPN (www.shadowvpn.com) som annonserer å være *" outside of the jurisdiction of the US, UK, EU, and other surveillance societies"*. Kommunikasjon som foregår over krypterte linjer via land som ikke har tilsvarende regler om lagring av trafikkdata, gjør det tilnærmet umulig å identifisere avsender/mottaker uavhengig av om de rent fysisk sitter få meter fra hverandre eller i hver sin verdensdel. Eventuell dekryptering og analyse av trafikkdataene lokalt eller innenfor direktivets virkeområde, vil gi begrenset verdi i og med at det er satt en effektiv stopper for muligheten for å identifisere avsender/mottaker fordi trafikkdataene allerede er slettet i et eller flere ledd.
IP-telefoni, herunder også bruk av IP-telefoni på mobiltelefon, enten via mobilt bredbånd, trådløst nettverk eller via nettverksdeling fra PC/Mac, kan også benyttes via anonyme nettverk og VPN-tjenester som nevnt ovenfor.

Teknologi konvergerer raskere enn tidligere, og det er et spørsmål om tid før man får støtte for anonymiseringstjenester også for forskjellige typer av mobiltelefoner. Det som da sannsynligvis vil lagres hos operatøren er at man er koplet opp mot en basestasjon, og at det går krypterte data frem og tilbake. Regjeringen har selv dokumentert akselererende konvergenstendenser, se NOU 1999:26 Konvergens (Sammensmelting av tele- data- og mediesektorene) og Ot.prp. nr. 58 (2002-2003), særlig punkt 2.4.3 Teknologiutviklingen (Om elektroniske kommunikasjonsnett). Her hevdes det at ekom-loven tar høyde for fremtidig konvergens. Historien har vist at dette er svært vanskelig i og med at det er tilnærmet umulig å forutsi retningen den fremtidige konvergensen vil ta.

I datalagringsdirektivet fremgår det ikke hvordan fremtidig konvergens skal håndteres, og dette er heller ikke problematisert i høringsnotatet. Høringsnotatet nevner konvergens i relasjon til lagringstid (punkt 4.8) og antyder at på grunn av konvergensen bør lagringstiden være den samme uavhengig av tjeneste/teknologi. Dette bygger tilsynelatende på en misforståelse av konsekvensene av konvergens. Direktivets utfordringer med konvergens er ikke lagringstiden, men at utviklingen gjør det stadig enklere å omgå lagring av trafikkdata og dermed øke mulighetene for å være anonym uavhengig av hvilken kommunikasjonsform som benyttes. Resultatet blir at direktivet vil virke for de det ikke er ment å virke for, mens de man ønsker å fange opp enkelt kan omgå systemet.

Lagringstid
Direktivet fastslår at medlemsstatene skal lagre bestemte kommunikasjonsdata i en viss tidsperiode. Lagringstiden kan bli fra seks måneder til to år. Høringsnotatet angir at myndighetene vil utsette å angi hvilken lagringstid som velges. En slik utsettelse er sterkt kritikkverdig fordi man på den måten splitter opp debatten.

Samfunnsdebatten rundt direktivet har i stor grad vært preget av synspunkter om "jo lenger lagringstid, jo farligere for personvernet". Det kan derfor tenkes å være vesentlig lettere å få et politisk flertall for direktivet når man utelater å ta stilling til lagringstiden. Slik sett er den prosedyre som er valgt sterkt kritikkverdig.

På den annen side må det fremheves at de prinsipielle personvernmessige problemer ikke alene er knyttet til lagringstid.

Høringsnotatet ber spesielt om tilbakemelding på lagringstid. Generelt er det slik at jo kortere lagringstid, jo mindre er personvernulempene. Det innebærer ikke at man kan si at det ikke foreligger personvernulemper ved en kort lagringstid. Her kommenteres ikke lagringstid ytterligere ettersom det ikke er foreslått noen konkret periode fra departementene.

Overvåking av uskyldige?
Mange mener at direktivet innfører et nytt prinsipp, nemlig overvåking av personer som ikke er mistenkt for noe. Prinsipielt er det ikke mulig å argumentere mot dette synspunktet. Og slik sett er det ikke rart at folk reagerer mot direktivet.

Det blir på mange måter en teoretisk diskusjon om man skal kalle dette overvåking eller ikke. Uansett medfører direktivet at det lagres vesentlig mer informasjon om oss enn tidligere.

Hvis man tror at informasjonen aldri vil bli brukt til noe annet enn hva direktivet angir, så kan man kanskje forsvare direktivet. Hvis ikke, er det mye mer komplisert.

Mange tror at bruken av opplysningene ikke vil være begrenset til dette direktivets regler. Det har lenge vært et personvernmessig prinsipp at individene skal ha kontroll med informasjon som

omhandler dem selv. Dersom stadig mer informasjon om oss registreres og brukes av myndighetene, uthules dette prinsippet.

Mange er redde for at direktivet varsler et vesentlig endret samfunn der vi alle er mer langt kartlagt av myndighetene – og kanskje av andre enn myndighetene. Det er ikke slik at de som forfekter dette synet er for kriminalitet eller terrorisme. Det at store folkemengder mobiliserer mot direktivet er i seg selv et argument for ikke å implementere det. Det handler om å respektere samfunnskontrakten.

Lekkasjer, utglidning og misbruk?
Over tid vil det ganske sikkert skje tilfeldige lekkasjer fra slike registre. I pressen har mange også nevnt faren for at ansatte hos teleoperatøren kan "snoke" i opplysningene. Det er heller ikke utenkelig at slike opplysninger kan tenkes å bli "kjøpt ut" hvis de representerer en stor verdi. Over tid er det uansett sannsynlig at det vil skje lekkasjer av informasjonen.

Direktivets hensikt er aktverdig. Men mange er redde for at reglene kan bli misbrukt. Det kan skje på mange måter. De aktuelle opplysningene *kan* brukes til å gi en ganske god oversikt over hvem som har kontakt med hvem i vårt samfunn. Noen av opplysningene kan også brukes til å lokalisere personer. De fleste vil forstå at dette er opplysninger som kan tenkes å ha interesse i mer enn kriminalrettslig forstand. Det er sannsynlig at slik informasjon også representerer en økonomisk verdi.

Det er i første rekke myndighetene som bestemmer hvordan opplysningene skal bli brukt. Etter dagens direktiv vil opplysningene som nevnt kun bli brukt til å oppklare grov kriminalitet. Men hva hvis vi skulle få et annet politisk regime? Hvordan vil et totalitært regimes definisjon av grov kriminalitet være? For totalitære regimer vil denne type opplysninger være ypperlige til å identifisere motstandere og deres nettverk. Hvem tør si at dette ikke kan skje hos oss?

Det er også ofte slik at det nesten er en naturlov i det at informasjon som eksisterer, vil bli brukt. Ofte i en helt annen sammenheng enn hva man først tenkte seg. Man trenger ikke et totalitært regime for at dette skal skje. Derfor må man tørre å se på direktivets konsekvenser i en større sammenheng enn hva direktivet selv oppsetter. Kritikerne av direktivet frykter at politikerne vil finne stadig nye måter å bruke opplysningene på slik at personvernet skrumper ytterligere inn.

Økonomiske hensyn
Det er teleoperatørene som skal lagre opplysningene. Lagring koster penger.

Informasjon om hvem en person eller en bedrift ringer eller sender e-post til kan være interessant for mange. Lagringen skal teleoperatørene naturligvis gjøre på en sikker måte, slik at opplysningene ikke lekker ut.

Teleaktører er private aktører med krav til overskudd og det vil bli fordyrende for forbrukerne at enda flere datasystemer må innføres. Datatilsynet har uttalt at mange av de aktørene som skal oppbevare opplysningene sliter med forsvarlig sikring av data. Det er ikke betryggende.

Dessuten kommer et betydelig kostnadselement til for å kontrollere systemene. Denne kostnaden vil i stor grad indirekte også bæres av forbrukerne.

Dersom datalagringsdirektivet blir vedtatt er det sikkert at en av de største vinnerne er konsulentselskapene som skal utvikle systemene som må til for å ivareta reglene.

Prinsipielle personvernmessige betraktninger
Et grunnleggende spørsmål er hva vi oppnår ved å innføre et slikt direktiv og hva man taper av personvernverdier. Vil direktivet virkelig redusere risikoen for alvorlig kriminalitet og terror samt øke muligheten for å oppklare slikt? Vi er i tvil om det vil være tilfelle.

Direktivet vil nok forhindre visse typer planlagt aktivitet, men det er tvilsomt om det vil forhindre impulsive fysiske overgrep. Undersøkelser viser at slike overgrep som regel er planlagt av gjerningsmannen. Da vil lagring av opplysninger neppe forhindre dem. Registreringen vil nok oppklare noen slike forbrytelser, men dette må ikke forkles som at overgrep vil forhindres.

De som planlegger terror vil antakelig ha ressurser til å kommunisere på måter som gjør at oppklaring likevel blir vanskelig.

Man må tørre å stille en økt oppklaringsprosent opp mot ulempen av at diverse små og store teleaktører sitter på opplysninger om bl.a. hvor Norges befolkning befinner seg når de bruker sin mobiltelefon. Det er store svakheter knyttet til bevisverdien av at oppklaringsprosenten vil øke med innføringen av direktivet.

Man må dessuten innse at misbruk av den lagrede informasjonen vil skje. Omfang og konsekvenser av slikt misbruk må tas inn i vurderingen av om direktivet skal innføres. Det er naivt å tro at alle små og store teleselskapene vil ha gode nok datasystemer, uansett hva slags regelsett som gjelder for informasjonssikkerhet. Det må dessuten antas at kriminelle miljøer både vil ønske og klare å få ut informasjon fra slike registre. Likeledes må man innse at ansatte vil kunne "snoke" i registrene. Historien viser at bevisste og ubevisste lekkasjer er et reelt problem. Selv politiets registre er med jevne mellomrom gjenstand for lekkasjer.

Det er ytterligere et tankekors at høringsnotatet gir uttrykk for at man av personvernhensyn ikke har ønsket å foreslå en sentral lagringsløsning for de aktuelle opplysningene som skal lagres. Dersom man valgte å oppbevare opplysningene i ett register, burde man kunne legge større ressurser i informasjonssikkerhet som skal hindre misbruk og lekkasjer. Når et slikt arbeid – av personvernhensyn - isteden settes ut til private små og store aktører – så må det i realiteten være et enormt tungtveiende argument mot selve direktivet.

Høringsnotatet argumenterer bla med at direktivet kan øke oppklaringsprosenten for politiet, og at ny teknologi kan gi avgjørende bevis i mange saker. Etter vår oppfatning har dette argumentet svært liten vekt, fordi det ikke angir noen kjerneverdi for hvor eventuelle grenser for innsamling av bevis går.

Hvis vi ved hjelp av ny teknologi kan sikre flere bevis, hvorfor stoppe med det som angis i dette direktivet? Og hvorfor forbeholde direktivets regler for grov kriminalitet? Kan man ikke både effektivisere og sikre flere bevis ved ytterligere overvåking og registrering?

Noen har allerede foreslått at alle biler bør ha ferdskrivere koblet opp mot GPS. Og hvorfor stoppe der? Hvorfor ikke fotoovervåke alle skolerom for å forhindre overgrep? Og hvorfor ikke videokamera i alle rom hjemme så det ikke skjer noen overgrep der heller. Er det helt utenkelig at også enkeltpersoners bevegelser bør registreres gjennom en liten implantert chip?

Konklusjon

Med bakgrunn i de betenkeligheter som er skissert ovenfor, anbefaler derfor Norges Juristforbund – seksjon NJ-Privat, at direktivet ikke implementeres i norsk rett.

For styret i NJ-Privat

Henry Tengelsen
styreleder