DET KONGELIGE
UTENRIKSDEPARTEMENT

Samferdselsdepartementet
Postboks 8010 Dep
0030 OSLO
Norge

10/00463-5 12.4.2010

Høring om datalagring

Det vises til brev av 08.01.2010 fra Samferdselsdepartementet angående høringsnotat utarbeidet av Samferdselsdepartementet, Justisdepartementet og Fornyings-, administrasjons- og kirkedepartementet i fellesskap. Utenriksdepartementet vil i det følgende gi innspill til spørsmålet som er reist i høringsnotatet om direktiv 2006/24/EF (datalagringsdirektivet) kan gjennomføres i norsk rett i samsvar med Norges menneskerettighetsforpliktelser. I tillegg vil departementet knytte noen kommentarer til forholdet mellom felles regler om tilgang til trafikkdata og Norges deltakelse i det internasjonale justispolitiske samarbeidet.

Utenriksdepartementet anser at temaet for høringen omfatter to i prinsippet adskilte spørsmålsstillinger. Det gjelder for det første om Norge skal akseptere at direktiv 2006/24/EF om datalagring innlemmes i EØS-avtalen som en ny internasjonal forpliktelse. For det annet dreier høringen seg om innholdet i bestemmelser som gjennomfører plikten til datalagring og regulerer myndighetenes tilgang til lagrede data innenfor det nasjonale handlingsrom som direktiv 2006/24/EF oppstiller.

I høringsnotatet vises til at det i forbindelse med innføring av nye og inngripende tiltak er nødvendig å se sammenhenger mellom de ulike tiltakene, og totaleffekten av dem. Hver for seg kan tiltakene være akseptable, men samlet kan de utgjøre et uakseptabelt inngrep. Dette aspektet må også være en del av personvernvurderingen når gjennomføring av datalagringsbestemmelser skal avgjøres (s. 26). Utgangspunktet for vurderinger knyttet til innlemmelse av internasjonale normer i norsk rett må likevel være det nasjonale handlingsrommet for regulering av vedkommende samfunnsområde som fremgår av den internasjonale normsettingen. Det betyr konkret at det står norske myndigheter fritt å endre eller oppheve parallelle eller konkurrerende nasjonale

N-, Norge N-0251 Oslo 7694.05.12618 972 417 920 +47 22 24 36 00 +47 22 24 95 80/81 post@mfa.no www.odin.dep.no/ud

bestemmelser for å sørge for en forsvarlig gjennomføring av nye internasjonale normer. Videre betyr det at vurderingen av hvorvidt et internasjonalt regelverk anses akseptabelt, må knyttes til de konkrete forpliktelser som er fastsatt. De nærmere vurderinger av hvordan det nasjonale handlingsrommet skal utnyttes, er derfor prinsipielt annerledes enn spørsmålet om aksept av den internasjonale normsetting. Dersom nasjonale myndigheter har et vidt spillerom, vil det likevel ha betydning for den overordnede vurderingen av om de internasjonale normene anses akseptable.

Skillet mellom vurdering av akseptabilitet og gjennomføring av direktivets handlingsrom gjelder også i forhold til vurderinger av Norges menneskerettsforpliktelser. Det er prinsipielt mulig å anse at direktivet er forenlig med gjeldende menneskerettigheter, samtidig som innholdet i og den konkrete anvendelse av nasjonale gjennomføringsbestemmelser til direktivet potensielt kan resultere i krenkelse av de samme forpliktelser.

For det tredje må det understrekes at uavhengig av hvordan direktivet vurderes, er det behov for å ta stilling til spørsmålet om rettshåndhevende myndigheters tilgang til trafikkdata i norsk rett. Som påpekt av Metodeutvalget, gjengitt i høringsnotatet, er det i dag den enkelte teletilbyders praksis som er avgjørende for hvilke krav som stilles til politiets beslutning om å innhente trafikkdata. "Dette kan enten skje ved at teletilbyder utleverer opplysningene frivillig, etter beslutning fra Post- og teletilsynet om å oppheve tilbyders taushetsplikt, etter beslutning om beslag eller utleveringspålegg, eventuelt etter straffeprosessloven § 216b. Denne situasjonen er etter utvalgets oppfatning lite tilfredsstillende." Etter gjeldende regelverk som følger av direktiv 2002/58/EF, skal dessuten trafikkdata slettes av tjenestetilbyder når de ikke lenger er nødvendige for å utføre eller fakturere tjenesten, men statene har etter direktivets artikkel 15 (1) kompetanse til å fastsette nasjonale regler for lagring av slike data. Ulikhet i utøvelsen av denne nasjonale kompetansen har medført behov for en slik ytterligere harmonisering som følger av datalagringsdirektivet. Det kan på denne bakgrunn ikke utelukkes at mer presis europeisk lovgivning om datalagring vil kunne påvirke vurderingen av de krav til klarhet og forutberegnelighet i nasjonal rett som følger av gjeldende menneskerettsforpliktelser.

Direktivet søker å avveie hensynet til en effektiv kriminalitetsbekjempelse med ivaretakelse av personvernet. Gjeldende menneskerettsforpliktelser pålegger myndighetene en plikt til bl.a. å respektere individets privatliv, familieliv, hjem og korrespondanse. Særlig relevante er bestemmelsene i Den europeiske menneskerettskonvensjon (EMK) artikkel 8 og tilhørende praksis fra Den europeiske menneskerettsdomstol (EMD), artikkel 17 i FNs konvensjon om sivile og politiske rettigheter og artikkel 16 i FNs konvensjon om barnets rettigheter. Disse reglene er gjort til norsk rett i lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven).

EMK artikkel 8. *Retten til respekt for privatliv og familieliv*

1. Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.
2. Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.

FNs konvensjon om sivile og politiske rettigheter artikkel 17
1. Ingen må utsettes for vilkårlige eller ulovlige inngrep i privat- eller familieliv, hjem eller korrespondanse, eller ulovlige inngrep på ære eller omdømme.
2. Enhver har rett til lovens beskyttelse mot slike inngrep eller angrep.

FNs konvensjon om barnets rettigheter artikkel 16
1. Ingen barn skal utsettes for vilkårlig eller ulovlig innblanding i sitt privatliv, sin familie, sitt hjem eller sin korrespondanse, eller for ulovlige angrep mot sin ære eller sitt omdømme.
2. Barnet har rett til lovens beskyttelse mot slik innblanding eller slike angrep.

Ved anvendelsen av disse bestemmelsene må det først tas stilling til om et bestemt tiltak innebærer et inngrep i rettigheten. Hvis svaret er ja, må det deretter tas stilling til om inngrepet er legitimt ut fra de kriterier som er fastsatt. At det antas å foreligge et inngrep i retten til privatliv, er derfor ikke det samme som at menneskerettighetene må anses krenket ved det aktuelle tiltaket. Det avgjørende er om tiltaket er "i samsvar med loven og er nødvendig i et demokratisk samfunn" av hensyn til ett av de fastsatte målene.

Plikten til å verne retten til privatliv er både negativ, dvs. at myndighetene selv skal avstå fra inngrep, og positiv, dvs. at myndighetene skal beskytte mot krenkelser begått av andre. Internasjonale vedtak og anbefalinger om samarbeid for å bekjempe kriminalitet kan dessuten gi veiledning om den konkrete avveiningen mellom disse hensynene, bl.a. ved bekjempelse av terrorisme og annen alvorlig, organisert kriminalitet og i forhold til datakriminalitet.

Selv om direktivet pålegger en lagringsplikt som statene skal rette mot tilbydere av relevante telekommunikasjonstjenester, er det forholdet mellom myndighetene og brukerne av disse tjenestene som utløser personvernspørsmål. EMD har forutsatt at tjenestetilbyderes egen håndtering av slike data ikke berører retten til privatliv, se bl.a. Malone mot Storbritannia, saksnummer 8691/79, dom 2. august 1984, avsnitt 84, og P.G. og J.H. mot Storbritannia, saksnummer 44787/98, dom 25. september 2001, avsnitt 42. Tjenestetilbyderes innhenting og lagring av trafikkdata for å ivareta forbrukerhensyn til kvalitetskontroll og korrekt fakturering må anses legitim så lenge uvedkommende hindres i å få tilgang til slike data. Det er derfor direktivets plikt til å lagre slike data for det angitte formålet – dvs. å sikre kompetente myndigheter tilgang

til trafikkdata på nærmere bestemte betingelser - som gjør det aktuelt å anse at det foreligger et inngrep i retten til privatliv. Dette henger sammen med at trafikkdata kan gi informasjon om den individuelle bruken av slike tjenester dersom trafikkdata sammenstilles med aktuell kundeinformasjon. Ved å koble opplysninger om bruken av telekommunikasjonstjenester og personlig identitet til brukeren av tjenesten, kan det indirekte gi informasjon som er vernet av retten til privatliv og korrespondanse. Det gjelder selv om innholdet i telefonsamtaler, e-post og annen digital kommunikasjon faller utenfor plikten til å lagre trafikkdata. EMD har i avgjørelsen i P.G. og J.H. mot Storbritannia, i avsnittet referert ovenfor, likevel ansett at registrering av innholdsdata, f.eks. ved å avlytte en telefonsamtale, er et mer inngripende tiltak enn lagring av trafikkdata.

Direktivets pålegg om lagring av trafikkdata er en konsekvens av den teknologiske utviklingen. Det antas i mindre utstrekning å være påkrevd for tilbydere av telekommunikasjonstjenester å lagre trafikkdata for de angitte forbrukerrelaterte formål. Direktivet innebærer derfor i hovedsak at data som hittil er blitt lagret av tilbyderne av tjenester av forretningsmessige hensyn, fortsatt skal lagres på grunnlag av et annet hensyn, nemlig rettshåndhevende myndigheters evne til fortsatt kriminalitetsbekjempelse. EMD har ansett at slik lagring av trafikkdata i sammenheng med potensiell tilgang til data for kompetente myndigheter utgjør et inngrep i henhold til artikkel 8, se i tillegg til de avgjørelser som er nevnt ovenfor, Amann mot Sveits, saksnummer 27798/95, dom 16. februar 2000, avsnitt 69, og S. og Marper mot Storbritannia, saksnummer 30562/04 og 30566/04, dom 4. desember 2008, avsnitt 67. Dette gjelder uavhengig av om det faktisk kan godtgjøres at det er gitt tilgang til individuelle lagrede data, se Klass og andre mot Tyskland, saksnummer 5029/71, dom 6. september 1978, avsnitt 38 og 41, og Campbell mot Storbritannia, saksnummer 13590/88, dom 25. mars 1992, avsnitt 33. At bruken av telefontjenester er omfattet av artikkel 8 er klart, se bl.a. Craxi mot Italia, saksnummer 25337/94, dom 17. juli 2003, avsnitt 57. I dom 3. april 2007 i saken Copland mot Storbritannia, saksnummer 62617/00, bekreftet EMD at retten til privatliv også omfatter vern mot innsyn i e-post som sendes fra kontoradresse og personlig internettbruk (avsnitt 41).

Direktivet er basert på den forutsetning at lagringsplikten som sådan er forenlig med EMK artikkel 8, særlig basert på erfaringer fra flere medlemsstater som viser at tiltaket er nødvendig for å bekjempe organisert kriminalitet og terrorisme, se fortalens punkt 9.

Myndighetenes tilgang til lagrede trafikkdata må i tillegg vurderes for seg som et inngrep i forhold til den individuelle retten til privatliv som er nedfelt i EMK artikkel 8, og dermed kan slik tilgang bare være legitim så langt det er fastsatt i lov og det konkret er nødvendig og forholdsmessig for å ivareta et av de formål som er angitt i artikkel 8 (2). Direktivet overlater til medlemsstatene selv å fastsette nødvendige regler for tilgang til data, men utøvelsen av denne nasjonale kompetansen må skje innen de rammer som EMK artikkel 8 oppstiller, se direktivets fortale, punkt 25.

FNs konvensjon om sivile og politiske rettigheter oppstiller i artikkel 17 et vern om retten til privatliv som pålegger forpliktelser som langt på vei er sammenfallende med EMK artikkel 8, se nærmere "General Comment" nr. 16 (1988) fra FNs menneskerettskomité, som også understreker statens ansvar for å treffe effektive tiltak for å hindre at borgerne krenker hverandres privatliv (avsnitt 1 og 9), og faktaark nr. 32 fra FNs Høykommissær for menneskerettigheter, s. 45-46. Barnekonvensjonens artikkel 16 har en tilsvarende bestemmelse om vern mot krenkelse av privatlivet, og innebærer at barn er gitt en individuell rett til beskyttelse mot krenkelser, bl.a. via digitale medier.

Plikten til å lagre trafikkdata og betingelsene for myndighetenes tilgang til lagrede data må derfor vurderes hver for seg i forhold til kriteriene i artikkel 8 (2) om at inngrep må være nødvendige i et demokratisk samfunn for å ivareta ett av de oppregnede formål. Særlig relevant her er hensynet til kriminalitetsbekjempelse og til å ivareta andres friheter og rettigheter.

Kriminalitetsbekjempelse

Direktivet knytter denne nødvendighetsvurderingen opp til behovet for å forebygge, etterforske, avdekke og strafforfølge kriminelle handlinger, særlig organisert kriminalitet og terrorisme (fortalens punkt 7 og 8). Tilgang til trafikkdata har vist seg nødvendig og effektivt for dette formål i flere medlemsstater (fortalens punkt 9).

Sammenhengen mellom informasjonsteknologi og terrorisme og annen alvorlig kriminalitet er understreket i en rekke internasjonale fora. FNs generalforsamling har i resolusjon 55/63 av 22. januar 2001 uttrykt bekymring for at den teknologiske utvikling har skapt nye muligheter for kriminell atferd, særlig kriminell utnyttelse av informasjonsteknologi, og anbefalt at: *"Legal systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations,"* (punkt 1 f). FNs Sikkerhetsråd har ved flere anledninger uttrykt bekymring for at terrornettverk utnytter ulike media, inkludert internett, for å spre propaganda og oppfordre til terrorangrep (resolusjon 1617 (2005)), og besluttet at forpliktelsen til å fryse økonomiske midler "*apply to financial and economic resources of every kind, including but not limited to those used for the provision of Internet hosting or related services, used for the support of Al-Qaida, Usama bin Laden and the Taliban and other individuals, groups, undertakings, or entities associated with them*" (resolusjon 1822 (2008), operativ paragraf 4). Se også beslutning av ministerrådet i OSSE, nr. 7/06, 5. desember 2006 – "*Countering the Use of the Internet for Terrorist Purposes*" og artikkel 5 i Europarådets konvensjon av 16. mai 2005 om forebygging av terrorisme, som kriminaliserer handling med siktemål "å spre eller på annen måte gjøre tilgjengelig for offentligheten et budskap i den hensikt å tilskynde en terrorhandling" – jf St.prp. nr. 50 (2008-2009).

Tilgang til trafikkdata kan også ha betydning for effektiviteten av det justispolitiske samarbeidet mellom nasjonale politi- og påtalemyndigheter.

Med hensyn til kriminalitet som begås ved bruk av et datasystem er trafikkdata omfattet av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi, jf bl.a. artikkel 16 og 17 om bevaring av lagrede data, inkludert trafikkdata, og artikkel 20 om sanntids tilgang til trafikkdata. En tilleggsprotokoll til konvensjonen vedtatt i 2003 beskytter mot hatefulle ytringer, rasisme og fremmedfrykt.

Konvensjonen om gjensidig hjelp i straffesaker mellom Den europeiske unions medlemsstater av 29. mai 2000 gir i artikkel 18 en bestemmelse om umiddelbar overføring av telekommunikasjon som i tillegg til kommunikasjonskontroll også omfatter uttak av trafikkdata. Norge har undertegnet en avtale om tilknytning til EUs konvensjon og en tilhørende protokoll, og Justisdepartementet har sendt et forslag til lovmessig gjennomføring av konvensjonen m.m. i norsk rett på høring.

Utenriksdepartementet anser på denne bakgrunn at direktivet ut fra sin egen begrunnelse må vurderes i forhold til en felles europeisk trusselvurdering, hvor oppfatning av nødvendighet og proporsjonalitet ikke kan ses som et rent nasjonalt anliggende, løsrevet fra en felles erfaringsbakgrunn. Videre anses tilgang til trafikkdata å utgjøre et element i det felles europeiske politi- og strafferettslige samarbeidet, hvor forutsetningen er at rettshåndhevende myndigheter i ett land skal ha mulighet til å innhente relevant etterforskningsmateriale fra samarbeidende land, særlig for å kunne bekjempe terrorisme og alvorlig grenseoverskridende kriminalitet. Dersom Norge avskjærer muligheten for å benytte spor fra elektronisk kommunikasjon i etterforskningen av alvorlig kriminalitet, vil det derfor kunne ha betydning for mulighetene til etterforskning også for rettshåndhevende myndigheter i samarbeidende land, i den grad det viser seg å være behov for å søke elektroniske spor hos en tjenestetilbyder i Norge.

Beskytte andres rettigheter og friheter

Spørsmålet om plikten til datalagring er nødvendig og forholdsmessig må også vurderes i lys av statens forpliktelse til å verne individer mot krenkelse av retten til privatliv utført av andre, slik denne er nedfelt i artikkel 17 i FNs konvensjon om sivile og politiske rettigheter, artikkel 16 i barnekonvensjonen og praksis i relasjon til EMK artikkel 8. Den positive forpliktelsen til å beskytte retten til privatliv er ikke begrenset til spørsmål om kriminalisering og strafforfølging. Også andre egnede tiltak for å motvirke overgrep via digitale medier kan være aktuelle.

Krenkelser av retten til privatliv kan finne sted gjennom aggressive og krenkende handlinger utført via internett, mobiltelefon eller e-post. Overgripere kan benytte nettsamfunn som Facebook, YouTube og MySpace, og misbruk av datasystemer kan

generelt være knyttet til aktiviteter som botnets, phishing, pharming, spam, identitetstyveri og spionvareprogrammer. De elektroniske mediene gjør det mulig for mobbere og andre overgripere å være anonyme. "Anonymiteten gjør det også vanskeligere å stoppe mobberne fordi man ikke vet hvem de er," se NOU 2009:1 Individ og integritet, s. 136.

Staten kan på denne måten ha en plikt til å kriminalisere krenkelser av retten til privatliv, se EMDs avgjørelse i saken X. og Y. mot Nederland, saksnummer 8978/80, dom 26. mars 1985, avsnitt 27. Statene har en viss skjønnsmargin i avveiningen mellom den positive forpliktelsen til ikke å gripe inn i retten til privatliv og den negative forpliktelsen til å hindre krenkelser utført av andre, se EMDs avgjørelse i Ovièdre mot Frankrike, saksnummer 42326/98, dom 13. februar 2003, avsnitt 40. Det er antatt at en felles oppfatning blant konvensjonsstatene om hvilke tiltak som anses legitime for å hindre krenkelser, vil ha betydning for denne grensedragningen, se *Harris, O'Boyle and Warbrick, Law of the European Convention on Human Rights,* Oxford 2009, s. 384-5 og EMDs avgjørelse i Christine Goodwin mot Storbritannia, saksnummer 28957/95, dom 11. juli 2002, avsnitt 85, hvor det ble lagt vekt på *"a common European approach"*.

I relasjon til barnekonvensjonens artikkel 16 er det stilt spørsmål om manglende straffereaksjoner på krenkelser av privatlivet leder til at barn reelt sett får en svak beskyttelse, se Karl Harald Søvig, "Barnets rettigheter på barnets premisser", utredning gjort på oppdrag fra Barne- og likestilingsdepartementet, Bergen 2009, s. 172.

Med hensyn til krenkelser av privatlivet som er strafferettslig vernet i norsk rett, og i andre tilfeller der det anses nødvendig å gripe inn for å verne retten til privatliv mot andres krenkelse, er det avgjørende for mulighetene til videre undersøkelser eller etterforskning å kunne avdekke identiteten til overgriperen. I EMDs avgjørelse i K.U. mot Finland, saksnummer 2872/02, dom 2. desember 2008, ble det konkret tatt stilling til denne avveiningen, og EMD uttalte bl.a. i avsnitt 49 at: *"Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others."* Domstolen slo videre fast at lovgivers oppgave er*"to provide the framework for reconciling the various claims which compete for protection in this context"*. I mangel av rettslig mulighet til å avveie hensyn til konfidensialitet mot hensynet til vern av den krenkedes rett etter EMK artikkel 8, ble konklusjonen at Finland hadde krenket den positive forpliktelsen i artikkel 8 til å sørge for et effektivt vern.

I den utstrekning det anses nødvendig å pålegge plikt til å lagre trafikkdata for å beskytte individers integritet og rett til privatliv i samsvar med menneskerettighetene, er dette et legitimt formål.

Proporsjonalitetsvurderingen i forhold til nasjonale bestemmelser om lagring og tilgang til trafikkdata

Det ligger et generelt påbud i kravet til nødvendighet og proporsjonalitet at et hvert inngrep må skje på måter som er så lite inngripende som mulig for å oppnå det legitime formål som ligger til grunn. I tillegg til at direktivet ikke gir tillatelse til at innholdet i telekommunikasjon lagres, skal trafikkdata lagres på en slik måte at disse ikke i seg selv kan røpe personopplysninger. Direktivets artikkel 9 forutsetter videre at det føres betryggende tilsyn med at vilkårene for lagring og beskyttelse av data etterleves. Lagringstiden må ikke settes lenger enn det som anses nødvendig. Faktisk tilgang til trafikkdata i etterforskningsøyemed må være omgitt av tilstrekkelige rettssikkerhetsgarantier, slik at den nødvendige avveiningen mellom rett til konfidensialitet og rett til beskyttelse mot andres krenkelser kan foretas og rettslig prøves i individuelle saker, jf EMDs konklusjon i K.U. mot Finland, referert ovenfor.

I valg av teknisk løsning for tilbyderes lagring av trafikkdata bør det legges vekt på, slik det er gjort i høringsnotatet, at dersom borgerne opplever at deres kommunikasjon ikke er tilstrekkelig vernet, kan dette få negative konsekvenser for den frie meningsdannelse, som er grunnleggende i et demokrati (s. 41). I EMDs avgjørelse i S. og Marper mot Storbritannia, referert ovenfor, ble det understreket at "*an individual's concern about the possible future use of private information retained by the authorities is legitimate and relevant to a determination of the issue of whether there has been an interference,"* (avsnitt 71). Selv om trafikkdata i følge direktivet skal slettes etter en periode som ikke kan overstige 24 måneder, kan en slik mulig bekymring være relevant i forhold til mulige nye tilgangsbestemmelser eller bruksmåter for trafikkdata som lagres i fremtiden. Det bør derfor velges en løsning for lagring av trafikkdata som er best egnet til å skape den nødvendige tillit blant brukerne av telekommunikasjonstjenester.

Med hilsen

Kjell Kristian Egge
Avdelingsdirektør

Maren Edvardsen
Seniorkonsulent