

Institutt for informatikk

Postboks 1080 Blindern
0316 Oslo

Telefon: 22 85 24 10

Telefaks: 22 85 24 01

Dato: 14. april 2010

Nettadresse: www.ifi.uio.no

Høringsuttalelse om Datalagringsdirektivet

Det vises til høringsbrev fra Samferdselsdepartementet av 8. januar 2010 med tilhørende høringsnotat utarbeidet av Samferdselsdepartementet, Justisdepartementet og Fornyings-, administrasjons- og kirkedepartementet i fellesskap. Høringsnotatet gjør rede for de lovendringer som regjeringen mener er nødvendige eller ønskelige dersom datalagringsdirektivet innlemmes i EØS-avtalen, og det bes om høringsinstansenes synspunkter på disse.

Her følger kommentarer fra Institutt for informatikk (Ifi) ved Universitet i Oslo.

Sammendrag

EUs datalagringsdirektiv er en regulering som griper inn i livet til hver enkelt borger ved å redusere verdien av privatliv og integritetsvern, svekker pressens kildevern og svekker yringsfriheten.

Påstanden om at direktivet vil bistå politiet i arbeidet med bekjempe alvorlig kriminalitet er ikke tilfredsstillende dokumentert, og en del av den dokumentasjonen som er lagt fram i høringsnotatet ser ut til å bygge på svikende grunnlag.

Direktivet vil koste fellesskapet mange millioner kroner. Dersom det er ønskelig å bruke ressurser av et slikt omfang til å styrke politiets arbeide med kriminalitetsbekjempelse kan disse pengene etter Ifis oppfatning gi større uttelling ved å styrke politiets datasystemer slik at disse er bedre tilrettelagt for systematisering og søk i de opplysningene politiet allerede i dag har tilgang til, men som de ikke alltid mestrer å utnytte godt nok.

Ifi fraråder derfor at datalagringsdirektivet innlemmes i EØS-avtalen, eller på annen måte tas inn i norsk rett.

Omfanget av direktivet

Høringsnotatet gjør rede for hva slags kommunikasjonsformer og hva slags abonnements-, lokasjons og trafikkdata som omfattes av direktivet (i det etterfølgende bruker vi «trafikkdata» om alle disse tre typene data som omfattes av direktivet).

Høringsnotatet fortier imidlertid at det finnes en rekke elektroniske kommunikasjonsformer som *ikke* omfattes av direktivet. Årsaken til at disse ikke omfattes ser ut til å ha praktiske årsaker (kommunikasjonsformene genererer ikke trafikkdata som kan lagres, eller kommunikasjonen skjer på måter som gjør trafikkdata utilgjengelig for lagring, eller trafikkdata har lav politimessig verdi fordi de ikke identifiserer de som kommuniserer). Blant slike kommunikasjonsformer finnes blant annet (listen er ikke utdømmende):

- De fleste former for bredbåndstelefonti/VoIP (Skype et al) som leveres av andre tilbydere enn brukerens primære telekom-leverandør.
- Anonyme mobilabonnementer kjøpt fra utenlandske tilbydere.
- Ulike former for gratis web-baserte epost-tjenester som skjer fra tjenesteleverandører i utlandet og som ikke krever noen form for identifisering av brukeren (eks. Gmail).
- Ulike former for direktemeldings- og chattetjenester over Internett (eks. IRC). I tillegg til dedikerte chattetjenester har nesten alle online-spill en privat chattemodus som kan benyttes dersom man ønsker å kommunisere uten at trafikkdata om kommunikasjonen blir lagret.
- Private meldinger og direktemeldinger på ymse elektroniske oppslagstavler og sosiale nettstedet (eks.: Twitter, Facebook, Orkut, Biip).
- Diverse tjenester som benyttes via ulike former for anonymiseringstjenester, inklusive TOR, VPN, og Proxyer.
- Offentlige Internett-terminaler på biblioteker, bydelshus og Internett-kafeer.
- Åpne trådløse nett (disse finnes det for øyeblikket flere tusen av, bare i Oslo).

Etter vår mening vil det være sannsynlig at profesjonelle kriminelle, dersom lagringsdirektivet blir innført, rimelig raskt vil tilpasse seg den omstendighet at trafikkdata knyttet til bruk av epost, fasttelefoni, mobiltelefoni og internetttoppkoblinger vil bli lagret, og derfor velge å benytte seg av *alternative* elektroniske eller fysiske kommunikasjonskanaler der data *ikke* blir lagret. Som en følge av dette er det likeledes sannsynlig at formålet med direktivet (bekjempelse av alvorlig kriminalitet) ikke vil bli oppnådd. De som i første rekke vil bli «fanget opp» av den lagringen som vil skje i henhold til direktivet er alle ikke-kriminelle som benytter seg av internett og telefon i hverdagen, og evt. noen få svært inkompetente kriminelle.

Vi ser allerede eksempler på at slik kunnskap er i ferd med å spre seg. Den 7. januar 2010 ble det for eksempel lagt ut på Internett alvorlige trusler mot Kongsbakken videregående skole i Tromsø. Politiet etterforsket saken, men har nå lagt den til side med følgende begrunnelse:

*Etterforskningen har blant annet brakt på det rene at det er benyttet avanserte metoder for å skjule dataspør på nettet, og det har ikke vært mulig å spore trusselen til en konkret datamaskin.
(Pressemelding fra politiet, 2010-02-25)*

Det er overveiende sannsynlig at trusselen ble framsatt av mindreårige elever med tilknytning til skolen. Behersker skoleelever teknikker som gjør at de kan skjule sine elektroniske spor for politiet, er det ikke usannsynlig at profesjonelle kriminelle kan skaffe seg de samme kunnskapene.

Trafikkdata som bevis

I høringsnotatet hevdes det at trafikkdata har vært eller kunne vært «viktige bevis» i en rekke større kriminalsaker. Rent spesifikt nevnes Finance Credit-saken, Baneheia-saken, «Operasjon ENEA» og NOKAS-saken (ss. 39-41).

Det er uklart hva slags trafikk-bevis det kunne vært snakk om i Finance Credit-saken. Saken dreier seg om svindel gjennomført mot flere banker ved hjelp av forfalskede regnskaper og andre dokumenter. *Innholdet* i disse dokumentene var helt sentrale bevis i saken, og ble funnet hos bankene og hos de skyldige. Det er ikke umiddelbart klart hva lagrede trafikkdata kunne tilført denne saken i form av bevis, utover innholdet i de dokumentene som ble beslagnaglagt hos de tiltalte i henhold til gjeldende rett, og som altså ledet fram til en fellende dom.

I høringsnotatet hevdes det at trafikkdata var et «viktig bevis» i Baneheia-saken (s. 41). Dette er etter vår oppfatning å snu saken på hodet. Tvert i mot kan det argumenteres for at trafikkdata tilsynelatende ga hovedtiltalte alibi, jf.:

Telenor Mobil har i all hemmelighet gjennomført nye tester av mobildekningen i Baneheia. Målingene konkluderer på nytt med at det er umulig å ringe fra drapsstedet via basestasjonen Eg A. [VK] skal på drapstidspunktet ha sendt tekstmeldinger via denne basestasjonen.

- Vi har ikke klart å gjenskape en slik situasjon, sier dekningsdirektør Bjørn Amundsen i Telenor Mobil. (Dagbladet 2001-12-09, s. 11)

Mens basestasjonen Eg A altså ikke dekker Baneheia, dekker den området rundt tiltaltes hjem, som er der tiltalte ifølge egen forklaring oppholdt seg på det tidspunktet drapene skjedde.

Heller ikke firmaet Teleplan, som av retten var oppnevnt som sakkyndig, klarte noensinne å oppnå mobildekning fra basestasjon Eg A på Baneheia. Teleplan konkluderte imidlertid med at nevnte trafikkdata var usikre og derfor ikke kunne gi tiltalte alibi, jf.:

Fram til ankesaken tidligere i år, ble firmaet Teleplan oppnevnt som uavhengig rettsoppnevnte sakkyndige i mobilspørsmålet. Deres konklusjon var at det var umulig å si noe sikkert om dekningsgraden for basestasjonen den aktuelle drapsdagen, 19. mai 2000. (Adresseavisen 2002-09-14, s. 12)

Det skal ut fra dette godt gjøres å tolke overstående dit hen at trafikkdata fra tiltaltes mobiltelefonbruk var et «viktig bevis».

«Operasjon ENEA» var en større koordinert aksjon som politiet i Norge og Danmark i 2004 gjennomførte mot fildelingsnettverket Kazaa. I et fildelingsnettverk eksponerer de som deltar i nettverket sin IP-adresse. Politiet overvåket nettverket i tre døgn. Filene som ble utvekslet, ble automatisk sammenliknet med for politiet kjente bilder som viser overgrep mot barn. Totalt 850 000 bilder ble brukt som referansedatabase for operasjonen. På den måten identifiserte politiet IP-adressene til de som utvekslet overgrepsbilder som befant seg i politiets referansedatabase. Ved å koble disse IP-adressene med trafikkdata hos Internett-tilbydernes abonnementsregister kunne politiet identifisere hvilke datamaskiner og abonnementer som utvekslet overgrepsbilder. I Norge ble det i etterkant av aksjonen aksjonert mot ca. 250 abonnenter, noe som resulterte i 253 straffesaker, med 149 domfellelser og flere forelegg. Det er ingen tvil om at «Operasjon ENEA» var en viktig og vellykket politiaksjon mot de som utveksler overgrepsbilder på Internett.

Vi mener imidlertid at det ikke er korrekt å anføre denne aksjonen som begrunnelse for å innføre langtidslagring av trafikkdata. Politiet overvåket nettverket i sann tid, og hadde dermed løpende oversikt over de relevante IP-adresser. I dag lagrer Internett-tilbyderne de data politiet er interessert i i tre uker. Det burde være tilstrekkelig med tid for politiet til å rette henvendelse til tilbyderne for å sikre bevis. Dersom politiet har behov for mer enn tre uker for å analysere materialet har straffeprosessloven flere bestemmelser (jf. §§ 203, 210 og 216b) som gir politiet fullmakter til å sikre de nødvendige bevis. I høringsnotatet hevdes det (s. 39), på bakgrunn av den lange etterforskningstiden i ENEA-saken at «Politiet erfarer i dag at de ikke får tilgang på nødvendige data fordi disse rettmessig er slettet av tilbyderne.» Dette kan ikke være riktig. I den utstrekning politiet hadde behov for data i ENEA-saken som rettmessig var slettet må politiet selv bære ansvar for at de ikke utviste den nødvendige aktivitet for å sikre disse bevisene i tidsvinduet på tre uker etter at overvåkingen fant sted. Den omstendighet at politiet i en konkret sak valgte ikke å benytte seg av de rettsmidler de hadde til rådighet, kan ikke være et argument for å innføre en ordning med generell langtidslagring av data.

I NOKAS-saken i 2004 var de impliserte seg bevisst at politiet benyttet trafikkdata fra mobiltelefoner for å kartlegge bevegelsesmønstre. I følge boka «Dødsranet» (Hans Petter Aass og

Rolf J. Widerøe, Gyldendal 2009) la derfor ranerne mobiltelefonene sine igjen i Oslo, slik at de ikke skulle kunne knyttes til Stavanger ved hjelp av lokasjonsdata. Ranerne var imidlertid ikke klar over at politiet også benytter trafikkdata til å kartlegge sosiale nettverk. Ved hjelp av trafikkdata fra Telenor og Netcom var således politiet i stand til å kartlegge hvilke personer i ransmiljøet som sto i hyppig forbindelse med hverandre i forkant av ranet, og på den måten å peke ut de mest sannsynlige mistenkte.

Det er ingen tvil om at politiets bruk av trafikkdata til å kartlegge kommunikasjonsmønstre i ransmiljøet var viktig for oppklaringen av NOKAS-ranet og opprullingen av det sentrale ransmiljøet på Østlandet. Det er imidlertid mer tvilsomt om dette vil fungere like godt i fremtiden. Som eksemplet fra NOKAS viser, har også profesjonelle kriminelle evne til å lære. På samme måte som NOKAS-ranerne hadde lært seg om politiets bruk av lokasjonsdata for å kartlegge bevegelser, vil etter alt å dømme kriminelle med «lærdommen» fra NOKAS-saken avholde seg fra å avsløre forbindelser seg imellom gjennom å bruke kommunikasjonskanaler som kan analyseres av politiet på denne måten. I fremtiden vil profesjonelle kriminelle derfor tilpasse seg ved å kommunisere på måter som ikke er sporbare på denne måten.

I diverse presseoppslag har Kripas fremhevet et annet aspekt ved NOKAS-saken. I Aftenpostens nettutgave 18. mars er det et oppslag der man under tittelen «Uten datalagring blir Norge kriminell frihavn» der det blant annet står følgende:

Ifølge Kripas var pågripelsen av David Toska et direkte resultat av at IP-adressene for hans epost-bruk ble identifisert og sporet.

Vi må anta at dette er korrekt. Toska var som kjent på rømmen i Spania, og brukte diverse internett-kaféer for å kommunisere med medsamsvorne som politiet hadde under mistanke og som derfor var underlagt kommunikasjonskontroll.

Kommunikasjonskontroll er noe som politiet i dag har rett til å bruke mot personer det er skjellig grunn til å mistenke for en forbrytelse: Det har altså ingen verdens ting med Datalagringsdirektivet å gjøre. IP-adressene til Toska ble altså snappet opp i sann tid gjennom kommunikasjonskontroll, og vi antar at den også i tilnærmet sann tid ble sporet, med bistand fra den spanske ISP'en til den kafeen der Toska satt og emailen, og der man hadde et team klar til å pågripe ham.

Dersom man skal tillegge pågripelsen av Toska vekt i debatten om Datalagringsdirektivet, så er det åpenbart at den omstendighet at Toska ble pågrepet på den måten han ble er et argument for at politiet allerede i dag, gjennom lovens bestemmelser om kommunikasjonskontroll, har tilgang til de data de trenger for å samle inn de elektroniske spor de har behov for i denne typen saker.

Sammenlignet med de virkemidlene politiet *allerede* rår over, er det ingen ting som tilsier at effekten av den foreslåtte lagring mht. kriminalitetsbekjempelse vil være noe annet enn marginal. Samtidig vet vi at kostnadene for samfunnet vil være på flere millioner. Dermed må det stilles spørsmål om forventet nytteverdi ved lagring rettferdiggjør kostnadene for samfunnet. Vi mener at samfunnet hadde fått bedre uttelling i forhold til kriminalitetsbekjempelse dersom de samme pengene hadde vært brukt på å ruste opp politiets evne til å systematisere, samordne og søke i de spor de allerede samler inn. Med «Lommemann-saken» som den mest kjente, har det kommet fram at flere alvorlige kriminalsaker kunne ha blitt oppklart raskere dersom politiet hadde hatt tilgang til mer effektive dataverktøy for å systematisere spor.

Personvernkommissjonen etterlyste flere steder i sin sluttrapport (ss. 24, 70, 222) en grundigere klargjøring i form av dokumentasjon av behovet for lagring, og viste i den sammenheng til dokumentasjonskravet om nødvendigheten av inngrepet som følger av artikkel 8 i EMK.

Ifi konstaterer at det i høringsnotatet ikke gjøres noe seriøst forsøk på å svare på Personvernkommissjonen spørsmål, ut over rent anekdotiske referanser til fire kriminalsaker. Etter vår mening er

tre av de fire saker som trekkes fram misvisende referert. Således bekrefter høringsnotatet Personvernkommissjonens inntrykk av at nødvendigheten av datalagring for kriminalitetsbekjempelse *ikke* er tilstrekkelig dokumentert til å oppfylle EMK art. 8.

Strategisk informasjonsanalyse

I høringsnotatet åpnes det opp for at politiet skal få tilgang til lagrede data dersom det finnes skjellig grunn til mistanke, selv om mistanken ikke kan knyttes til en konkret person (s. 48).

Dersom direktivet blir implementert i en slik versjon, innebærer dette i praksis at man i Norge åpner opp for å gjøre de lagrede data tilgjengelig for såkalt «strategisk informasjonsanalyse» (*data mining*). Dette er en teknikk der man analyserer store mengder data med sikte på å finne mønstre som kan identifisere mulige gjerningsmenn. Teknikken er ikke helt ukjent, for eksempel benytter politiet i dag en slik teknikk dersom en forbrytelse er begått på eller nær et sted der det skjer videoovervåkning. Politiet vil da gjerne gå gjennom tilgjengelige overvåkningsvideoer for å kartlegge hvilke personer som befant seg på eller nær åstedet.

Det er ingen tvil om at strategisk informasjonsanalyse kan være nyttig for politiet i arbeidet med å identifisere mulig mistenkte og oppklare en forbrytelse. Samtidig er dette en teknikk som ansees som svært inngripende i forhold til personvernet. Dette blant annet fordi den gjør samtlige som er registrert i datamaterialet gjenstand for etterforskning, og fordi det gir politiet tilgang til såkalt overskuddsinformasjon som kan angå andre forhold enn det som er under etterforskning. Høyesterett i flere saker (Rt-1990-1008 (355-90), HR-2007-1742-A - Rt-2007-1409) bekreftet at politiet har rett til å benytte seg av overskuddsinformasjon.

Vi mener at politiets analyse av overvåkningsvideoer befinner seg innenfor rammen av det som er forholdsmessig. Teknikken omfatter et lite antall personer (de som faktisk befant seg på eller nær åstedet på et bestemt tidspunkt), gir politiet tilgang til forholds lite sensitiv informasjon (hvem som befant seg på et offentlig sted på et bestemt tidspunkt), og gir samtidig politiet anledning til å identifisere mulige vitner og gjerningsmenn.

Når det gjelder å gi politiet adgang til strategisk informasjonsanalyse av trafikkdata er dette etter vår oppfatning *ikke* forholdsmessig. For det første ligger det i datalagringsdirektivets natur at all kommunikasjon mellom norske borgere registreres og lagres, og det er derfor mulig at data som gjelder for et svært stort antall personer blir underlagt analyse. For det andre gir teknikken politiet mulighet til å kartlegge personers sosiale nettverk, som etter vår oppfatning er forholdsvis sensitiv informasjon. For det tredje truer strategisk informasjonsanalyse pressens kildevern, ved at slik analyse av trafikkdata eller lokasjonsdata kan benyttes til å identifisere hvilke personer som har kommunisert med, eller befunnet seg i nærheten av, redaksjonslokaler og journalister. For det fjerde er faren for at uskyldige blir trukket inn i etterforskningen (såkalte «falske positive») ved bruk av denne teknikken forholdsvis stor. Det å være uskyldig mistenkt og etterforsket for en forbrytelse er en stor belastning for de som det måtte gjelde, og er altså et uforholdsmessig sterkt inngrep i den enkeltes integritet.

Norge bør på ingen måte åpne opp for politimessige metoder som øker befolkningens eksponering for dette.

Mer om forholdet til kildevernet

I høringsnotatet (s. 50ff) gjøres det et poeng ut av at kildevernet ikke svekkes ved innføring av direktivet. Dette medfører etter vår mening ikke riktighet. Kildevernet etter gjeldende rett innebærer at politiet ikke kan etterforske saker ved å gjøre ransaking eller beslag i presselokaler. Beslag av en journalists PC vil for eksempel kunne fortelle hvilken kilde som har gitt en journalist

informasjon om en bestemt sak ved bruk av epost. Et slikt beslag kan politiet i dag ikke gjøre pga. rettspraksis mht. kildevernet.

Denne retten uthules utvilsomt dersom man innfører bestemmelser som innebærer at politiet kan kartlegge hvem journalisten har kommunisert med, ved å hente ut trafikkdata om journalists epost-korrespondanse fra en teletilbyder. Dersom direktivet innføres i norsk lov må derfor kildevernet styrkes ved at det innføres bestemmelser som ikke bare beskytter redaksjonslokalene og journalisters utstyr mot beslag, men også mot utlevering av trafikkdata om kommunikasjon til og fra journalister og avisredaksjoner.

Direktivet i forhold til ytringsfriheten

I tillegg til at datalagringsdirektivet er ytterst problematisk sett fra et personvernperspektiv, mener Ifi at direktivet også er problematisk i forhold til ytringsfriheten.

Rent spesifikt mener vi at nytteverdien av lagring bør veies opp mot effekter på frimodighet, og at 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 trafikkdata og lokasjonsdata om alle dine kontakter og kommunikasjoner både i det virkelige rommet og på Internett blir registrert, og at disse kan gjøres gjenstand for politimessig etterforskning og analyse, kan være nok til å hemme borgere i utøvelsen av sine friheter til å samles, til å ytre seg, til å søke kontakt med andre individer, og til å søke opplysninger. Dette er helt grunnleggende rettigheter i et demokrati, som kommer til uttrykk både i norsk lovgivning og i Den europeiske menneskerettskonvensjon (EMK). Etter Ifis oppfatning vil innføring av direktivet utvilsomt svekke rettsnyttelsen hva angår privatliv og privat kommunikasjon, og vil dermed være et uforholdsmessig inngrep i ytringsfriheten.

Sikkerheten ved de data som lagres

Høringsnotatet berører bare summarisk hvordan de data som skal lagres skal sikres, og legger klare føringer på at dagens tekniske løsninger skal benyttes mer eller mindre uendret. Mye tyder imidlertid på at diverse organisasjoner som i dag lagrer data, ikke har fullgode mekanismer for sikring av trafikkdata mot uautorisert spredning.

Ifølge Teleplans analyse vil lagring, inklusive sikring, koste mellom 207 og 261 millioner NOK over en femårsperiode (s. 52). Så vidt vi kan forstå tar Teleplan i så fall ikke høyde for kostnader forbundet med *bedre* sikring av data enn det søm følger av minimumskravene. Telenor har ifølge Berit Svendsen vurdert kostnaden til å ligge på 250 millioner NOK pr år¹. Vi kan ikke gå inn på disse konkrete tallene, men mener at dersom data skal lagres, så må de sikres vesentlig bedre enn det ser ut til at Teleplan har lagt til grunn.

Ifi vil i den forbindelse vise til den såkalte Tele2-saken, hvor Tele2 våren og sommeren 2007 lot kredittopplysninger om et sekssifret antall personer tilflytte uvedkommende. En enda større skandale fant sted i Storbritannia høsten 2007, hvor to ukrypterte disketter med personopplysninger vedrørende alle familier i Storbritannia med barn under 16 år kom på avveie². Det øker utvilsomt risikoen for misbruk når man øker mengden med data som lagres, og når man forlenger tiden data skal lagres. Dette må kompenseres med at det fra myndighetens side settes krav til bedre sikring i form av kryptering og deponeringsmekanismer (eschrow) som hindrer at så vel teletilbyderen selv, som myndighetene, kan få tilgang til lagrede data før korrekt rettslig grunnlag for tilgang kan fremlegges. Det må også sikres at enhver tilgang som gis, avgrenses til kun de data det skal være

¹ <http://www.liberaleren.no/2008/03/13/referat-fra-horingen-om-datalagringsdirektivet/>

² Se: *Brown apologises for records loss*, BBC News, 21. november 2007, http://news.bbc.co.uk/2/hi/uk_news/politics/7104945.stm.

lovlig tilgang til, og det må etableres sikringer – tekniske og organisatoriske så vel som juridiske – mot at det lagrede materialet kan brukes til strategisk informasjonsanalyse eller andre former for generell informasjonssøking. I forhold til den tekniske siden vil dette innebære at det må utvikles helt nye, finmaskede systemer for tilgangskontroll og datasikring som, dersom de tekniske problemene knyttet til slik utvikling overhode lar seg løse, kommer til å koste langt mer i utvikling og drift enn de lagringsløsninger som benyttes i dag.

Direktivet i forhold til EMK

EMK artikkel 8 annet ledd åpner for at det kan gjøres inngrep i personvernet. For at et slikt inngrep skal være forsvarlig må det blant annet være nødvendig i et demokratisk samfunn. Dette berører i høringsnotatet på sidene 26-28. I høringsnotatet hevdes det at et slikt nødvendighetsprinsipp eksisterer, men uten at det gjøres noe seriøst forsøk på å argumentere for den påstanden.

I høringsnotatet underslås det dessuten at det etter praksis i Den Europeiske Menneskerettighetsdomstolens (EMD) framgår at «nødvendig» må tolkes strengt. EMD sier at det må være en «pressing social need» for å gripe inn i personvernet. Det holder ikke at det er hensiktsmessig, rimelig eller ønskelig. Vi mener at dette vilkåret på ingen måte er oppfylt. Dette blant annet fordi politiet allerede i dag gjennom blant annet straffeprosessloven har de fullmakter de trenger for å innhente og sikre bevis i saker der trafikkdata er viktige for kriminalitetsbekjempelse.

I tillegg til nødvendighetskravet følger det av EMDs praksis at inngrepet i personvernet som gjøres må være proporsjonalt i forhold til formålet som ønskes oppnådd. Proporsjonalitetsprinsippet drøftes ikke i høringsnotatet.

Den omfattende lagringsplikten som følger av direktivet bryter etter Ifis oppfatning både med nødvendighetsprinsippet og proporsjonalitetsprinsippet som følger av EMK art. 8.

Konklusjon

Ifi mener at en innføring av direktivet vil innebære sterke personvernulemper, og bryter med grunnleggende demokratiske rettigheter. På den annen side er nytteverdien av en innføring av direktivet i forhold til kriminalitetsbekjempelse ikke dokumentert. Ifi mener således at direktivet ikke er forenlig med EMK art. 8 og dermed heller ikke med menneskerettsloven § 2, og at Norge derfor ikke bør innføre datalagringsdirektivet.