Rapport fra seminaret om lagring av trafikkdata den 08. september 2006 i Oslo

Av Per Inge Østmoen, EFN

Arrangøren for dette møtet var Norsk Forening for Jus og EDB - NFJE.

Temaet for seminaret var EUs direktiv om lagring av trafikkdata, heretter kalt Datalagringsdirektivet eller bare Direktivet, Direktiv 2006/24EU som vedtatt av Europarådet den 21. februar 2006. Seminaret var ikke åpent, det var påmelding med deltakeravgift, og det var i alt 49 påmeldte deltakere. Seminaret hadde fire hovedinnledere og tre kommentatorer. De sistnevnte leverte sine kommentarer etter lunchpausen, hvoretter det hele ble avsluttet med en diskusjonsrunde ledet av Line Coll.

Innleder 1: Simon Watkin, UK Home Office

Watkin startet sitt foredrag med å beskrive to ulike kriminalsaker med bilder av i alt fire ikke utpreget sympatisk utseende gjerningsmenn, mens han fortalte om hvilke grusomme forbrytelser disse hadde gjort seg skyldig i. Etter beskrivelsene av grusomhetene ledsaget av fotografiene av de brutalt utseende mennene beskrev Watkin hvordan de aktuelle drapssakene hadde blitt oppklart ved hjelp av elektroniske spor, i begge tilfeller sporing av mobiltelefoner.

Watkins innlegg fremsto som et sammenhengende forsvar for at menneskers elektroniske trafikkdata skal lagres, selv om Watkin også bidro med en god del nyttig informasjon. En av de vesentlige opplysningene er at de største omkostningene forbundet med lagring av alle borgeres trafikkdata ikke er kostnadene forbundet med selve lagringen. De virkelig store, og i stor grad uforutsigbare kostnadene, kommer når denne informasjonen som er lagret om borgerne skal brukes og analyseres. Slike kostnader kommer til å være kontinuerlige, og de vil nødvendigvis måtte øke over tid dersom mengden av data øker. Dette både på grunn av selve mengden, og fordi også kvaliteten (relevansen) av slike data avtar sterkt over tid slik at det blir mer krevende å finne noe som er av nytteverdi. Å sortere, analysere og finne ut hvilke data som er viktige kommer alltid til å forbli kostnadskrevende.

Watkin fortalte hvor lenge de innsamlede trafikkdataene er tenkt lagret, og tidene er som følger:

- Telefoni: 12 måneder
- IP-logger: seks måneder
- E-postlogger: seks måneder

I september 2006 foreligger ingen krav i UK om at disse lagringstidene skal forlenges, i følge Watkin. Han medgikk likevel at det er de som ønsker en mye lengre lagringstid, og det ble heller ikke sagt noe om hva som skjer med elektroniske spor som sjekkes uten å kunne knyttes til noe konkret lovbrudd. Hvor lenge vil den som har kommet i søkelyset, bli værende i søkelyset? Det vet ingen, heller ikke de som har ønsket denne lagringen.

Et interessant tall som fremkom, var antallet forespørsler som det britiske politiet gjør pr. uke

for å få tak i lagrede trafikkdata. Dette antallet er mellom 6000 og 8000 pr. uke for hele Storbritannia. Verd å merke seg er at dette tallet angår forespørsler som er gjort angående alle typer kriminalitet og lovbrudd. Det er, på samme måte som i Norge, ingen nedre grense for hvor små lovbrudd som kan få politiet til å søke opplysninger om enkeltpersoners elektroniske kommunikasjon. Dette var altså situasjonen i september 2006, før langtidslagring av elektroniske trafikkdata er gjennomført i Storbritannia.

En annen interessant opplysning: Blant de forespørsler om elektroniske spor som kommer fra det britiske politiet, er det bare 14% som er forespørsler om data som er over 7-12 måneder gamle. Disse tallene ga en meget viktig informasjon, av to grunner. For det første illustrerer tallene at det alltid er nye data som er viktige i etterforskninger, for det annet ble det konkret sagt "7-12 måneder." Det er tross alt et stort sprang mellom 7 og 12 måneder. Hvor mange forespørsler gjaldt da elektroniske spor som skriver seg 12 måneder tilbake eller mer i tid? Det må da nødvendigvis være færre, trolig betydelig færre, enn 14%. Tatt i betraktning at nytteverdien reduseres over tid samtidig som omkostningene forbundet med å tråle gjennom slike elektroniske spor like nødvendig må øke over tid, bør det kunne stilles et stort og berettiget spørsmålstegn ved hensiktsmessigheten av trafikkdatalagring i lengre tid enn hva som er nødvendig for faktureringsformål – også ut fra de opplysninger Watkins selv la frem.

Watkin skisserte også tidsplanene for gjennomføringen av Datalagringsdirektivet i Storbritannia: Innen september 2007 for fasttelefon og mobiltelefoni, internett-data i mars 2009. Deretter sa han noe vel verd å merke seg: "Vi ønsker å samarbeide med telekommunikasjonsbransjen, ikke mot den." Watkin brukte uttrykket "å samarbeide direkte med teleselskapene," og fortalte at britiske myndigheter hadde regelmessige møter med representanter for teleselskapene. Et av temaene for disse samtalene var hvem som skal bære merkostnadene ved trafikkdatalagring og kanskje også søkning i disse dataene. Watkin sa det slik: "Britiske myndigheter mener at teleselskaper og internettleverandører bør kompenseres for merkostnadene."

Watkin understreket at den britiske regjeringen la stor vekt på hva han kalte "samarbeid" mellom internettleverandører/teleselskaper og politiet. Det var tydelig at de britiske myndigheter var oppsatt på å forhindre at telekombransjen skulle stille seg på sine kunders side, selv om denne strategien ikke ble åpenlyst erkjent. Her var det ikke vanskelig å få øye på strategien: Myndighetene inviterer til "samarbeid" med teleselskapene som nå blir pålagt å lagre dataene om sine kunders elektroniske kommunikasjon. Selskapene på sin side vet at de vil få et lovverk å forholde seg til, og når de da blir forespeilet at de økede omkostningene de påføres kan kompenseres av det offentlige er det lettere for dem å bli samarbeidsvillige. Her sitter myndighetene med alle kort på hånden, og det er åpenbart at denne strategien er beregnet på å få teleselskapene til å akseptere trafikkdatalagringen – og ikke minst forhindre allianser mellom teleselskapene og deres kunder som slett ikke har noen grunn til å ønske trafikkdatalagringen velkommen. Ved at myndighetene tilbyr seg å dekke kostnadene, regner de med at teleselskapenes motstand skal fjernes fordi teleoperatørene og internettleverandørene vet at loven pålegger dem å gjennomføre tiltaket.

Bare en massiv protest fra store deler av befolkningen kan sette en stopper for lagringen av borgernes trafikkdata. I fravær av våkne borgere har kontrollivrige myndigheter lett spill.

Innleder 2: Inger Marie Sunde

Sundes foredrag hadde tittelen "Relationship of Directive to Council of Europe Cybercrime

Convention."

Sunde startet foredraget med å si: "Data fra elektronisk kommunikasjon har blitt stadig viktigere (til etterforskningsformål). Dette på grunn av at kriminelle er stadig mer sofistikerte, og fordi det er vanskelig å få vanlige borgere til å vitne i kriminalsaker."

Sunde fortsatte med å understreke at Cybercrime Convention ikke gir noen som helst forpliktelser til å lagre kommunikasjonsdata. Dette er det "Data Retention Directive" - Datalagringsdirektivet – som gjør. Cybercrime Convention omhandler inntrengning i datasystemer, forfalskning/misbruk av passord, samt datamaskinrelaterte lovbrudd av alle typer inkludert brudd på opphavsrettslovgivning og barnepornografi. Videre gjorde hun det klart at politiet i dag kan etterspørre og få utlevert trafikkdata når som helst, mens innholdsdata krever rettslig avgjørelse. Her snakket Sunde mye om nødvendigheten av å få tilgang til slike trafikkdata fra telekommunikasjonsselskapene, og la til at "dette er ikke mulig uten at dataene eksisterer." Med andre ord: Slik er altså begrunnelsen for lagring av alle borgeres trafikk- og lokasjonsdata. Sunde fortsatte med å kritisere konseptet om at man skal kunne være anonym: "Jeg synes ikke det er noen holdbar grunn til at borgere skal kunne være anonyme for hverandre." Derimot aksepterte hun at det eksisterte et behov for anonymitet mellom stat og borger. Deretter kom Sunde med en rekke interessante politisk/filosofiske utsagn som det er verd å dvele ved:

"Gitt at vi ikke liker undertrykkende regimer, kan noen lov gjøre oss sikre mot at et undertrykkende regime oppstår?" Sunde besvarte sitt eget spørsmål med et klart "Nei," og fortsatte: "Hvis det skulle oppstå et slikt regime, så vil alle tilgjengelige metoder og all teknologi for overvåkning bli brukt. Teknologien er der. Hvis vi ønsker å styrke menneskerettene, hvis vi ønsker å styrke folks rettigheter, så må vi styrke demokratiet. Debatten om lagring av (elektroniske) trafikkdata har fjernet fokus fra de virkelig viktige temaene som frihet, likeverd, demokrati."

Disse momentene er meget viktige, og undertegnede ga etter foredraget Sunde ros for å fremheve disse tingene. Problemet er dessverre at Inger Marie Sunde, sitt tydelige engasjement til tross, helt overser den realitet at demokratiet ikke er en evigvarende vaksine mot undertrykkende regimer eller autoritære og udemokratiske tendenser som kan oppstå i ethvert samfunn. I motsetning til hva Sundes ord legger opp til, er det en meget farlig feiltakelse å tro at eksistensen av et demokrati er noen som helst forsikring mot at dette demokratiet forvitrer og ødelegges. Sunde har fullstendig rett i at folks rettigheter og demokratiet som politisk system kontinuerlig må styrkes hvis vi ønsker å beholde det. Men, Sunde synes ikke å ville forstå at dersom samfunnet i beste mening stadig øker kontrollnivået overfor sine borgere, vil resultatet bli en alvorlig økende ubalanse mellom borgerne og de myndigheter som skulle være borgernes tjenere. Det er feil og meget farlig å tro at fordi et samfunn sies å være "demokratisk," så er myndighetenes økende bruk av kontrollmekanismer av den grunn ingen trusel. Forholdet er jo at dersom demokratiet skal styrkes og opprettholdes, så er den viktigste faktoren i så måte å begrense myndighetenes makt over borgerne. Å gi makthaverne og statens maktapparat den kontrollmakt som ligger i å beslutte loggføring og langtidslagring av opplysningene om alle borgeres elektroniske kommunikasjoner, er et kontrolltiltak som i alvorlig grad vil øke makthavernes makt over samfunnets medlemmer. Hvis man ikke har mulighet til å bruke telefon, sende/motta e-post eller bevege seg på internett uten at ens bevegelser skal kunne spores i lang tid etterpå, så er dette en tilstand som står i meget sterk motstrid til den ideelle målsetning om å styrke demokratiet og forsvare folks rettigheter. Og da hjelper det dessverre ikke om hensikten og sinnelaget er aldri så godt.

En meget gammel erkjennelse hos politiske tenkere, er nettopp at statens makt overfor individet må begrenses – for at folkestyret og menneskers rettigheter skal kunne forsvares. Innsamling av opplysninger om samtlige borgeres bevegelser i "den elektroniske sfære" innebærer en dramatisk økning av statens makt over innbyggerne, og datalagringsdirektivet betyr at et tiltak som tidligere var reservert for tilfeller der noe kriminelt har skjedd, nå utvides til å omfatte også lovlydige borgere.

Innsamling av alle enkeltindividers bevegelser på denne måten er dermed noe fundamentalt nytt. Realitetsinnholdet i tiltaket kan derfor ikke feies vekk med henvisning til at det viktige er å styrke demokratiet, når forholdet er at en massiv innsamling av opplysninger om samtlige borgeres elektroniske bevegelser er uforenlig med det frie samfunnet.

Innelder 3: Doris Liebwald, Vienna Centre for Computers and Law (VCCL)

Liebwald fortalte først at gjeldende østerriksk lov sier at lagring av folks trafikkdata ikke er tillatt uten at der foreligger rettslig kjennelse. Angående Datalagringsdirektivet, karakteriserte Liebwald situasjonen på denne måten: "Det har ikke vært noen offentlig debatt, og folks bevissthet er svak." Deretter gikk hun over til å si mer om gode, eksisterende lover i Østerrike og Tyskland, lover som i utgangspunktet skjermer individet fra overvåkning fra myndighetenes side. Politiet kan bare få tilgang til elektroniske trafikk- og lokasjonsdata i disse landene ved en rettsavgjørelse. Liebwald fortalte at det er minimumskravene i Datalagringsdirektivet som i Tyskland vil bli oppfylt. Merkostnadene for tyske internett- og teleselskaper vil bli dekket av det offentlige.

Liebwald fortsatte med å beskrive diverse menneskerettighetsgruppers og borgerrettighetsorganisasjoners kamp mot Datalagringsdirektivet, og fortalte at Det tyske menneskerettighetsforum den 16. juni 2006 kom med følgende offisielle ytring: "Trafikkdatalagring bryter med fundamentale rettigheter og underminerer det frie samfunnet."

I Tyskland har det blitt opprettet en egen hjemmeside for kampen mot trafikkdatalagring:

http://initiative.stoppt-die-vorratsdatenspeicherung.de/

På den andre ytterligheten finner vi Bundestag-representanten Klaus-Uwe Benneter, som har sagt følgende: "Det er opp til hvert enkelt land å skape en balanse mellom beskyttelsen av kommunikasjon og beskyttelsen mot terrorisme." Det er denne misforståtte og overforenklende motsetningen det er så viktig å få bukt med: Det legges opp til at det er et motsetningsforhold mellom folks rett til privatliv (kommunikasjon, derunder elektronisk kommunikasjon, tilhører privatlivet) og samfunnets beskyttelse mot terrorisme. Problemet er at ingen noengang har sannsynliggjort at øket overvåkning beskytter mot terrorisme, dette er en påstand og et dogme som hele tiden gjentas av de som ut fra ulike motiver er tilhengere av å kontrollere folks elektroniske bevegelser.

Innleder 4: Steven Karanja

Karanja hadde egentlig ikke noe foredrag, men kom med oppsummeringer og problemstillinger til den etterfølgende diskusjonen. Karanja tok først opp en rekke praktiske spørsmål:

- Hvor alvorlige lovbrudd skal gi grunnlag for politiets etterspørsel etter trafikk- og lokasjonsdata?
- Hvor lenge skal det lagres? (Her står det hvert land fritt å øke lagringsperioden ut over hva som er bestemt sentralt, og vi kan forvente politisk press fra forskjellige hold for å få øket lagringstiden)

- Hva skal skje etter lagringstidens utløp? Skal trafikk- og lokasjonsdataene slettes automatisk, eller hvordan skal det skje?
- Hvem skal betale de ekstra kostnadene?

Deretter var det lunch.

Etter lunch var det duket for ytterligere bidrag fra tre aktører. Førstemann ut var Odd Martin Helleland fra det norske Post- og teletilsynet. Hans bidrag skulle vise seg å være spesielt interessante.

Helleland begynte med å beskrive de hovedhensyn som vil søkes ivaretatt når EU-rådets Datalagringsdirektiv skal gjennomføres i Norge:

- Hensynet til etterforskning og rettergang
- Hensynet til personvernet
- Hensynet til konkurransesituasjonen innenfor elektronisk kommunikasjon

Deretter stilte Helleland spørsmålet om lagring av trafikkdata er nytt i Norge. Han impliserte at svaret er "nei," og begrunnet dette med at trafikk- og lokasjonsdata i dag (september 2006) lagres i en periode på mellom 3-5 måneder for administrative formål og faktureringsformål.

Helleland nærmest bagatelliserte betydningen av den nye situasjonen som er oppstått når telekommunikasjonsselskapene nå skal pålegges lagring av kunders kommunikasjonsdata, og sa at det er opp til nasjonale myndigheter å fastlegge kriteriene for utleveringen av dataene. Det vil si hvilke forhold som skal utløse en forespørsel om utlevering av trafikk- og lokasjonsdata. Deretter understreket Helleland at politiet i dag hadde mulighet til å kreve utlevering av trafikkdata, og mente at det da var et problem dersom teleselskapet har slettet dataene.

Deretter gikk han over til å beskrive de praktiske problemstillingene knyttet til lagringen:

- Hvem skal lagre?
- Hva skal lagres?
- Hvor skal det lagres?
- Hvor lenge skal det lagres?
- Hvem skal ha tilgang til dataene?

De som skal lagre etter Direktivets påbud, er "tilbydere av tilgjengelige kommunikasjonstjenester eller -nett." Igjen syntes Helleland å bagatellisere lagringen, og forsøkte å ufarliggjøre den ved nok en gang å si at trafikkdata også i dag blir lagret. Her var det både forunderlig og foruroligende at en fremtredende representant for Post- og teletilsynet tilsynelatende ikke ønsker å se den fundamentale forskjellen på å lagre kundenes kommunikasjonsdata for administrasjons- og faktureringsformål, og å lagre dataene i den hensikt å gjøre dem tilgjengelig for politi og eventuelle andre etater som kunne tenkes å ha eller få interesse av tilgang til dem. At denne forskjellen også har en praktisk side, ble understreket da Helleland refererte til den pågående diskusjonen om trafikkdataene som viser den enkeltes elektroniske bevegelser skal lagres hos tjenesteleverandøren eller på et sentralt lagringssted. Her var ingenting avgjort, men bare det faktum at det i fullt alvor diskuteres å lagre hele befolkningens elektroniske trafikkdata på et sentralt sted burde få selv den mest blåøyde til å våkne opp og forstå at nå har kontrollviljen gått urovekkende langt. Helleland mente at selve lagringstiden i Norge sannsynligvis ville bli på mellom seks og 12 måneder, med referanse til Direktivets minimumstid på seks måneder.

Deretter kom Helleland med nok et interessant utsagn. Han mente at en lengre lagringstid enn den som praktiseres for faktureringsformål er viktig for etterforskning av kriminalitet over landegrensene, og henviste til internasjonalt politisamarbeid. I tillegg til at dette med tidsaspektet og selve behovet for data langt bak i tid er kontroversielt, blir Hellelands tidligere utsagn om at det er opp til nasjonale myndigheter å fastsette kriterier for utlevering langt mindre troverdig. Når alle borgernes trafikkdata skal lagres i den hensikt å være tilgjengelig for også internasjonalt politi, slik det her helt tydelig er snakk om, kan rimeligvis ikke hvert enkelt lands myndigheter være suverene med hensyn til hvilke kriterier som legges til grunn for utlevering av disse høyst private dataene.

Etter Helleland snakket den faglig usedvanlig dyktige Eric Ekern fra Telenor. Ekern markerte seg kraftig med stor teknisk innsikt og frapperende formuleringsevne paret med utpreget pedagogisk evne til å gjøre sitt budskap forståelig for forsamlingen. Ekern er teknisk ansvarlig for Telenor Nordic's tilpasning til Eus Datalagringsdirektiv.

Ekern åpnet sitt innlegg med å fastslå at selv om Direktivets krav vedrører lagring, så er det slik at de store praktiske utfordringene knytter seg til søk i og utlevering av disse dataene. Han fortalte så at Telenor i 2006 har seks personer som er spesifikt engasjert i å tilrettelegge og utlevere telekommunikasjonsdata for politiet. Ekern var opptatt av de økte kostnadene forbundet med lagringen. Han beskrev situasjonen slik at det er naivt å tro at teleoperatørene vil bære kostnadene forbundet med Datalagringsdirektivet. Enten må kundene betale høyere priser, eller myndighetene må gå inn med økonomisk støtte, mente ingeniør Ekern, og understreket at systemutvikling og systemtilpasninger til en trafikkdatalagring av alle borgeres data vil koste mye. Også tilrettelegging av rutiner for utlevering av data vil bli kostbart. For de nordiske landene antydet Ekern en initiell utgift på 50 millioner Euro. Deretter kommer naturligvis de påløpende kostnadene forbundet med å opprettholde et slikt system. Ekern argumenterte for at Norge burde legge seg på mininumsnivået for lagringstid.

Neste kommentator var Guro Slettemark fra Datatilsynet. Vi har tidligere registrert at Datatilsynet helhjertet og med prisverdig kunnskap og innsikt forsvarer borgernes rett til et privatliv. Slettemark fulgte opp denne gode tradisjonen med å gi uttrykk for sin bekymring

over Datalagringsdirektivet. Hun fortsatte med å beskrive de nåværende (2006) vilkårene for sletting av elektroniske trafikkdata, som typisk tilsier at de skal slettes etter tre eller fem måneder, avhengig av faktureringshyppighet. Deretter sa Slettemark: "Norge har fremdeles et valg. Vi trenger ikke å implementere dette direktivet." Hun poengterte at Datalagringsdirektivet innebærer at hele befolkningens bruk av telefon, e-post og internett logges og lagres. Med andre ord, det er ikke et tiltak som er målrettet mot kriminell aktivitet, men derimot rettet mot hele befolkningen. Slettemark konstaterte at generell trafikkdatalagring krenker den grunnleggende retten til fortrolig kommunikasjon. Videre fremhevet hun det betenkelige i at tilbydere av elektroniske kommunikasjonstjenester skal fungere som "politiets forlengede arm, det er faktisk dette de blir pålagt," sa Slettemark. Hun fortsatte i den samme saklige, nøkterne stil: "Jeg har problemer med å se behovet. Allerede i dag har politiet mulighet til kommunikasjonskontroll og til å beordre frysing av trafikkdata." Slettemark, som selv er jurist, antydet så at Data Retention Directive er "en type lovgivning som har til hensikt å gi en hjemmel i tilfelle det skulle bli behov for det," og hun mente at det er svært uheldig dersom lovgivningen utformes etter prinsippet om "i tilfelle."

Slettemarks synspunkt var at det ville være tilstrekkelig om mistenkte individers trafikkdata lagres. Angående trafikkdatalagring, pekte hun på at ved langtidslagring av slike data vil kvaliteten (relevansen) av dataene alltid og helt uunngåelig forringes over tid. Her hadde Guro Slettemark et svært vektig poeng. Til etterforskningsformål er det vesentlig at politiet har mest mulig ferske spor, og som allerede nevnt har bare en liten andel av de etterspurte kommunikasjonsdataene vært eldre enn et halvt år. Slettemark fortsatte: "Data som er lagret representerer en nesten uimotståelig fristelse for andre – hva blir det neste? Skal det til slutt sies at lagring av kommunikasjonsdata gjøres for å forebygge kriminalitet?" Hun fremhevet videre at trafikkdatalagring innebærer et paradigmeskifte i kriminalitetspolitikken: Tidligere har det vært slik at politiet bare samlet opplysninger om individer som var under konkret mistanke om noe kriminelt. Ved lagring av hele befolkningens elektroniske kommunikasjonsdata utsettes hele befolkningen for et etterforskningspreget tiltak. Slettemark stilte følgende tankevekkende spørsmål: "Er konsekvensen av dette at hele befolkningen er under mistanke?"

Avsluttende diskusjon

Etter Guro Slettemarks kommentar kom turen til den avsluttende runden med diskusjon, spørsmål og kommentarer fra salen. Diskusjonen ble som nevnt ledet av Line Coll, en tidligere praktiserende advokat som i 2006 arbeider som stipendiat ved Institutt for rettsinformatikk ved UiO. Coll deltok selv i samtalen, og markerte en stillingstagen til fordel for borgernes personvern. Hun slo fast at "Det foreligger en forventning om at kommunikasjon skal være privat." Coll mente at dersom en slik lagring av trafikkdata som Direktivet krever skal tillates, så må effekten på oppklaringsprosenten i kriminelle saker kunne dokumenteres. Noen slik dokumentasjon foreligger naturligvis ikke, så Colls poeng er et tungtveiende sådant. Coll advarte mot at den frie og demokratiske diskusjonen kan dempes hvis alles kommunikasjons skal kartlegges. Angående den praktiske nytten av lagrede trafikkdata, fokuserte Coll på at politiet i etterforskning av hverdagskriminalitet har liten eller ingen nytte av opplysninger som er eldre enn seks måneder. Coll antydet at lagring av borgernes trafikkdata innebar at prinsippet om uskyldspresumpsjon blir snudd til en presumpsjon av skyld. ("Omvendt uskyldspresumpsjon.") Dette må kunne kalles sterke ord når de kommer fra en person som har arbeidet som advokat.

Coll stilte et spørsmål, med adresse til Post- og teletilsynets Odd Martin Helleland, om hvorfor frysing av konkret mistenkte personers trafikkdata ikke kunne praktiseres i stedet for lagring av alle borgeres trafikkdata. Hellelands svar var oppsiktsvekkende: "Men det gjøres jo ikke!" Dette svaret var lite relevant i forhold til spørsmålet som ble stilt. Hvis mistenktes elektroniske trafikkdata i dag ikke spesifikt lagres, så skulle det være all grunn til å begynne å gjøre dette. Fremfor alt kan manglende rutiner med å fryse konkret mistenkte personers data umulig være noen holdbar begrunnelse for å lagre alle borgeres trafikkdata. Hva som var oppsiktsvekkende ved Hellelands opptreden under dette seminaret, er at Post- og Teletilsynet i utgangspunktet skal være en nøytral instans. Men både Odd Martin Helleland og en annen person fra samme sted viste til fulle at dette tilsynet langt i fra spiller noen nøytral rolle, men derimot har tatt et klart partsstandpunkt til fordel for lagring av samtlige borgeres trafikkdata. Det hadde vært av betydelig interesse å få vite hvorfor det norske Post- og teletilsynet har tatt det standpunktet.

Helleland henviste til en ikke nærmere definert bestemmelse i Straffeprosessloven som sier at en som er under etterforskning må underrettes om dette, noe som i følge Helleland vanskeliggjorde frysing av trafikkdata uten vedkommendes vitende. Line Coll repliserte imidlertid med at det da kanskje kunne være en tanke å se på bestemmelsene i Straffeprosessloven. Til det hadde Odd Martin Helleland intet svar. Dette viser at uavhengig av hva Straffeprosessloven sier, har Helleland og dermed Post- og teletilsynet inntatt et prinsipielt standpunkt om at trafikkdatalagring er ønskelig. Beklageligvis viste diskusjonen at motforestillinger ikke nådde frem, noe som var både foruroligende og høyst merkelig ettersom det dreier seg om et offentlig tilsyn som ikke burde ha interesser i noen retning. Helleland hevdet at langtidslagring av trafikkdata vil gi mulighet for oppklaringer av kriminalsaker. Men dette er ikke og kan ikke være et gyldig argument. Skal man argumentere på den måten, vil man i prinsippet kunne argumentere for et hvilket som helst tiltak som kan føre til oppklaringer eller som kan fremkalle tilståelser som ellers ikke ville kommet. Det ubehagelige spørsmålet som nå må stilles, er om man ved å lovfeste lagring av opplysningene om befolkningens elektroniske bevegelser går langt ut over hva som bør kunne aksepteres i et fritt samfunn.

Man hører ofte påstander om at i store og alvorlige kriminalsaker har politiet behov for å samle data over lengre tid. Det er bare det at til dette formålet er ikke lagring av alle borgeres trafikkdata nødvendig. I store og alvorlige kriminalsaker som etterforskes over lengre tid har man så godt som alltid mistenkte personer – og disse mistenkte personenes trafikkdata kan fryses dersom det har betydning for etterforskningen. Det vil i så fall være analogt med spaning i den "fysiske" verden, og bør følgelig ikke være mer kontroversielt enn konvensjonell spaning når konkrete straffbare forhold er avdekket. I store og alvorlige saker har politiet allerede de prosessuelle verktøyene som skal til for å kartlegge de mistenktes aktivitet. Hvor ligger da egentlig nytteverdien av å lagre alle borgeres trafikkdata? Politiet har først og fremst behov for ferske data når de etterforsker et lovbrudd. Enhver polititjenestemann eller -kvinne kan fortelle om den sentrale betydningen av ferske spor når en forbrytelse har skjedd. Det kan overhodet ikke dokumenteres at elektronisk trafikkdatalagring vil ha en effekt på oppklaringsprosenten i alvorlige kriminalsaker som tilnærmelsesvis kan forsvare et tiltak som innebærer at hele befolkningens bevegelser gjøres sporbare i lang ettertid.

En annen tilstedeværende (kvinnelig) representant for Post- og teletilsynet kom i løpet av spørsmålsrunden med en ytring som formidlet at "Hva er det man er redd for? Jeg har jo ingen grunn til å være motstander av lagring av trafikkdata, jeg er jo lovlydig." Slik argumentasjon er ikke overbevisende sterk når man går den nærmere etter i sømmene, selv om den kan være

forførende når man ikke tenker seg om. Tenker en seg om, ser man at utsagnet om at “den som har rent mel i posen har ikke noe å frykte” innebærer at virkeligheten dreies opp-ned. Det er nettopp den lovlydige borger, som ikke har gjort seg skyldig i kriminalitet, som bør ha et selvfølgelig krav på å ikke bli utsatt for et etterforskningspreget tiltak som lagring av alle borgeres trafikkdata innebærer. Som Guro Slettemark så korrekt pekte på, er dette en form for detaljert kartlegging av menneskers bevegelser som tidligere bare har vært godtatt og praktisert i kriminelle saker. I en hverdag hvor elektronisk kommunikasjon har fått stadig større betydning, betyr en kartlegging av alles elektroniske bevegelser et desto mer gjennomgripende og alvorlig inngrep i borgernes privatliv.

Undertegnede EFN-representant hadde også en sluttkommentar, som fremhevet at det enkelte individets telefoniske kommunikasjon, e-postutveksling og internettbruk tilhører privatlivet. Dersom ikke myndighetene og politiet respekterer dette, vil borgernes respekt for rettsstaten uthules litt etter litt, noe som er den på sikt alvorligste følgen av omfattende kontrolltiltak av denne typen. Det er vanskelig å komme bort fra at en lagring av alles kommunikasjonsdata bygger på den uuttalte forutsetning at "også du kan være en kriminell." En slik tilnærming overfor statens innbyggere burde være rettsstaten fremmed, og beklagelig nok ser det ikke ut til at de personer som ønsker å gjennomføre et kontrolltiltak med så vidtrekkende konsekvenser for individets privatliv har hatt vilje til å forutse de langsiktige følgene av de negative signaler de dermed sender til befolkningen.

Hvis vi skal være realistiske, bør vi dessuten være klar over at kriminelle vil være de første til å finne utveier for å unndra seg overvåkningen gjennom det altomfattende og derfor upresise kontrolltiltaket som Datalagringsdirektivet representerer. Dette må i særlig grad forventes å være tilfellet for de mest ressurssterke og derfor aller farligste og best organiserte kriminelle. Effektivt arbeide mot kriminalitet forutsetter målrettede virkemidler, hvilket er viktigere desto mer avansert kriminalitet det dreier seg om. Derfor kan man stille et enda større spørsmålstegn ved effektiviteten og hensiktsmessigheten. Guro Slettemarks ord om at Direktivet er en type lovgivning hvis formål er å gi en hjemmel for inngrep overfor borgerne “i tilfelle” fremstår etterhvert som ubehagelig treffsikre. I en rettsstat bør aldri en slik lovgivning aksepteres. Et etablert demokrati er ingen garanti mot at dette demokratiet ødelegges gjennom virkemidler som underminerer det frie samfunn. Tvert i mot, skal folkestyret overleve og bevare sin sunnhet er det en forutsetning at også fenomener som vi misliker, som skremmer oss, eller som er farlige møtes med virkemidler som aldri går over grensene for hva demokratiet tåler. Å kartlegge alle borgeres elektroniske og/eller fysiske bevegelser er, uavhengig av hvilken hensikt og hvilket sinnelag som ligger bak, et tiltak hvis virkning er å gi myndighetene en kontrollmakt over hvert individ som i alvorlig grad forrykker balansen mellom borgerne og deres representanter. Å lukke øynene for dette, er å lukke øynene for selve grunnforutsetningene for at demokratiet skal kunne opprettholdes. Den stat eller statsdannelse som ønsker å kartlegge og kontrollere stadig mer av sine borgeres handlinger og bevegelser, har kommet i skade for å adoptere et samfunnssyn som er karakteristisk for den tilstand av kontroll og ufrihet som finner sitt mest ekstreme uttrykk hos terrorister og andre alvorlig kriminelle.

Terroristenes og forbrytersyndikatenes idealsamfunn er slett ikke det åpne demokrati. Deres ideal er nettopp det gjennomkontrollerte samfunn hvor de som innehar maktposisjoner har muligheten til en størst mulig grad av oversikt over og kontroll av enkeltindividets bevegelser og disposisjoner. Hvis staten og myndighetene faller for fristelsen til å benytte udemokratiske virkemidler overfor befolkningen som fratar mennesker deres rett til privatliv, vil resultatet bli at man beveger seg i retning av å organisere staten på kriminelles premisser. Det er

vanskelig å tro at nettoresultatet vil bli mindre kriminalitet. Å gi avkall på rettsstatens hevdvunne prinsipper i troen på at man skal bli mer effektive i kriminalitetsbekjempelse, vil bekrefte de kriminelles verdensbilde og gradvis svekke normalbefolkningens tillit til rettsvesenet. De langsiktige følgene av et slikt scenario kan ikke overvurderes. Demokratiet kan aldri være noen vaksine mot undertrykkende tendenser, vil man forsvare demokratiet vil det til alle tider være nødvendig å forsvare borgernes og individets rett til størst mulig frihet fra kontroll fra makthavernes side. I et sosialt fellesskap er dette en frihet under ansvar. Den borger som sviker sitt ansvar gjennom å gjøre seg skyldig i destruktive handlinger, må naturligvis bli gjenstand for samfunnets inngripen. Men slik inngripen må kun skje mot individer som beviselig opptrer destruktivt, og tiltakene må alltid være spesifikke og rette seg mot de som påviselig har gjort seg skyldig i onde handlinger.

I et fritt samfunn som skal være demokratisk, må det dessuten aksepteres at det ikke kan finnes “endelige løsninger.” Man kan søke å skape et så godt fellesskap som mulig, men det må erkjennes at nullvisjoner er uforenlige med et demokratisk og fritt samfunn. Man kan aldri ha null kriminalitet. Man kan ikke fjerne alt som er vondt, vanskelig og farlig, man kan ikke ha null trafikkulykker, man kan ikke ha null skrubbsår på knærne.

Georg Apenes har sagt det slik i Datatilsynets Personvernrapport for 2005: “Det er en eiendommelighet i tiden at stadig flere synes å foretrekke en falsk og fiktiv trygghet, fremfor en reell, men oversiktlig utrygghet.”

Årsaken til at befolkningen i Europa i skrivende stund ennå ikke har reist seg i massiv protest mot kartleggingen av deres elektroniske bevegelser, er en ulykksalig kombinasjon av liten politisk interesse, et øredøvende og bedøvende trykk fra allestedsnærværende underholdningstilbud samt massemedienes dramatisering av triste og tragiske foreteelser som er en del av virkeligheten selv om de er en forholdsvis liten del av den. Disse faktorene fører til politisk passivitet og en trang hos mange mennesker til å søke trygghet. Omfattende kontrolltiltak fra myndighetenes side kan i en slik situasjon se ut som om de tilbyr trygghet, og politikere på sin side får en følelse av å "gjøre noe." De ovenfor nevnte mekanismene er forklarlige og forståelige, og vi har alle et medansvar for å gjøre noe med dem for å kunne påvirke i positiv retning. Utfordringen ligger i å få mennesker til å våkne og bli bevisste om at vi aldri kan bytte bort vår frihet for å oppnå trygghet, og at kontrollsamfunnets fiktive trygghet er langt mindre trygg enn det frie samfunnets reelle men (relativt) oversiktige utrygghet.

I et fritt samfunn har kartlegging og lagring av opplysningene om alle borgeres kommunikasjonshandlinger eller andre bevegelser ingen plass.

Per Inge Østmoen, 17. september 2006