



Elektronisk Forpost Norge

Pb. 2631 Solli
0203 Oslo

Samferdselsdepartementet
Postboks 8010 Dep
0030 Oslo

HØRINGSUTTAELSE - MULIG GJENNOMFØRING AV DATALAGRINGS DIREKTIVET (2006/24/EC) OM LAGRING AV DATA FREMKOMMET VED BRUK AV ELEKTRONISK KOMMUNIKASJON I NORSK LOVVERK.

Elektronisk Forpost Norge har mottatt høringsnotatet[1] om Datalagringsdirektivet fra Samferdselsdepartementet, Justis- og politidepartementet og Fornyings-, administrasjons- og kirke departementet og vil her komme med synspunkter og kommentarer til forslaget.

(Også sendt elektronisk til postmottak@sd.dep.no, postmottak@jd.dep.no og postmottak@fad.dep.no)

OVERSIKT OVER EFNS HØRINGSUTTAELSE

Del 1 av EFNs høringsuttalelse legger frem rammeverket og premisene vi bygger på, ved en gjennomgang av noen sentrale aspekter ved og innvendinger mot personvern-begrepet. Vi skisserer også noen historiske linjer i forhold til overvåkning/demokrati, frihet/kontroll og maktbalansen mellom individet og sivilsamfunnet på den ene side, og stat og myndigheter på den annen side.

Del 2 går gjennom en del konkrete sider ved og forutsigbare konsekvenser av Datalagringsdirektivet (DLD), og relaterer disse til rammeverket som ble lagt i del 1, dvs. betingelsene for å bevare og styrke rettsstaten, sivilsamfunnet og demokratiet.

Del 3 diskuterer viktigheten av målrettet etterforskning, kommunikasjonskontroll over mistenkte personer, viktigheten av å styrke politiets ressurs situasjon, og hvordan disse faktorene både kan erstatte og fungere mye bedre enn Datalagringsdirektivet, samtidig som de er mye billigere.

Del 4 påpeker at Datalagringsdirektivet ikke innfrir de oppgitte formål, og viser hvordan kriminelle lett kan omgå DLD.

Del 5 bygger videre på at DLD ikke innfrir sine formål, ved en gjennomgang av problemene forbundet med "falske positive" og uoverstigelig beregningskompleksitet.

Del 6 går gjennom hvordan DLD øker utryggheten i samfunnet - både for kildevernet og varslere spesielt, og for folk flest generelt.

Del 7 drøfter hvordan DLD kommer i konflikt med andre deler av lovverket og med rettsprinsipper som er grunnleggende i en rettsstat.

Del 8 gir en sammenfatning med utgangspunkt i tillit, kontroll og maktbalanse i samfunnet, og avsluttes med konklusjonen på EFNs høringsuttalelse.

INNHOLDSFORTEGNELSE

0.0 OVERSIKT OVER EENS HØRINGSUTTALELSE

1.0 INNLEDENDE BEMERKNINGER

1.1 HVA MENES MED "PERSONVERN"?

1.2 KRITIKK AV PERSONVERNET

1.3 STOREBROR OG STOREMOR

1.3.1 STORSTILT OG OMFATTENDE REGISTRERING

1.3.2 SAMFUNNETS SVAKESTE RAMMES ALLTID MEST AV ØKT KONTROLL

1.3.3 TILGANGSUTVIDELSER OG FORMÅLSGLIDNING

1.3.4 ALLE ER IDEOLOGISKE, INGEN ER VERDINØYTRALE

1.4 KONKLUSJON OM PERSONVERNBEGREPET

2.0 DATALAGRINGSDIREKTIVET OG "ALVORLIG KRIMINALITET"

2.1 KRITERIENE FOR UMLEVERING VIL ENDRES OG FORMÅLSGLI

2.1.1 UMLEVERING TIL UTLANDET AV OPPLYSNINGER OM STATENS INNBYGGERE

2.2 TRAFIKKDATALAGRING ER OVERVÅKNING

2.3 OVERVÅKNING AV WEB-BRUK

2.4 IKKE KRAV OM DOMSTOLSBEVLUTNING ELLER SKJELLIG GRUNN FOR UMLEVERING AV DATA

2.5 NOKAS OG BANEHEIA OPPKLART UTEN DLD

2.5.1 NOKAS

2.5.2 BANEHEIA

3.0 KOMMUNIKASJONSKONTROLL OG STYRKING AV POLITIET

3.1 MÅLRETTET ETTERFORSKNING OG MER RESSURSER

4.0 DATALAGRINGSDIREKTIVET INNERIR IKKE DE OPPGITTE FORMÅL

5.0 FALSKE POSITIVE OG KOMPLEKSITET VED DATABEREGNINGER

5.1 FALSKE POSITIVE

5.2 PLIKT TIL Å LEGGE FREM DOKUMENTASJON AV USKYLD

5.3 KONKLUSJON PÅ FALSKE POSITIVE OG DATABEREGNINGER

6.0 DATALAGRINGSDIREKTIVET GIR ØKT UTRYGGHET I SAMFUNNET

6.1 ALVORLIG TRUSSEL MOT KILDEVERNET OG VARSLERE I SAMFUNNET

6.2 DATA PÅ AVVEIE GIR ENDA MER UTRYGGHET

6.3 PRIVATISERING AV POLITIOPPGAVER

7.0 DLD I STRID MED ANNEN LOVGIVNING OG RETTSPRINSIPPER

7.1 GRUNNLOVEN

7.2 METODEUTVALGET OM DATAAVLESING

7.3 EMK OG DLD

7.4 USKYLDSPRESUMPSJONENS PRINSIPELLE OG PRAKTISKE RELEVANS

8.0 SAMMENFATNING OM TILLIT OG KONTROLL, MAKTBALANSENS BETYDNING, OG KONKLUSJONEN PÅ EFN SIN HØRINGSUTTALELSE

8.1 KONTROLLSAMFUNNETS NEDBRYTENDE SOSIALE EFFEKTER

8.2 HVORFOR ER MAKTBALANSEN SÅ VIKTIG?

8.3 KONKLUSJON

9.0 KILDEHENVISNINGER

10.0 FORFATTERE OG KREDITERING

1.0 INNLEDENDE BEMERKNINGER

EFN er av den oppfatning at spørsmålet om innarbeidelse av Datalagringsdirektivet i norsk rett er et både praktisk og prinsipielt spørsmål som bare kan behandles på forsvarlig vis ved at saken ses i lys av de følgene det vil få for samfunnet dersom et slikt invaderende inngrep i menneskers privatliv blir gjennomført. Derfor er det etter vårt syn av sekundær betydning hvordan et slikt direktiv skulle gjennomføres med hensyn til lagringstider, lagringsmåter, lagringssted og såkalte sikringsrutiner i forhold til prosedyrer og tekniske installasjoner som uansett heller aldri vil kunne sikres mot at data kommer på avveie.

EFN vil i det følgende legge vekt på en analyse av de personvernmessige konsekvensene av en tenkt gjennomføring av Datalagringsdirektivet veid opp mot andre hensyn. Her vil vi vektlegge de konklusjoner som etter vårt skjønn følger naturlig ut fra kjernen i de problemstillingene Datalagringsdirektivet (og for såvidt også andre tilsvarende eksisterende eller mulige kontrolltiltak overfor befolkningen) aksentuerer. Kjernen er selve den balansen mellom borgere og myndigheter som er en ufravikelig, om enn kanhende ikke alltid i like høy grad erkjent, forutsetning for rettsstaten og for demokratiet slik de fleste innbyggere i vårt land må antas å ønske at vår samfunnsform skal være. Forrykkes denne balansen i borgernes disfavør, ødelegges forutsetningene for et samfunn der innbyggerne har medbestemmelsesrett og trygghet mot overgrep. Denne samfunnsforståelsen er bestemmende for de resonnementer og standpunkter vi utvikler i dette dokumentet.

I Samferdselsdepartementets, Justisdepartementets og Fornyings-, administrasjons- og kirkedepartementets høringsbrev datert 08.01.2010[1] beskrives følgende situasjon: "Det fremgår av regjeringens politiske plattform at det ikke er enighet i regjeringen om at Datalagringsdirektivet skal innlemmes i EØS-avtalen: Arbeiderpartiet vil implementere Datalagringsdirektivet forutsatt at det i utredningen ikke fremkommer klare negative konsekvenser for personvernet. Sosialistisk Venstreparti og Senterpartiet vil av personvernmessige hensyn gå i mot implementering av EUs datalagringsdirektiv i norsk rett. SVs og SPs representanter stilles fritt i denne saken."

Situasjonsbeskrivelsen i ovenstående er verdt å merke seg. Ett av de i regjeringen deltagende partiene deklarerer på forhånd at de vil implementere Datalagringsdirektivet under forutsetning av at det ikke fremkommer klare negative konsekvenser for personvernet. Samtidig er de to andre nevnte partiene like sikre på at de sier nei, på grunn av følgene for personvernet. Det foreligger altså uenighet om enten de faktiske konsekvenser for personvernet, eller om hvorvidt eller i hvilken utstrekning disse konsekvensene skal tillegges vekt - eller begge deler.

1.1 HVA MENES MED "PERSONVERN"?

Før vi med utgangspunkt i departementenes høringsnotat går inn på diskusjonen om denne delikate balansen og hvordan oppnå og vedlikeholde den, er det nødvendig å etablere en forståelse for hva som menes med begrepet "personvern". Å unnlate å diskutere begrepets innhold, gjør at personvernets forsvarere legger seg åpne for en usaklig men ofte forbausende effektiv kritikk mot personvernet og forsvaret av dette.

Noe av det problematiske i begrepet ligger i at vi i et komplekst samfunn har å gjøre med ulike interesser, som hver for seg representerer sin egen vilje. Hver og en av disse interessene vil

hevde at deres synspunkter er like legitime som de andres. Her har vi å gjøre med et helt sentralt punkt som aldri kan fokuseres for sterkt: Når kompliserte avveiningsspørsmål og problemstillinger skal finne sitt svar, handler diskusjonen i høy grad om definisjonsmakt. Det finnes en betydelig risiko for at myndigheter i et samfunn gjennom sin psykologiske autoritet og påvirkningsevne i kraft av å fremstå som ledende influerer deler av befolkningen til å anta at de representerer rettferdigheten, det trygge og ansvarlige, mens borgerne som helhet må underkastes en omfattende kontroll for å ikke oppføre seg "ondt" og uansvarlig. Vi skal merke oss at troen på den eskalerende kontrollens nødvendighet viser en lei tendens til å øke i takt med at de teknologiske muligheter for kontroll og overvåkning utvides.

Det eksisterer utallige eksempler fra både historien og vår samtid på hvor galt det kan gå, når de som besitter makt blir gjenstand for en uforholdsmessig stor tillit og betraktes som berettiget til å på borgernes vegne definere hvilke normer som skal gjelde i samfunnet. Derav vår fokusering på definisjonsmaktens betydning også når det er snakk om personvern. Etter EFNs oppfatning kan normer for borgernes personvern bare sikres og etterleves dersom borgerne klarer å unngå en overdreven tillit til myndigheters maktutøvelse, og tar konsekvensen av at maktbalansen mellom samfunnets aktører er avgjørende og til alle tider vil være det. Denne maktbalansen er aldri gitt en gang for alle. Man kan i realiteten aldri skape et demokrati gjennom vedtak, ei heller permanent sikre dets overlevelse gjennom lov. Bare borgernes egen årvåkenhet, kritiske sans og aktive deltakelse kan gi samfunnets og statens felles verdier en trygg forankring i det lange løp. Lovverket kan naturligvis og bør reflektere og støtte demokratiets målsetning, og det konstitusjonelle demokrati gir et rammeverk som legger til rette for dets eksistens og funksjon, men for at folkestyret slik vi ønsker det skal overleve er borgernes innsats og vilje til å opprettholde et kritisk øye mot myndigheter og myndighetsinstitusjoner en avgjørende faktor. Det er i dette lys EFN betrakter personvernbegrepet, og søker å utbre en forståelse for nødvendigheten av å mobilisere den kritiske sans når det hevdes at borgernes trygghet øker når kontrollerende tiltak som rammer samtlige borgere foreslås gjennomført.

Staten og myndighetene har et utall vitale oppgaver i et komplekst samfunn. En av statens viktigste funksjoner er å sørge for lov, likhet for loven, rettsikkerhet og orden i samfunnet. Politioppgaver, derunder etterforskning av forbrytelser og pågripelser av individer som utgjør en fare for samfunnet, samt overvåkning av individer som utgjør særlig stor risiko, tilligger staten å administrere på samme måte som domstolenes funksjoner gjør det. Dette krever at makt delegeres til maktapparatet for at de aktuelle funksjonene skal ivaretas. Staten og dens maktapparat har dermed et stort ansvar, som må forvaltes på ansvarlig måte. Det er spesielt i forbindelse med politioppgaver at kravet til ansvarlig maktutøvelse i tråd med rettsstatens prinsipper må være absolutt.

I forbindelse med dette kravet til ansvarlighet er det at et annet element kommer inn: Også i et demokratisk rettssamfunn foreligger det en reell fare for at statens myndigheter og maktapparat i mangel av tilstrekkelig motkraft i form av kritiske borgeres blikk kan utvikle en selvstendig "maktkultur" hvor bestemte etater og deler av slike over tid tøyser rettsstatens grenser i sin praksis eller blir til en selvstendig politisk kraft som utøver press mot rettsstaten og dermed borgernes rettsikkerhet. I en slik situasjon vil de samme etater og organisasjoner som har til oppgave å forsvare rettsstaten, paradoksalt nok kunne bli til en trussel mot den samme rettsstaten gjennom en lukket maktfullkommenhet hvor man blir en stat i staten og lett kan komme i skade for å utvikle en modus hvor man trår over et antall av de skranker som rettsstaten er avhengig av for å overleve. Dette er et mønster vi ser i mange land i verden, og at vi på grunn av gunstige historiske og sosiale faktorer i stor grad har vært forskånet mot de verste utslagene av slike tendenser i Norge er ingen grunn til å redusere årvåkenheten. Den gamle regel om at makt korrupperer, gjelder fortsatt.

Heller ikke i Norge har vi unngått utslag av at maktapparatet har tatt seg til rette, Lund-

kommisjonen fra 1994 fastslo utvetydig at det hadde forekommet lovstridig overvåking av et stort antall norske borgere på bakgrunn av disse borgernes politiske oppfatninger og maktapparatets negative forestillinger om disse oppfatningene. I enkelte graverende tilfeller ble mennesker overvåket på rent politisk grunnlag i årtier, lenge etter at det burde vært klart for det daværende overvåkningspolitiet at de angjeldende personene aldri utgjorde noen risiko for rikets sikkerhet. Eksemplet viser hva som kan skje til og med i det "uskyldige" Norge, når en maktkultur får utvikle seg uten tilstrekkelige korreksjonsmekanismer. Her overtrådte rettsstaten også i vårt land sine grenser, selv om dens innebyggede mekanismer klarte å rydde opp gjennom nedsettelsen av Lund-kommisjonen og den etterfølgende politiske utluftning.

Selv om hensikten med å ha en stat og opprettholde statens maktapparat er å øke samfunnets og samfunnsmedlemmenes trygghet mot de mange forskjellige sosiale, økonomiske, fysiske og politiske utfordringer og farer, må det være skranker mot maktutøvelsen, fullmaktene må ikke være for omfattende. Et lands myndigheter skal heller ikke oppkaste seg til å være borgernes herrer, men i stedet være deres tjenere. Det er borgerne som skal kontrollere staten, og ikke omvendt. Vi finner at hensynet til dette premisset, som bør være grunnleggende i et fritt samfunn, tilsier at regjeringen snur i denne saken og at rettsstatens prinsipper gir et imperativ om at personvernbegrepet skal tolkes og defineres i lys av befolkningens rettssikkerhet og trygghet mot maktmisbruk. Vi finner at argumentasjon som baseres på hva som påstås å være "samfunnets behov for å beskytte seg mot kriminalitet" eller "politiets behov" ikke er overbevisende, når vi legger til grunn historiske erfaringer og hva slags praksis som må være gjeldende i en demokratisk rettsstat.

1.2 KRITIKK AV PERSONVERNET

Det syn som går ut på at personvernet er noe brysomt, noe som står i veien for "overordnede samfunnsinteresser" hvor eksempelvis "politiets behov" eller "hensynet til kriminalitetsbekjempelse", kommer til uttrykk på karakteristiske måter og vises gjennom en type argumentasjon som vi for illustrasjonens og analysens skyld har gjengitt i sitats form nedenfor. Sitatenes opphavsmann er direktør i det Kriminalitetsforebyggende råd Erik Nadheim, og sitatene er hentet fra "Fokus" nr. 2-2007. "Fokus" er en publikasjon utgitt av Politiets kriminalitetsforebyggende forum. Vi siterer her to avsnitt fra Nadheims artikkel "Storebror har fått ufortjent dårlig rykte" for deretter å analysere dem:

Sitat 1:

Det er drøyt 30 år siden begrepet "personvern" dukket opp i det norske språket. I offentlige dokumenter ble ordet brukt første gang i 1974. I ordbøker og leksikon trykket langt opp på 1980-tallet er "personvern" fremdeles ikke noe oppslagsord. Etter mer enn 30 år har begrepet ikke noen entydig, definert mening. Professor Jon Bing, vår fremste jus og edb-ekspert har en gang kalt ordet "luftig lik en klam, kald skydott". Det bekymringsfulle er at den praktiske anvendelsen av dette udefinerte begrepet stadig brukes i den offentlige debatt, og - hva verre er - i det offentliges styring av vårt samfunn. Dette har, etter mitt skjønn, fått negative konsekvenser for trygghet, ro og orden og mulighetene for å drive kriminalitetsforebyggende arbeid. Helt fra første gang mennesket flokket seg sammen og etablerte samfunn, har det sentrale vært vernet av de personene som samfunnet består av. Våre forfedre søkte samfunnsfelleskap til trygghet mot ytre fiender, mot sult, nød, ville dyr og røvere. Intet samfunn kan etablere slik trygghet uten å måtte innskrenke friheten til den enkelte. Vi kjøper trygghet og sivilisasjon, mot å gi avkall på noe av vår personlige integritet. I alle samfunn må hensyn til fellesskapet avveies mot hensynet til enkeltindividets personlige integritet. Denne avveiningen er ofte meget vanskelig, og den er klart politisk.

Sitat 2:

Personvernet er blitt et honnørbegrep, ladet med positive og beskyttelsesverdige verdier. Jeg har dessverre alt for ofte følelsen at mange er blitt fristet til å bruke "personvern" som en populistisk trylleformular. Etter at det kastes inn i en debatt, faller alle andre argumenter maktesløse til jorden. Slik bør det ikke være. Etter mitt syn representerer personvernet en interesse, som må veies mot andre interesser. Det bør på ingen måte være gitt at personvernet skal vinne, i hvert fall ikke alltid. Ikke minst hensynet til det offentlige - til fellesskapet - bør etter mitt syn tillegges større vekt enn i dag.

Til det første sitatet vil vi si: Avsnittet inneholder et utsagn som få vil kunne si seg uenig i, men en selvfølgelighet gir ingen svar på hvordan takle de vanskelige avveiningsspørsmålene. Hva som er det vesentlige, og som Nadheim må gis ubetinget rett i, er at slike avveininger er vanskelige - og først og sist er de politiske. Det handler om politiske spørsmål, hvor samfunns- og menneskesyn bestemmer hvor grensene for statens myndighetsutøvelse og inngripen skal trekkes.

Menneske- og samfunnssynet avgjør ikke bare hvilke verdier vi tillegger størst vekt, disse ideologiske faktorene farver hvordan vi oppfatter situasjonen i hvert enkelt av de avveiningsspørsmålene som oppstår når noen i en ansvarlig posisjon må ta beslutninger som innebærer at det tas ansvar for kanskje et større antall menneskers sikkerhet, liv og helse. Da kan det være forståelig, men ikke dermed tillatelig, at vektleggingen til tider søkes forskjøvet i retning av en øket kontroll for å oppfylle hva som kan oppfattes som et trygghets- eller sikkerhetsimperativ. Den i og for seg lite kontroversielle påpekningen av at nødvendigheten av å ivareta fellesskapsansvaret nødvendiggjør at noen aspekter av individets personlige integritet påvirkes, gir intet retningsgivende svar på hvor kompromissenes balansepunkt skal legges. **Uten noen inngående analytisk vurdering av de aktuelle tiltak i lys av hvilke følger tiltakene får i forhold til den fine, og for et demokrati livsviktige, balansen mellom myndighetene og statens maktapparat på den ene side og borgerne og deres interesser på den andre, ligger veien åpen for maktmisbruk fra statens og myndighetenes side.**

Erik Nadheim gir i sin artikkel uttrykk for at den praktiske anvendelsen av begrepet personvern etter hans skjønn "har fått negative konsekvenser for trygghet, ro og orden og mulighetene for å drive kriminalitetsforebyggende arbeid". Det er liten tvil om at med et slikt idemessig utgangspunkt som grunnlag for behandlingen og avgjørelsene i saker som angår balansen mellom tillit og kontroll i samfunnet, så er risikoen stor for en kontinuerlig utvidet kontroll- og inngrepsmakt fra myndighetenes side overfor innbyggerne ettersom man på forhånd har bestemt seg for at kontrollmulighetene og bruken av dem er hva som skal gis første prioritet i avveiningene.

Å bruke våre forfedres kollektive forsvar mot ytre fiender og belastninger som "sult, nød, ville dyr og røvere" som argument til fordel for øket statlig kontrolltrykk er å overse at i våre dager skaper moderne teknologi tidligere ukjente muligheter til detaljkontroll og maktmisbruk på grunnlag av de informasjonen kontrollen innsamler, og at de som i våre nåværende samfunn forvalter makten derfor har blitt en selvstendig risikofaktor dersom denne makten blir for inngripende. Til alle tider har det vært slik at uforholdsmessig mye makt fører til misbruk av den samme makten. Erkjennelsen av dette er uavhengig av tid og sted, og må alltid ligge i bunnen når vi skal bedømme hvor stor faren er for statlig maktmisbruk.

Tatt i betraktning de teknologiske muligheter som i dag foreligger for å kartlegge nær sagt samtlige bevegelser mennesker gjør i løpet av en normal hverdag, synes det utvilsomt at

faren for en stadig eskalerende kontroll er mye større enn faren for at det skal bli for lite kontroll. Dette handler naturlig nok om hvem og hva som skal kontrolleres og etter hvilke kriterier, for teknologien har ingen egen vilje eller innebygget retning. Her gjelder det å være bevisst på å unnlate å bruke en teknologi når bruken har effekter vi ønsker å unngå. Dette valget ligger der som en menneskelig mulighet. Vi har muligheten til å forme vår fremtid ved å velge bort noe og i stedet velge noe annet.

Til sitat 2 er å bemerke at personvernet der kritiseres for å være et "honnørbegrep", og at Erik Nadheim bruker betegnelser som "populistisk trylleformular" når han skal beskrive hvilken rolle personvernet spiller. EFN mener det er meget beklagelig dersom den form for negative forestillinger om personvernets innhold som her formidles får legge premissene for utformingen av politikken, og **vi er sterkt uenige i den virkelighetsbeskrivelse som kommer til uttrykk når det hevdes å foreligge en motsetning mellom hensynet til fellesskapet og hensynet til personvernet. For fellesskapet er det av den aller største viktighet at balansen og tillitsforholdet i samfunnet mellom myndigheter og borgere opprettholdes. Da er det påkrevet å forstå at fellesskapet vil komme til å lide, dersom vi går inn på en vei der de foreliggende kontrollmuligheter benyttes fullt ut** fordi noen som besitter ansvarlige posisjoner har bestemt på samtlige innbyggers vegne at "dette er til deres eget beste". Her er det konsekvensene, og absolutt ikke hensiktene bak, som må tillegges vekt når vi skal vurdere hvorvidt et tiltak eller en lov kan anses som akseptabel.

Det må presiseres på det sterkeste at temaet her ikke er "ond vilje". De fleste som leser dette vil trolig være kjent med ordtaket om at "veien til et 'visst sted' er brolagt med gode forsetter". Vi går ikke ut i fra at det være seg den direktøren i KRÅD som her fikk være eksempeleverandør, eller andre av de aktørene i personverndebatten som har gitt uttrykk for beslektede synspunkter som impliserer at det ikke er så farlig om kontrollnivået øker, har bevisst "onde" hensikter. På samme måte ser vi heller ingen grunn til å tro noe annet enn at de etater og tjenestemenn som gjennom Lund-kommisjonens arbeide ble funnet å ha trådt over lovens grenser gjorde dette i en dyp overbevisning om at de beskyttet samfunnets interesser. Fraværet av balansemekanismer og manglende årvåkenhet er hva som baner veien for denne type uønskede fenomener.

Vårt syn er at konsekvensene er hva som må holdes i fokus hele veien, for mest mulig effektivt å kunne forebygge uheldige utslag av maktutøvelse. Så ligger det en utfordring i å bedømme konsekvensene på en mest mulig nøktern og analytisk måte slik at de beste valgene kan foretas. Ingen sier at dette er lett. **Vi sier imidlertid at maktbalansen mellom myndigheter og borgere må tillegges den største vekt dersom vi skal unngå at det foreskrives en medisin som senere viser seg å bli meget verre i sine konsekvenser enn de uønskede fenomener det var den gode intensjon å få bukt med. Et sentralt prinsipp her er at borgerne skal kunne kontrollere myndighetenes forvaltning av den makt som ligger i at de bestyrer staten på borgernes vegne.**

1.3 STOREBROR OG STOREMOR

Når vi betrakter kriminalitetspolitikk og kriminalitetsforebygging i et "fugleperspektiv" og ser på hvilke politiske tendenser eller partier som i vår samtid tar til orde for en strengere kontrollstat, kan vi si at vi litt grovt skissert har å gjøre med to politiske hovedstrømninger som tenderer mot å ville øke kontrollnivået i samfunnet. De er ikke absolutt atskilte, men tendensene er tydelige.

Den ene tendensen representeres av deler av den konservative høyresiden, som tradisjonelt har vektlagt aspektene med ansvar for dine handlinger og strenge reaksjoner som respons på sosialt uakseptabel atferd som alvorlig kriminalitet. Et slikt primærfokus vil gjerne senke tersklene for å iverksette en inngripende kontroll overfor individene, fordi man ser lov og orden som et sentralt mål i samfunnsbyggingen ("lov og orden-staten"). Mens deler av venstresiden ønsker fokus på

omsorg og vil beskytte individene mest mulig, også mot seg selv ("omsorgsstaten").

Lov og orden-staten (Storebror) har en del sosialpolitiske prioriteringer som skiller seg fra omsorgsstaten (Storemor) sine kontrollmotivasjoner, og som ikke er tema her, men de utgjør skillelinjer som gjør det enklere å beskrive de forskjellige motivasjonene bak ønsker om å utsette statens innbyggere for et uforholdsmessig kontrolltrykk.

1.3.1 STORSTILT OG OMFATTENDE REGISTRERING

Særlig når det gjelder vår privatøkonomi er vi gjenstand for en storstilt registrering av opplysninger. For eksempel behandler og lagrer bankene kunde-, konto- og transaksjonsopplysninger i meget stort omfang, og alle elektroniske betalinger ut og inn, samt hvem til og fra registreres. Men, kanskje overraskende for mange, i tillegg registreres det hvor du er når du bruker kortet og også hva du betaler for. Dessuten føres det statistikk over ditt pengeforbruk over tid. Alle disse opplysningene uten unntak registreres og lagres. Både skatteetaten, NAV og politiet har legalt blitt gitt vide hjemler for innsyn i disse opplysningene, men det er mellom 20 og 30 forskjellige offentlige etater som har forskjellige grader av lovhjemmel til å få innsyn i folks bankkonti og økonomiske forhold.

At mange typer opplysninger allerede lagres om statens innbyggere, er i motsetning til hva det regelmessig gis inntrykk av i offentlige debatter ikke et gyldig argument for å registrere og lagre enda mer. Det er tvert i mot et argument for å stille spørsmålet om vi er i ferd med å gå så langt i å registrere menneskers bevegelser at vi har å gjøre med en situasjon hvor privatlivet og personvernet allerede er i ferd med å bli ofret på effektivitetens alter. Dersom våre bevegelser og vår private kommunikasjon i tillegg skal lagres for å kunne tilgjengeliggjøres for politiet, og i fremtiden med stor sannsynlighet også for andre etater, vil vi mene at viktige verdier i et fritt samfunn tapes.

1.3.2 SAMFUNNETS SVAKESTE RAMMES ALLTID MEST AV ØKT KONTROLL

Storemors kontrollvilje bunner i første rekke i ønsket om sterk samfunnskontroll for å sikre at alt går "riktig" for seg. Representantene for denne tendensen vil typisk legge forholdsvis mindre vekt på straffeaspektet, og kombinere kontrollen og kriminalitetsbekjempelsen med en åpning henimot muligheter til rehabilitering og tilbakeføring til samfunnet. Likevel ser vi ofte at parallellt med omsorgen vektlegges kontrollen i uforholdsmessig grad, og det skjer ofte på områder hvor omsorgseffekten kan komme til å motarbeides av en altfor rigid kontrollpraksis. Et godt eksempel her er hvordan enkelte NAV-klientgrupper må stå til rette for sine økonomiske disposisjoner i den grad at ikke bare må NAV få innsyn i bankkonti før stønad tildeles, man vil i tillegg også ha oversikt over eventuelle realiserbare verdier som vedkommende klient eier.

Besitter klienten eiendeler av salgbar verdi, kan sosialetaten/NAV kreve at disse blir solgt for å skaffe penger selv om klienten ikke har noen gjeld, og uansett om klienten dermed tvinges til å avhende salgbare verdier som både har stor praktisk og trivselsmessig betydning for henne eller ham. Vi trenger ingen spesielt velutviklet fantasi for å forstå at følgene for mange ville bli kjedelige, dersom adgangen til å benytte kontanter som betalingsmiddel ble stoppet, og staten benyttet anledningen til innsyn i hvor mye penger folk bruker og på hva som faktor i ulike typer saksbehandling ville få betydelig negativ virkning for individet. Selv om dette eksemplet ikke er hentet fra kriminalitetsbekjempelsens arena er det relevant i en personverndiskusjon, ettersom det illustrerer hva som skjer når det offentliges kontroll omfatter stadig flere områder og berører mange mennesker.

Det er som regel de svakeste blant oss som først lider under den overdrevne kontrollviljen,

og dette er et poeng når det hevdes at samfunnets interesser krever tett kontroll med det enkelte samfunnsmedlems bevegelser og disposisjoner.

Eksempler på hvordan myndigheter og etater søker kontroll og griper inn i individers disposisjoner gir en pekepinn på hvordan normene for hva samfunnets ulike etater kan betrakte som områder for kontroll og inngrep, med stor sannsynlighet kan forventes å bli forsøkt utvidet i takt med at de teknologiske kontrollmulighetene øker. Dette gjelder dermed også i tilfeller hvor et tiltak søkes innført og forsvart med begrunnelse i påberopte hensyn i forhold til kriminalitetsbekjempelse, men hvor sannsynligheten for formålsglidning realistisk må vurderes til å være svært stor fordi selve systemet synes bygget opp på mistenksomhet og tro på nødvendigheten av rigid kontroll snarere enn tillit til mennesker.

1.3.3 TILGANGSUTVIDELSER OG FORMÅLSGLIDNING

Den av regjeringen oppnevnte Personvernkommisjonen fra 2007 har publisert en uttalelse hvor Datalagringsdirektivet ble vurdert. I uttalelsen ble det lagt vekt på hvordan også andre etater enn politiet med god grunn vil kunne hevde at samfunnet vil bli tryggere ved at de får utlevering av trafikkdata:

Kredittilsynet og tollvesenet kan finne gode begrunnelser for at utlevering av trafikkdata vil bistå disse etatene i sitt arbeid. Helsevesenet kan argumentere for at kartlegging av sosiale kontaktnett gjennom trafikkdata kan redde liv og helse når man trenger å spore bærere av alvorlige smittsomme sykdommer. Nød- og redningsetater vil kunne argumentere for at trafikkdata vil kunne hjelpe dem med sporing av savnede personer.

EFN deler Personvernkommisjonens bedømmelse av at slike formål hver for seg kan være gode, men at den samlede bruken av de tilknyttede tiltakene kan utgjøre en alvorlig trussel mot personvernet. I det hele tatt er det viktig å erkjenne at vi i vår forståelse av betydningen av "personvern" hele tiden er bevisste om at uforholdsmessige inngrep i enkeltmenneskers liv kan skje som en følge av også "gode" intensjoner når kontrollaspektet vektlegges i så stor grad at enkeltindividenes gjøren og laden på forskjellige livsområder betraktes som nødvendige arenaer for statens og myndighetenes innsyn og kontroll også når hverken kriminell handling eller begrunnet ("skjellig grunn til") mistanke om en faktisk kriminell handling foreligger. Vi vil understreke at vi med disse betraktningene ikke vil eller kan ha noen partipolitiske preferanser, vi ønsker å påpeke at ulike politiske ambisjoner med selv de beste hensikter kan "gå over sine bredder" og føre til et kontrollsamfunn hvor tryggheten til slutt blir skadelidende.

1.3.4 ALLE ER IDEOLOGISKE, INGEN ER VERDINØYTRALE

Noe vi finner beklagelig i debatten, er de forsøkene som med ujevne mellomrom har forekommet på å påklistre motstandere av Datalagringsdirektivet merkelapper som "ideologiske korsfarere" mens tilhengerne presenterer seg selv som realistiske og ansvarlige samfunnsstøtter. Vi mener her å ha vist at standpunkter som favoriserer statens økende kontrollmakt over befolkningen i sin natur er like ideologiske og verdiladete som andre standpunkter, og vi oppfordrer til en diskusjon med fokus på forutsigbare konsekvenser.

1.4 KONKLUSJON OM PERSONVERNBEGREPET

Som konklusjon på vår gjennomgang av personvernbegrepet vil EFN derfor hevde at synspunkter om at personvernet har fått uforholdsmessig stor vekt i vårt samfunn mangler dekning i den faktiske situasjon i Norge. At personvernet er satt under stort press, ser vi

når vi betrakter det politiske klima, der høylytte og taleføre tilhengere av øket kontrollnivå har gjort seg sterkt gjeldende i debatten og også har gått så langt som til å antyde at Datatilsynet burde erklæres inhabilt i spørsmålet om Datalagringsdirektivet. Vi finner også at påstander om at det skulle være en motsetning mellom personvernets interesser og samfunnets/fellesskapets interesser og at personvernet må vike ytterligere i forhold til dagens situasjon ikke har noen dekning i virkeligheten. Når det gjelder registreringen av personopplysninger og vanlige borgeres handlinger i deres hverdag, så er denne i Norge som i andre teknologisk avanserte samfunn allerede mer enn stor nok til å fremkalle bekymring på personvernets vegne.

2.0 DATALAGRINGS DIREKTIVET OG "ALVORLIG KRIMINALITET"

I departementenes høringsnotat på side 47 sies følgende:

Det foreslås at utlevering av data bør kunne pålegges dersom det straffbare forholdet har en strafferamme på fengsel i 3 år eller mer. Dette er i samsvar med den definisjonen av alvorlig kriminalitet som er nedfelt i Den europeiske arrestordre 13. juni 2002 (2002/584/RIA). Denne standarden er også anvendt i andre sammenhenger (Rammebeslutning 2006/960 av 18. desember 2006, om forenkling av utvekslingen av opplysninger og etterretninger mellom medlemsstatenes rettshåndhevende myndigheter).

Viktig her er at hva som beskrives i sitatet er de norske myndighetenes definisjon og norm i 2010. Avtaleteksten i EUs datalagringsdirektiv inneholder ingen angivelser for hvor små eller store lovbrudd som skal kunne utløse utlevering av de lagrede opplysningene, og det er dermed ikke forutsatt i avtalegrunnlaget at slik utlevering av kommunikasjonsdata bare skal finne sted i forbindelse med særlig alvorlige lovbrudd.

I tillegg kommer at heller ikke de norske departementenes standard representerer noen høy terskel. I slike sammenhenger er det forskjell på minstestraft og strafferamme. Og her dreier det seg ikke om minstestraft, men om strafferamme. Høringsnotatets tekst kan vanskelig feiltolkes. At en lov har en strafferamme på tre år eller mer, skal være tilstrekkelig for å kunne kreve opplysningene utlevert fra teletilbyderne. Denne strafferammen omfatter et betydelig antall forbrytelser.

Dertil åpnes det for at lover som har en betraktelig lavere strafferamme enn to år skal være grunnlag for utlevering. Dette gjelder straffelovens (strl) paragraf 91a som har to års strafferamme, og strl. paragraf 145a som har seks måneders strafferamme, bare for å nevne to eksempler. Sitat fra høringsnotatet som illustrerer:

§ 210. Ting som antas å ha betydning som bevis, kan retten pålegge besitteren å utlevere såfremt han plikter å vitne i saken. Retten kan likevel bare pålegge besitteren å utlevere data som er lagringspliktige etter ekomloven 2-8 annet ledd såfremt noen med skjellig grunn mistenkes for en handling eller forsøk på en handling som etter loven kan medføre straff av fengsel i 3 år eller mer, eller som rammes av straffeloven §§ 91, 91a, 104 a, 132 b, 145 annet ledd, 145 a, 162, 201a, , 203, 204a, 317, jf. §§ 162 eller 390 a. Reglene i § 137 og domstolsloven § 206 gjelder tilsvarende.

Dette illustrerer godt at departementenes høringsbrev alene forteller oss at de mange forsikringer om at bare særlig alvorlige forbrytelser skulle medføre utleveringsplikt ikke overbeviser om at de lagrede dataene bare skal utleveres i tilfeller av helt spesielt grov kriminalitet. Vi nevner dette fordi det i den offentlige debatt har vært hevdet fra tilhengerne av Datalagringsdirektivet at bare

særlig alvorlig kriminalitet er relevant i diskusjonen om hvilke lovbrudd og straffebed som utløser plikt til utlevering av elektroniske trafikk- og lokasjonsdata i henhold til direktivet.

På side 50 i høringsnotatet står følgende:

Et unntak fra taushetsplikten slik som her er antydnet innebærer ingen opphevelse av taushetsplikten i andre tilfeller enn de som er nevnt i unntaket, herunder tilfeller der andre myndigheter har lovlig tilgang til trafikkdata, se avsnitt [4.13]. I slike andre tilfeller som ikke omfattes av unntaket vil Post- og teletilsynet fortsatt ha en rolle når det gjelder å fritta tilbyder fra taushetsplikten. Dette gjelder også i saker om bevisføring etter tvisteloven paragraf 22-3.

I tvistelovens paragraf 22-3 står følgende:

(3) Etter en avveining av hensynet til taushetsplikten og hensynet til sakens opplysning kan retten ved kjennelse bestemme at beviset skal føres selv om samtykke er nektet, eller at beviset ikke skal mottas selv om departementet har samtykket. Departementet skal få redegjøre for sitt standpunkt før retten treffer avgjørelse. Redegjørelsen meddeles partene.

Ifølge tvisteloven paragraf 22-3, synes det ikke å være noen garanti mot at andre enn politiet får tilgang til data. Det eneste vilkår for utlevering, er at Post- og teletilsynet gir fritak fra taushetsplikten, og at retten bestemmer at beviset (= data) skal gjøres tilgjengelig. I tvisteloven står intet om "serious crime" eller noen bestemt strafferamme. Dermed er det tenkelig at data som er lagret i henhold til direktivet blir utlevert til andre enn politiet, uavhengig av hvilken strafferamme det er snakk om. Det foregående er bare ett av mange mulige eksempler.

2.1 KRITERIENE FOR UTLIVERING VIL ENDRES OG FORMÅLSGLI

I høringsbrevet gis det uttrykk for at det kun er politi og påtalemyndighet som skal gis tilgang til denne informasjonen, og det samme har DLDs tilhengere gitt uttrykk for i den politiske debatten rundt dette. Men igjen er dette utelukkende norske myndigheters posisjon i 2010, og vi kan med sikkerhet gå ut i fra at det vil være mange blant både offentlige etater og andre som vil ønske å få tak i dette materialet. Verdt å merke seg er at ingenting i direktivets originaltekst sier at det kun er politimyndigheter som skal få utlevert dataene. Hva som sies i direktivets artikkel fire om den saken, er gjengitt i høringsbrevet:

Medlemsstaterne træffer foranstaltninger til at sikre, at data, der lagres i overensstemmelse med dette direktiv, kun udleveres til de kompetente nationale myndigheder i særlige sager og i overensstemmelse med national lovgivning. Hver medlemsstat fastsætter i sin nationale lovgivning den procedure, der skal følges, og de betingelser, der skal være opfyldt for at få adgang til lagrede data i overensstemmelse med kravet om nødvendighed og proportionalitet, under hensyn til de relevante bestemmelser i EU-retten og folkeretten, herunder navnlig den europæiske menneskerettighedskonvention, således som den er fortolket af Den Europæiske Menneskerettighedsdomstol.

I klartekst betyr dette at det er opp til hvert enkelt land å bestemme hvilke betingelser som skal innfris for at det skal gis adgang til dataene, derunder hvilke etater som til enhver tid skal defineres som "kompetente myndigheter". At norske politikere i 2010 da avgir "forsikringer" om at politiet alene skal få slik tilgang, er ikke egnet til å berolige overhodet. **All erfaring fra andre kontrolltiltak forteller at man over tid vil ønske å benytte den nye muligheten til flere formål enn opprinnelig påtenkt eller annonsert. Denne formålsglidningen synes uunngåelig,**

og dens følger er mer alvorlige desto mer inngripende det opprinnelige formål var.

Etter EFNs mening har vi ganske enkelt ikke lov til å overkjøre befolkningens privatsfære i den grad en massiv innsamling av alles trafikk- og lokasjonsdata innebærer. Dette er en slutning vi trekker både når direktivets bestemmelser og formål betraktes isolert og når det tas i betraktning at et system som er innrettet på å utøve kontroll vil tendere mot å optimalisere sin "produktivitet" ved å søke formålsoppfyllelse i form av å oppdage og gripe inn mot de uregelmessigheter eller uønskede fenomener det er innført for å kontrollere, over tid også vil være gjenstand for formålsglidning. Denne skjer når den relative suksessen i forhold til å kartlegge for det opprinnelige formålet gjør at det også blir tydelig at enda flere "gode" hensikter vil kunne oppnås dersom man lar systemet utøve kontroll med enda flere fenomener, livsområder og normale hverdagshandlinger hvorav et økende antall over tid betraktes som noe som bør kartlegges og kanskje reageres mot - simpelthen på grunn av at muligheten foreligger til å gjøre flere livsområder som det tidligere var enighet om tilhørte privatlivet til gjenstand for statens innsyn og kontroll.

Det innebærer å snu det hele på hodet, når det hevdes at øket teknologisk kontrollinnsats der vanlige menneskers bevegelser i sin hverdag registreres uten at noe kriminelt er påvist er nødvendig for å bekjempe terrorisme, barnepornografi og andre former for kriminalitet. Nødvendigheten er ikke dokumentert.

Videre er situasjonen at de økte kontrollmulighetene skaper muligheter for myndigheter til å foreta kontroll og inngrep på livsarenaer som tidligere tilhørte privatsfæren fordi kontrollmulighetene dengang ikke eksisterte. Den maktubalanse mellom myndigheter og borgere som et slikt scenario medfører er en betraktelig større risiko enn kontrollsamfunnets tilhengere i store deler av debatten har villet erkjenne. Kriminelle vil ikke klare å destabilisere samfunnet, og kriminaliteten øker ikke i et slikt omfang at det er nødvendig å bruke virkemidler fra en unntakstilstand for å begrense den. Dette handler om rettsstatens forutsetninger som vi ikke har råd til å tukle med.

Datalagringsdirektivet vil innebære en lovpålagt, statlig registrering og lagring av opplysninger om hvem som til enhver tid har kommunisert med hverandre, så vel som når og hvorfra kommunikasjonen har skjedd. **Når det gjøres til et stort poeng at selve innholdet i utvekslingen derimot ikke skal lagres, er det på ingen måte klart at dette dermed gjør innsamlingen mindre inngripende i privatlivet. Hvilke mennesker man har kontakt med, når og hvor ofte, forteller over tid svært mye om ens omgangskrets, interesser, kanskje om sykdommer, spesielle tilbøyeligheter som seksuell atferd eller annet. Å kunne sammenfatte et "sosiogram" over individer basert på slike opplysninger, vil ofte være mer beskrivende for hvem individet er enn dersom det ofte relativt banale innholdet i e-poster, SMS-meldinger eller telefonsamtaler skulle vært lagret. At innholdet i kommunikasjonen ikke foreslås lagret, gjør ikke Datalagringsdirektivet mindre alvorlig i sine konsekvenser eller mer akseptabelt.**

Det prinsipielt helt nye i en slik praksis som Datalagringsdirektivet foreskriver, er at opplysninger om normalbefolkningens bevegelser og handlinger skal registreres og lagres for politimessige formål. Dette reflekterer at det åpenbart må ha funnet sted en radikal endring i den rettspolitiske tenkningen rundt kriminalitetsbekjempelse og rettssikkerhet.

I Straffeprosesslovens paragraf 224 knesettes følgende prinsipp:

§ 224. Etterforskning foretas når det som følge av anmeldelse eller andre omstendigheter er rimelig grunn til å undersøke om det foreligger straffbart forhold som forfølges av det offentlige.

Det er gode grunner til å anse lovpålagt innsamling av opplysninger om hele befolkningens elektroniske bevegelser og handlinger for politiformål for å være et statlig pålagt etterforskningstiltak overfor hele befolkningen. Hva som er så spesielt med det, er at innsamlingen og lagringen foretas uten at det foreligger noen av de i rettsstaten aksepterte grunnlag for å undersøke om det foreligger straffbart forhold. **Uten at det foreligger mistanke, uten at det i det hele tatt er brakt på det rene hvorvidt noe lovbrudd overhodet har skjedd, samles dataene. EFN mener at dette er å fremme et tiltak som bryter på avgjørende måte med sentrale deler av grunnlaget for rettsstaten, ved at man legger opp til å behandle mennesker på en måte som ville vært naturlig dersom de hadde vært under mistanke for noe kriminelt, men uten at skjellig grunn til mistanke foreligger. Det er grunnlag for å si at dette innebærer at hele folket settes under mistanke, noe som er et hittil ukjent prinsipp i vestlige demokratiske stater. I en rettsstat må det eksistere vel definerte grenser for når borgerne kan gjøres til gjenstand for etterforskning, og Datalagringsdirektivet overskrider disse grensene markant på en måte som er til alvorlig skade for tillitsforholdene i samfunnet.**

2.1.1 UTLEVERING TIL UTLANDET AV OPPLYSNINGER OM STATENS INNBYGGERE

I debatten om Datalagringsdirektivet, og i forlengelsen av denne debatten, har det ofte blitt henvist til behovet for internasjonalt politisamarbeid. Mange vil kanskje umiddelbart føle at det må være ønskelig med en mest mulig strømlinjeformet utlevering av opplysninger og mistenkte individer mellom politimyndigheter fra ett land til et annet. Spesielt etter den dramatiske terrorhendelsen i USA den 11 september 2001, og senere bombeeksplosjoner i London og Madrid har mange mennesker gjennom dramatisk mediedekning kommet til å få det inntrykk at vårt samfunn er alvorlig truet av terrorister. Virkeligheten er en annen. Man må heller ikke glemme at det er store rettssikkerhetsproblemer forbundet med at en stat kan kreve mennesker utlevert fra en annen. Mange borgere i Europa vil føle seg definitivt ukomfortable med at medmennesker eller opplysninger om deres liv med loven i hånd skal kunne utleveres til politiet i stater der styresettet er mindre preget av et solid rettssystem og hvor myndighetene og maktapparatet i verste fall er influert av kriminelle. Slike stater finnes i Europa, selv om vi misliker å tenke på det.

Terroristene kan aldri vinne, og så godt som alle samfunn over hele verden vil alltid motarbeide og bekjempe terrorisme. Å fokusere på den farlige og skumle terrorist som infiltrerer samfunnet, er å la et skremmebilde diktere samfunnet. Paradoksalt nok er dette presis hva terroristene ønsker. Deres samfunnsideal er et autoritært, gjennomkontrollert samfunn der lederne har full kontroll over alle andre. Vi gir terroristene en stor gavepakke dersom vi bygger samfunnet på deres premisser.

2.2 TRAFIKKDATALAGRING ER OVERVÅKNING

Vi vil kort slå fast at det dreier seg om overvåkning når det samles inn detaljerte opplysninger om menneskers bevegelser. I et samfunn hvor elektronisk kommunikasjon i mange former blir en fremtredende del av menneskers hverdag, blir registrering av denne informasjonen med henblikk på senere utlevering til politi eller andre myndigheter et desto alvorligere inngrep siden slik registrering medfører en inngripende kartlegging av svært mye av de daglige aktiviteter.

Flere regjeringsoppnevnte utvalg har tidligere definert dataavlesing som overvåkning. I tillegg til Metodeutvalgets rapport NOU 2009:15 kan vi også vise til NOU 2004:6. At private teleoperatører pålegges overvåkningsoppdrag på vegne av staten, gjør ikke at man omgår Grunnloven. Snarere tvert imot. Når hensikten med datalagringen er å gi politiet mulighet til å

spore folk, da snakker vi om lagring av data som brukes til overvåkning.

Vi bør heller ikke la oss påvirke av lettvinte påstander om at "den som har rent mel i posen har ingenting å frykte"[3]. Enhver har et behov for et privatliv[4]. Påstander om at den som ikke har gjort noe kriminelt intet har å frykte, kan i sin ytterste konsekvens innebære at det legges opp til at den som misliker eller motarbeider kontrolltiltaket dermed blir tillagt skjulte kriminelle hensikter. Om mulig enda mer alvorlig er at budskapet om at "den som ikke har gjort noe galt..." i sin logiske ytterste konsekvens innebærer en påstand om at bare kriminelle har grunn til å ønske seg et privatliv hvor man unngår å være sporbar overfor staten.

Dersom informasjon om vanlige borgeres bruk av kommunikasjon via telefon, via SMS, med e-post, eller deres bruk av en IP-adresse i lengre ettertids lagres i den hensikt at materialet senere skal kunne hentes og brukes av landets myndigheter, så er vanlige borgere i et slikt scenario gjenstand for overvåkning. Om det forholdet kan det ikke herske tvil.

2.3 OVERVÅKNING AV WEB-BRUK

Til innholdsdata regnes også hvilke Internett-sider man besøker. I Datalagringsdirektivet er det ingen krav om at dette må registreres. Norske tilhengere av DLD har vært raskt ute med påpekningen av at noe slikt ikke er aktuelt i Norge. Her skal vi huske på at for ti år tilbake var det heller ikke på tale å lagre opplysninger om hvem som snakket med hvem. Dertil har lovgiverne i Danmark i sin innarbeidelse av direktivet i dansk lovverk tatt inn en bestemmelse om at også de IP-adressene du besøker skal lagres. Dette betyr at de kompetente myndigheter i Danmark i ettertids vil kunne lage en oversikt over hvilke nettsider danske borgere besøker. Ikke alltid helt nøyaktig helt ned til den enkelte side, ettersom et varierende antall nettsider kan dele en IP-adresse, men likevel kan man komme nokså nær et presist bilde av hver enkelt innbyggers nettaktivitet. I Storbritannia ønsker staten å gå enda lengre i sin innføring av Datalagringsdirektivet. Også der skal IP-adressene borgerne besøker lagres, slik som i Danmark. På toppen av dette ønsker britiske myndigheter å gi i alt 653 ulike offentlige etater lovlig rett til å få utlevert dataene som omfattes av lagringsplikten.

EFNs kommentar til dette, er at eksemplene fra Danmark og Storbritannia illustrerer med all mulig tydelighet hvilken glideflukt samfunnet står i fare for å begi seg inn på ved denne type tiltak overfor hele befolkningen. Det gjelder i høyeste grad også selv om den norske regjeringen i 2010 har planer om en "mildere" gjennomføring av Datalagringsdirektivet enn den danske og britiske myndigheter har lagt opp til. **Både lagringstid, kriterier for utlevering av disse dataene og bestemmelsene rundt hvilke "kompetente myndigheter" som skal få dem utlevert kan hele tiden endres i takt med skiftende politiske flertall eller stemningssvingninger. Så lenge dataene er lagret, har befolkningen ingen som helst sikkerhet mot misbruk. Skulle man snakke om sikkerhet, så er det snarere mer relevant å si at vi med til sikkerhet grensende sannsynlighet kan gå ut i fra at informasjonen om borgerne som blir lagret også vil bli benyttet over tid, og gjerne for utvidede formål i forhold til den opprinnelig angitte begrunnelsen for lagringen. Fristelsen er helt enkelt for stor til å i kriminalitetsbekjempelsens eller "samfunnets" navn utnytte mulighetene til utvidet kontroll av hva staten til enhver tid ønsker å føre kontroll med, når slusene først er åpnet ved å godta at alle skal gjøres sporbare i ettertids overfor myndighetene.**

Vår konklusjon her er etter vårt skjønn den eneste mulige, dersom rettsstatens prinsipper skal etterleves: Vi må på det aller sterkeste fraråde en omfattende lagring av data om borgeres kommunikasjon uten at de er mistenkt for noe kriminelt, eller er under etterforskning. Er man ikke under etterforskning, så skal det heller ikke lagres detaljert informasjon om hvem hver

enkelt av oss kommuniserer med, hvem som initierte kommunikasjonen og hvem som mottok den, når og hvorfra vi gjorde dette og hvor lenge kommunikasjonen varte, ei heller hvilke IP-adresser vi har benyttet.

2.4 IKKE KRAV OM DOMSTOLSBEKLUTNING ELLER SKJELLIG GRUNN FOR UTLEVERING AV DATA

I løpet av debatten rundt Datalagringsdirektivet, har det vært fremhevet at i Norge vil myndighetene implementere Datalagringsdirektivet på slik måte at de lagrede data bare skal kunne hentes ut etter avgjørelse i domstol. **Da er å bemerke at Datalagringsdirektivet, i motsetning til hva sikkert mange som ikke selv har lest dette tror, ikke forutsetter noen rettslig avgjørelse før lagrede data tilgjengeliggjøres for "kompetente myndigheter". Det er opp til den enkelte medlemsstat å bestemme hvilke krav som skal oppfylles før utlevering av data kan skje til de "kompetente myndigheter" staten bestemmer. Datalagringsdirektivet gir ingen anvisninger hverken når det gjelder hvilke myndigheter som skal anses som "kompetente" eller hvilke kriterier som skal legges til grunn for å utlevere opplysninger. Skiftende politiske flertall kan rimeligvis, i Norge som ellers, forandre på de gjeldende regler.**

Vi vil også nevne at Politiets sikkerhetstjeneste (PST) i sin høringsuttalelse om Datalagringsdirektivet sier følgende[5]:

Vi mener det er meget uheldig dersom det innføres et krav om at politiet må godtgjøre at "noen" med skjellig grunn kan mistenkes for en straffbar handling. Et slikt krav vil være for strengt, fordi det i en tidlig fase av etterforskningen ofte vil mangle oversikt over persongalleri/rollefordeling/tilknytning til saken. Det er også uheldig å knytte mistankevilkåret til person fordi det iverksettes etterforskning i mange saker med ukjent gjerningsperson, og hvor målet for etterforskningen nettopp er å finne fram til den som har begått den straffbare handlingen, samt utelukke uskyldige." I en slik sammenheng vil innhenting av historiske trafikkdata være ett av flere viktige virkemidler. Det vises til at høringsnotatet angir at det ikke innhentes trafikkdata i svært stor grad i dag; antallet oppgis til ca. 1900 tilfelle i året. Ivaretagelsen av personvernet gjelder neppe i stor grad utleveringen av trafikkdata; argumentasjonen har i hovedsak vist til selve lagringen som det personvernmessig problematiske. Det vises også til høringsnotatets vurderinger av at formålet med Datalagringsdirektivet i noen grad ikke vil bli oppnådd dersom det settes en slik begrensning på muligheten for politiet til å få tilgang til informasjonen. Høringsnotatet viser i siste avsnitt på s. 47 og første avsnitt på s. 48 til behovet for taushet i forbindelse med benyttede tvangsmidler. For PST gjelder behovet for at alle involverte bevarer taushet også når det benyttes tvangsmidler - herunder innhenting av trafikkdata - i forebyggende saker. Det vises til at Metodekontrollutvalget foreslår en hjemmel til å ilegge straffesanksjonert taushetsplikt for forebyggende tvangsmidler ved en endring i politiloven § 17f. PST anmoder om at denne endringen gjøres i forbindelse med innføring av lagringsplikt for trafikkdata, da det særlig er i forbindelse med teletilbydernes utlevering av trafikkdata det har vist seg å være behov for en slik bestemmelse."

EFN kommenterer til ovenstående:

At det allerede mens eventuell innføring av Datalagringsdirektivet diskuteres blir tatt til orde for at kravet om skjellig grunn til mistanke må bortfalle, illustrerer meget tydelig hvordan rettssikkerheten vil settes på spill dersom slike tiltak innføres. PSTs utsagn illustrerer også at når data først er lagret vil de også bli brukt, særlig når det henvises til forebyggende saker. Det kan

tenkes et grenseløst antall begrunnelser for å ønske data utlevert i "forebyggende" øyemed. Er dataene lagret, vil presset for å få tilgang til dem etter ulike og varierende kriterier hele tiden øke, og det vil bokstavelig talt bli fremmet en uendelighet av argumenter for hvorfor dataene skal utleveres og benyttes. I likhet med hva vi gir uttrykk for andre steder i denne høringsuttalelsen, reagerer vi på påstandene om at tilgjengeligheten av slike trafikkdata skulle være nødvendig for å bevise uskyld. Det er skyld som skal bevises. Videre vil vi peke på at det fra PSTs side argumenteres for ikke bare at data om alle borgernes elektroniske bevegelser skal lagres, men også for at disse dataene som er lagret om alle innbyggere skal kunne utleveres uten at det foreligger skjellig grunn til mistanke. Denne argumentasjonen viser tydelig hvordan glideflukten inn i en stadig tettere kontroll er uunngåelig, dersom vi godtar premisset om at staten skal ha rett til å kreve at opplysningene om alle borgernes kommunikasjon og elektroniske bevegelser skal lagres.

Vi vil fremheve PSTs utsagn om lagring og utlevering:

Ivaretagelsen av personvernet gjelder neppe i stor grad utleveringen av trafikkdata; argumentasjonen har i hovedsak vist til selve lagringen som det personvernmessig problematiske.

EFN mener at denne påstanden er helt feilaktig. De viktigste og mest relevante begrunnelser for hvorfor Datalagringsdirektivet er et meget uheldig tiltak for borgerne, går nettopp på det faktum at tiltaket krever at data om hele befolkningen lagres for det eksplisitte formål å gjøre dem tilgjengelig for statens myndigheter. Det er nettopp dette formålet om å gjøre data om samtlige innbyggere tilgjengelig med henvisning til behovet for kriminalitetsbekjempelse som representerer det fundamentale brudd på en grunnregel i rettsstaten: Nemlig at individer som ikke er konkret mistenkt for noe kriminelt, heller ikke skal overvåkes. En kartlegging av alles bevegelser, i den hensikt å kunne bruke informasjonen i tilfelle menneskene det gjelder skulle gjøre noe galt, er et kjennetegn ved politistaten, og ikke ved et fritt og demokratisk samfunn.

PST gir til slutt i sitatet uttrykk for ønske om straffesanksjonert taushetsplikt i forbindelse med innføring av lagringsplikt for trafikkdata, med den begrunnelse at det er behov for en slik bestemmelse i forbindelse med utlevering av trafikkdata. Vår kommentar er at når den som er under oppsikt ikke har noen mulighet til å få vite at hennes eller hans bevegelser er undersøkt, er vedkommende også fratatt sine muligheter for å konfrontere sine anklagere eller forsvare seg. Vi ser her at allerede før Datalagringsdirektivet har blitt gjennomført, tas det til orde for en utvidelse av bruken ved at det ikke engang skal kreves skjellig grunn til mistanke for å få utlevert dataene. Dette er selvsagt helt lovlig i følge Datalagringsdirektivets tekst, men det er ikke desto mindre et radikalt brudd med rettsstatens prinsipper. Kravet om å få utlevert data selv uten konkret mistanke, kombinert med hemmeligholdelse gjennom taushetsplikt og straffebed for den som formaster seg til å fortelle at data er blitt utlevert, legger alt til rette for en alvorlig underminering av borgernes privatliv og av selve rettsstaten.

Historisk vil vi her peke på erfaringene fra overvåkingen av venstreorienterte i Norge. Den tidligere nevnte Lund-kommisjonen påviste at slik overvåking på politisk grunnlag forekom, og at denne overvåkingen gikk så langt at den gikk langt ut over gjeldende instruks. EFN forstår at det iverksettes overvåking av individer som offentlig erklærer at deres mål er en voldelig omstyrning av samfunnet. Men denne overvåkingen av norske venstreorienterte fortsatte i tiår, altså meget lenge etter at den informasjon som overvåkningspolitiet innhentet om disse menneskene må ha gjort det klart at mange av de aktuelle norske venstreorienterte ikke utgjorde noen risiko for rikets sikkerhet.

Likevel foregikk overvåking av mange mennesker med "feil" politiske holdninger eller "feil" kontakter på politisk grunnlag i tiår, i den dypeste hemmelighet, uten at de som ble gjenstand for

dette maktovergrepet fikk noen mulighet til å forsvare seg mot de urettmessige antakelsene og mot overvåkningen. Det er derfor åpenbart hvilken glideflukt Datalagringsdirektivet disponerer for, dersom data om alle innbyggere skal lagres for at myndighetene skal få tilgang til dem. Når det i tillegg argumenteres for at dataene skal kunne utleveres uten konkret mistanke, blir bildet fullstendig. Rettssikkerheten ødelegges i et slikt scenario, og EFN vil på det mest bestemte advare mot at det norske samfunnet gjennom innføring av Datalagringsdirektivet går lenger inn på denne veien. Hensynet til rettsstaten og tilliten i samfunnet tilsier en forkastelse av Datalagringsdirektivet.

2.5 NOKAS OG BANEHEIA OPPKLART UTEN DLD

På side 41 i høringnotatet omtales to kjente norske alvorlige kriminalsaker. Det argumenteres her for trafikkdataenes betydning ved at det henvises til de to sakene og det fremheves hvordan trafikkdata utgjorde viktige bevis. Vi mener at eksemplene mangler en relevans til Datalagringsdirektivet, og faktisk viser at DLD ikke er nødvendig for å oppklare forbrytelser.

2.5.1 NOKAS

Når det gjelder NOKAS-saken, så ble det av assisterende politidirektør Vidar Refvik i et innlegg i Bergens Tidende i desember 2009[6] poengtert at "I Nokas-saken var det elektroniske spor som bidro til å knytte forbindelser mellom de senere domfelte ransmennene, og som gjorde det mulig å spore David Toska til Spania". I Aftenposten på nett den 17.03.2010 står det[7]: "Ifølge Kripas var pågripelsen av David Toska et direkte resultat av at IP-adressene for hans epost-bruk ble identifisert og sporet".

Dette er utvilsomt helt korrekt, men beskrivelsen er korrekt uten at den har relevans i forhold til en diskusjon om hvorvidt det er hensiktsmessig å innføre Datalagringsdirektivet. Situasjonen var at nevnte hovedmistenkte var på rømmen i Spania, og der benyttet Internett-kafeer for å kommunisere med andre kriminelle som politiet på forhånd hadde under etterforskning på grunn av berettiget mistanke. Politiet har da anledning til å sette mistenkte under kommunikasjonskontroll. Da de så kommuniserte, ble dette inkludert IP-adressene registrert og sporet fordi det forelå skjellig grunn til mistanke mot deltakere i kommunikasjonen. Slik kommunikasjonskontroll, som tidligere var kjent som telefonavlytting, praktiseres i dag overfor også de mer moderne former for elektronisk kommunikasjon når det er skjellig grunn til mistanke om forbrytersk aktivitet.

Det er ingen som mener noe annet enn at politiet skal og må ha muligheten til målrettet kommunikasjonskontroll ved skjellig grunn til mistanke, men dette har vel å merke ingenting å gjøre med datalagring i den form DLD foreskriver. Om man skal bruke NOKAS-saken til å argumentere for noe, så må det være for å gi politiet tilstrekkelige ressurser til å gjennomføre etterforskning raskt og effektivt når de faktisk har noe å gå etter. Her kan det nok være mye å hente. Særlig når politiet idag får altfor lite - og minkende - ressurser.

Tilsvarende gjelder for andre saker hvor elektroniske spor er viktige for avdekking og etterforskning av forbrytelser. Hva politiet trenger, er nok ressurser og godt teknisk utstyr slik at de innenfor rettsstatens rammer kan reagere og iverksette etterforskning når det er grunn til å mistenke noe kriminelt - eller når en forbrytersk handling er påvist. Samme resonnement gjelder ikke minst også problematikk rundt datainnbrudd. Her må det etableres varslingsystemer som kan reagere når noe kriminelt skjer. **De som sier nei til øket elektronisk kontroll over menneskers bevegelser, ønsker ikke å redusere politiets muligheter til å utføre sine oppgaver i samfunnet, de ønsker derimot at den virksomhet som politiet bedriver for å**

forhindre eller oppklare kriminalitet skal være målrettet.

2.5.2 BANEHEIA

Vedrørende Baneheia-saken ble også denne i høringsnotatet beskrevet som et tilfelle hvor trafikkdata var viktige i bevisførselen. Her kan vi imidlertid vanskelig se at så kan være tilfelle. Under sakens gang ble det sagt at en av de tiltalte hadde ringt fra sin mobiltelefon på et tidspunkt som nokså nøyaktig sammenfalt med det da de to drapene ble begått. Da uttalte politiet at dette var et spor som kunne knytte den hovedtiltalte til Baneheia og på drapstidspunktet. Går man inn for å sjekke saken nøyere, fremkommer imidlertid opplysninger som motsier dette. På NRK-nytt den 16.01.2002 fremgår at stedet der drapene ble begått lå utenfor dekningsområdet for det aktuelle telefonselskapet (Telenor)[8].

Telenor utførte selv to målinger som konkluderte med at det ikke var mulig å ringe fra åstedet og til den nærmeste aktuelle basestasjon. Dekningsdirektør i Telenor mobil Bjørn Reidar Amundsen uttalte at: "Vi er ikke bastante på å si at dette er den definitive streken, men vi har ikke klart å gjenskape en situasjon som gjør at Eg-A slår inn fra åstedet. Vi kan ikke utelukke at det har skjedd, men vi har ikke klart å gjenskape denne situasjonen." En tilsvarende konklusjon ble trukket av firmaet Teleplan A/S, som ble oppnevnt som sakkyndig av retten. Dette firmaet kunne heller ikke klare å etablere mobildekning fra det samme området. Når konklusjonen fra de tekniske analysene så entydig gikk ut på at det ikke var mulig å etablere kontakt via Eg-A fra åstedet, blir det problematisk å hevde at elektroniske trafikkdata i dette tilfellet utgjorde et "viktig bevis" i saken.

3.0 KOMMUNIKASJONSKONTROLL OG STYRKING AV POLITIET

EFN er ikke i tvil om at elektroniske trafikkdata generelt er viktig for oppklaring av kriminalsaker der individer som begår kriminelle handlinger benytter seg av de ulike former for elektronisk kommunikasjon, men vi finner det ikke godtgjort at dette i seg selv er et tungtveiende argument til fordel for hverken Datalagringsdirektivet eller andre tiltak som på liknende vis utsetter hele befolkningen for tvungen registrering og lagring av opplysningene om deres bevegelser. Her ser vi dertil at de eksemplene som i departementenes høringsnotat trekkes frem for å underbygge argumentasjon til fordel for datalagring, slett ikke underbygger de konklusjoner man fra departementenes side må ha tenkt seg å komme frem til. Tvertimot, disse sakene ble jo nettopp oppklart UTEN at DLD er en del av norsk lov!

Vidar Refvik sier videre i ovennevnte innlegg:

For all kriminalitet begått via nettet er trafikkdata helt avgjørende, siden både lovbruddet og mulighetene for oppklaring er basert på elektroniske spor, eksempelvis datainnbrudd, trusler om skoleskyting og spredning av overgrepbilder av barn.

Vi er ikke uenige i Refviks oppfatning om at trafikkdata generert fra bruk av nettet er avgjørende for kriminalitet begått via nettet. Det må imidlertid innvendes at man begår en logisk feilslutning, dersom noen av den grunn konkluderer med at lagring av samtlige borgers trafikkdata derfor er nødvendig for kriminalitetsbekjempelsen.

Vi vil understreke vår oppfatning om at det vil være meget å hente dersom politiet gis ressurser, utstyr og personell samt opplæring av personellet til å fylle sine oppgaver etter en grundig gjennomgang av hva som konkret er flaskehalsene, og at det er et utpreget

blindspor med uakseptable følger for rettsstaten å gå inn for en ytterligere eskalering av det elektroniske kontrollnivå overfor befolkningen som helhet.

3.1 MÅLRETTET ETTERFORSKNING OG MER RESSURSER

Det har lenge vært en kjent sak at politiet i Norge har klaget over at de opplever å mangle ressurser til å utføre sin oppgave. Gitt at dette er tilfelle, mener vi at det her er en bedre måte å bruke samfunnets midler på enn å tildele store ressurser til lagring og senere analyser av opplysningene om alle innbyggers bruk av elektroniske kommunikasjonsmidler. Det er teknisk få problemer forbundet med å iverksette overvåkning av spesifikke individers trafikkdata og øvrige kommunikasjonsdata, og dersom enkelte av politiets representanter påstår at de trenger tilgang til hele befolkningens data for å gripe inn mot det mindretall som begår kriminalitet må resten av samfunnet bare si i fra at denne påstanden er uholdbar. Her er stikkordet spesifisitet.

For å påvise, avdekke og etterforske kriminalitet trengs rutiner, utstyr og prosedyrer som retter seg spesifikt mot kriminell aktivitet, og det kreves kompetanse. Det kreves også tilstrekkelig personell. Elektronisk registrering av alles bevegelser kan aldri erstatte et velutdannet politi som er til stede der behovet oppstår. Datalagringsdirektivet blir i dette perspektivet et uheldig politisk valg, en feil strategi i en knapp ressursituasjon, og en meget dårlig erstatning for det politiarbeidet som også i den elektroniske tidsalder er og fortsatt vil være nøkkelfaktoren for å etterforske og oppklare kriminalitet. Å utsette hele befolkningen for omfattende lovpålagt overvåkning som fjerner muligheten til å bevege seg fritt er en strategi som må avvises i en rettsstat. Er man ikke mistenkt for noe kriminelt, skal ens bevegelser heller ikke registreres.

4.0 DATALAGRINGS-DIREKTIVET INNFRIR IKKE DE OPPGITTE FORMÅL

Et spørsmål i tilknytning til datalagringens effektivitet til sine angitte formål er hvorvidt de kriminelle faktisk kommer til å fakkas i større omfang, dersom DLD innføres i Norge. Mye tyder på at tilhengerne av dette direktivet gjør seg overdrevne forestillinger om hvor virksomt det kan være i kampen mot kriminalitet. En overdreven tro på datalagring som virkemiddel har gjort at det i den politiske debatten rundt DLD er blitt malt skremmebilder som at Norge kommer til å bli en "frihavn for kriminelle" dersom vårt land ikke innfører direktivet.

Det er grunn til å tro at ressurssterke kriminelle vil kunne unndra seg det "garn" som Datalagringsdirektivet representerer. I så måte finnes det en rekke "frihavner". Eksempler på dette er:

- Anonyme mobilabonnementer kjøpt fra utenlandske tilbydere.
- De fleste former for bredbåndstelefonti/VoIP (Skype og liknende) som leveres av andre tilbydere enn brukerens primære telekom-leverandør.
- Ulike former for gratis web-baserte e-posttjenester som skjer fra tjenesteleverandører i utlandet og som ikke krever noen for identifisering av brukeren (eks. HotMail, Live og Gmail).
- Ulike former for meldings og chattetjenester over Internett (IRC, MSN, AIM, Spin). I tillegg til dedikerte chattetjenester har nesten alle online-spill en privat chattemodus som kan benyttes dersom man ønsker å kommunisere uten å bli overvåket.
- Nesten alle elektroniske oppslagstavler og sosiale nettsteder (Facebook, Orkut, Biip) har en funksjon for å sende private meldinger mellom individer og grupper.
- 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).

Vi må kunne gå ut i fra at kriminelle vil lære og tilpasse seg politiets metoder. I et scenario hvor lagring blir innført, vil kriminelle trolig raskt tilpasse seg og i stedet velge kommunikasjonsformer der data ikke blir lagret.

Disse "hullene" i overvåkningens nett kan muligens fremstå som mangler som bør utbedres. Problemet med en slik "utbedring", er for det første at en storstilt innsats for eliminering av slike "huller" i systemet vil gjøre datalagringens udemokratiske natur enda tydeligere. Eksempelvis vil man for å fjerne muligheten til å være anonym på nett via Internett-kafeer måtte tvinge folk som bruker slike til å legitimere seg før de kunne få tilgang til nettverkene. Dersom man vil fjerne muligheten til å benytte åpne trådløse nett, måtte man enten gjøre slike nett illegale, eller man vil måtte holde eieren av nettverket ansvarlig for hva andre foretar seg på hans eller hennes eget nett. Dersom opplysningene om bruken av web-baserte meldingstjenester, sosiale nettverk og oppslagstavler skulle lagres, måtte slike enten forbys, eller det måtte etableres en form for digitalt identifikasjonssystem som gjorde at man avslører sin identitet i langt større grad på nettet. Skal man forhindre bruk av anonymiseringstjenester, så blir man nødt til å forby dem og for sikkerhets skyld gjøre det straffbart å unndra seg registreringen. Slike tiltak har en ubehagelig smak av samfunnsformer og regimer vi ikke liker tanken på å sammenliknes med, og de ville ganske sikkert bli en politisk belastning ved å gjøre det enda tydeligere at myndighetene for å oppfylle sine kontrollambisjoner går langt over rimelige grenser for hva slags inngrep i folks privatliv som kan tåles i en rettsstat.

5.0 FALSKE POSITIVE OG KOMPLEKSITET VED DATABEREGNINGER

Datalagringsdirektivet er ugjennomførbart pga. mengden med "falske positive" som vil genereres, og pga. uoverstigelig beregningskompleksitet ved lovpåbudte forsøk på å bevise uskyld i henhold til Straffeprosessloven § 215 a.

I gjennom søk av trafikkdata vil man møte grunnleggende begrensninger for hva en datamaskin kan beregne når man sammenstiller hvilke kontakter personer har hatt. Det er også solid med feilkilder i moderne kommunikasjonssystemer. Disse iboende begrensningene i metodene som brukes for å sammenstille data, gjør at Datalagringsdirektivet teknisk sett har begrenset verdi som etterforskningsmetode eller strategi. Funksjonelt krever Datalagringsdirektivet lagring av alle trafikkoppkoblinger. Alle oppkoblingsdata blir lagret, det være seg mellom menneske og maskin eller mellom maskiner. Man får et gigantisk beregningsproblem, når man vil finne "kriminelle nettverk" blant alle mulige uskyldige oppkoblinger.

Dette er langt mer komplekst enn å finne en nål i en høystakk. Man skal finne synåler i mange forskjellige høystakker, og det skal gjøres uten at man forveksler dette med knappenåler. Også høystakkene er forskjellige. Selv om man besitter helt korrekt søkemetode for å finne de som har hatt kontakt, og at alle trafikkdata er korrekte, Selv om man forestiller seg en helt korrekt søkemetode, så vil det være praktisk umulig å levere treffsikker beregning av hvem som inngår i et kriminelt nettverk.

5.1 FALSKE POSITIVE

Siden det ikke er mulig å manuelt kombinere alle trafikkdata for å søke fram kommunikasjon man mistenker er gjort i kriminell sammenheng, må man ty til søkemetoder som har iboende feilkilder. Det hører med at det uansett er betydelige feilkilder i trafikksystemer på Internett. Selv med riktige søkemetoder, vil man få mange feil. Dette går på alt fra klokkesynkronisering og

pakketap til feiloppkoblinger og feil i inndata. Men la oss gå ut fra at man bruker metoder som kutter i svingen, og man slipper å kombinere alle trafikkdata. Man kan "gjette" seg fram til et resultat ved å snevre inn søkene. Problemet er at dette fortsatt gir altfor stor hyppighet av falske positive til å gi pålitelige resultater. De man er ute etter å ta forsvinner i mengden med falske positive.

For å eksemplifisere problemet med falske positive, henter vi et eksempel fra legenes virkelighet med bekjempelse av HIV. Dette fordi Datalagringsdirektivet begrunnes ut fra å bekjempe alvorlig kriminalitet. Humant immunsviktvirus (HIV) er en alvorlig diagnose som kan føre til livstruende opportunistiske infeksjoner fordi immunforsvaret svikter. I dag finnes rundt 3000 HIV-diagnostiserte personer i Norge. Sykdommen er så alvorlig at det kunne være fint å gjennomføre en HIV-test på den voksne befolkningen. Så hvorfor gjør man ikke det?

Problemet er feilkildene. En HIV-test har feil som gjør at den gir falske positive. Selv om testen skulle være meget god med bare noen prosent feil, står man fort i fare for å gi 50 000 friske personer en mulig HIV-diagnose. Dette er mange ganger mer enn de rundt 300 personene som blir diagnostisert med HIV hvert år. Legene ville ikke fått stort annet å gjøre med denne sykdommen enn å unnskyldte feildiagnoser, og trippelsjekke prøve-resultatene. Dette ville kreve enormt med ressurser, noe som ville gå ut over personer med andre sykdommer slik at disse ble dyttet bak i køen.

Hadde myndighetene pålagt HIV-test av alle, ville problemene det skapte vært mange ganger større enn problemene som uklarhetene rundt svineinfluensaen skapte. Gir man politiet adgang til å krysskoble trafikkdata vil man få samme problem med falske positive som med det tenkte eksemplet med HIV. Søkemetodene vil produsere solide mengder falske positive. For å finne de skyldige, må man lete etter noen få synåler i haugevis av knappenåler, der knappenålene ser ut som synåler. Vi snakker ikke om en haug med knappenåler, men store mengder trafikk- og lokasjonsdata. Dette er personer man tror har hatt kriminell kontakt, men hvor mange er uskyldige. De relativt sett ganske få skyldige derimot, blir i en lang rekke tilfeller borte i mengden av falske positive. Det er bare de man på forhånd har konkret mistanke mot, som man med sikkerhet kan ta. Men, man trenger ikke Datalagringsdirektivet for å ta de man har en skjellig grunn til å mistenke. Datalagringsdirektivet er et slag i luften.

Problemet med falske positive gjør altså slik såkalt "data mining"[9] (strategisk informasjonsanalyse, mønstersøk i store datamengder) like lite meningsfylt som å kjøre HIV-testing av hele den voksne befolkningen. Tiltaket som tilhengerne av DLD argumenterer for er helt feilslått, i forhold til de kriminelle som man ønsker å ta. Dette med falske positive alene burde være nok til å erkjenne at man ikke bør bruke de lagrede dataene til data mining, slik enkelte har tatt til ordet for. Man bør heller konsentrere innsatsen til situasjoner der man har konkret mistanke om at noe kriminelt har skjedd. Her har politiet allerede gode verktøy, men mangler ressurser og personell til å ta dem i bruk.

5.2 PLIKT TIL Å LEGGE FREM DOKUMENTASJON AV USKYLD

Det er også politiets oppgave å legge frem data og dokumentasjon som taler for den tiltaltes uskyld i en straffesak der trafikkdata brukes som bevis, slik Straffeprosessloven § 215 a legger opp til.

Dessverre kommer politiet i den situasjon at de velger metoder som kun peker mot skyld, uten å kunne fremlegge data og dokumentasjon som peker mot uskyld (noe som skyldes beregningskompleksitet, feil i datasystemene, og falske positive).

Straffeprosessloven forutsetter at politiet og påtalemakten også skal dokumentere det som taler for tiltaltes uskyld, dette for å unngå justismord[10].

5.3 KONKLUSJON PÅ FALSKE POSITIVE OG DATABEREGNINGER

Når det gjelder Datalagringsdirektivet har enkelte politikere og jurister vært i stand til å frembringe en plausibel fortelling, med indre sammenheng og som virker representativ i henhold til våre klisjeer og fordommer, uten at dette stemmer ifølge kompetente men mindre fargerike fagfolk som heller angir statistiske forhold og matematiske kjensgjerninger.

På den måten har en gal oppfatning festet seg i enkelte kretser, nemlig at data mining vil være virksomt. Denne feiloppfatningen har da kommet på bekostning av mer faglig holdbare forutsigelser som har et bedre matematisk og statistisk belegg. Vi kan ikke med sikkerhet vite om et nettverk av kommunikasjon mellom personer skyldes kriminell aktivitet, feil i dataene eller falske positive der man har stort innslag av uskyldig kommunikasjon.

De feilaktige forestillinger som tilhengere av data mining har argumentert ut i fra, vil med stor sikkerhet føre til at mange uskyldige kommer i søkelyset og i verste fall blir siktet uten grunn. Når det gjelder data mining er vi for vår del sikre i vår sak. Det er urealistisk å presist avdekke kriminelle nettverk blant alle uskyldige, dette grunnet falske positive og stadig økende beregningskompleksitet ved søk i enorme og økende mengder trafikkdata. Vi slår fast at det er et kompetanseproblem dersom noen mot naturvitenskapelige kjensgjerninger argumenterer for hva som er urealistisk. I tillegg kommer fortsatt alle de andre relevante innvendingene mot Datalagringsdirektivet, som hver for seg burde gjøre et slikt overvåkningstiltak uaktuelt.

Mange tilhengere av DLD påstår at det ikke er noen tvil om at DLD vil gjøre politiets arbeid lettere. EFN finner det relativt åpenbart at det kan gjøre politiets arbeid vanskeligere. Når man skal finne nåla i høystakken, hjelper det ikke å spa på mere høy.

Datalagring vil koste 200-400 millioner kroner i året (ifølge utenriksminister Jonas Gahr Støre som gjengir tall fra IKT Norge). Hadde man istedet brukt 20 millioner på å styrke Kripos med personell og ressurser til målrettet spaning og kommunikasjonskontroll med mistenkte, ville man kommet mye lengre i etterforskning av alvorlig kriminalitet, enn man vil gjøre med trafikkovervåking av hele det norske folk for anslagsvis 200-400 millioner kroner i året på noe som har liten eller ingen virkning.

Problemet med argumentasjonen for DLD er at Arbeiderpartiet og Kripos hevder de vil trenge overvåkning av alle for å sannsynliggjøre kriminell kontakt, der argumentet som blir brukt viser at man klarer seg innenfor dagens lovverk. Dagens lovverk gir alle nødvendige trafikkdata til Kripos når de etterforsker mistenkte for alvorlig kriminalitet, slik som i Nokas- og Baneheia-sakene.

6.0 DATALAGRINGS DIREKTIVET GIR ØKT UTRYGGHET I SAMFUNNET

6.1 ALVORLIG TRUSSEL MOT KILDEVERNET OG VARSLERE I SAMFUNNET

Høringsnotatet sier på side 50 følgende:

Selv om en innføring av Datalagringsdirektivet vil kunne medføre enkelte utfordringer for kildevernet, mener departementene før høringen at det ikke vil

innebære uforholdsmessige inngrep. Departementene ser at spørsmålet kan problematiseres, og ber om høringsinstansenes syn på dette.

Departementene mener altså i utgangspunktet at Datalagringsdirektivet ikke vil medføre uforholdsmessige inngrep for kildevernet.

En udiskutabel konsekvens dersom Datalagringsdirektivet innføres, er at det vil bli langt enklere for politiet å komme til kunnskap om hvem som har kommunisert med hvem i lang tid etter at kommunikasjonen for eksempel via telefon eller e-post fant sted. Den som enøyd fokuserer på muligheten til å fukke kriminelle overser at det dermed også blir svært mye mer krevende for pressen å beskytte sine kilder og informanter. Når en journalist har hatt e-postutveksling eller telefonkontakt med mennesker som er i politiets søkelys, lagres opplysningene om at denne kontakten har funnet sted. Når politiet får ut disse dataene, er det lett å gå videre og finne ut hvem som har hatt kontakt med hvem i forbindelse med spesielle saker og miljøer. På denne måten øker risikoen for både journalist og kilde(r), og i de tilfeller hvor samfunnets tjenere er utro sådanne vil varslere og informanter leve et mye farligere liv med en slik langtidslagring som Datalagringsdirektivet krever.

Det kan tas for gitt at kriminelle personer og organisasjoner vil være svært interessert i å få tak i det aktuelle materialet, eksempelvis for utpressingsformål og for å få tak i hvem som har lekket opplysninger om kriminell aktivitet og kriminelle forbindelser.

Hensynet til pressens kildevern er etter vår oppfatning så viktig at det er grunnlag for å si at Datalagringsdirektivet, gjennom å vanskeliggjøre ikke-sporbar kommunikasjon vil gjøre tilværelsen usikker for varslere og informanter, og også på denne måten vil bidra til å redusere trykningen i samfunnet.

6.2 DATA PÅ AVVEIE GIR ENDA MER UTRYGGHET

Det er ikke en forutsetning at dataene skal komme utedkommende i hende, for at følgene for en rekke uskyldige mennesker skal bli svært ubehagelige over tid. Likevel er det grunn til å understreke at det aldri har eksistert og heller aldri vil komme til å eksistere systemer skapt av mennesker som gir 100% sikkerhet. Vi vil advare mot at diskusjonen om Datalagringsdirektivet blir konsentrert om "sikker lagring". Noe slikt eksisterer ikke og er en teknisk umulighet. Dessuten er det utvilsomt at i et scenario der det lagres informasjon om hvem som har hatt kontakt med hvem og når og også hvor mennesker befant seg på et bestemt tidspunkt, vil en lang rekke etater, organisasjoner og mennesker med mer eller mindre gode hensikter etterhvert ønske å få tak i disse opplysningene.

6.3 PRIVATISERING AV POLITIOPPGAVER

Datalagringsdirektivet pålegger private aktører å samle opplysninger med det formål at dataene inn i fremtiden hypotetisk skal kunne bli til nytte i kriminalitetsbekjempelse. Dette er et helt nytt prinsipp, og innebærer at man beveger seg farlig nær en privatisering av politioppgaver som bidrar til ytterligere å svekke rettsikkerheten. Dette ville bli enda mer akutt dersom vi i et slikt scenario fikk private firmaer som spesialiserte seg på datalagring med det nevnte formål. I Europa finnes nå eksempler på at private firmaer går ut med at lagring av folks trafikkdata på vegne av staten er et kommersielt satsningsområde. Etter vårt skjønn innebærer kommersielle interesser i slik lagring en ytterligere økning av risikoen for data på avveie, da enhver sentralisert lagring av befolkningens data vil være et uhyre attraktivt mål for kriminelle. Dessuten er dette enda et eksempel på hvordan overdreven kontroll i samfunnet fører til negative effekter. En sentralisert lagring i det offentlige regi ville på den annen side i enda større grad fremstå som en

stor honningkrukke for kriminelle og for utro tjenere, og dessuten synliggjøre myndighetenes kontrollvilje og ansvaret bak overvåkningsambisjonene, og utgjøre en større politiske belastning. Uansett hvordan man tenker seg å gjennomføre datalagringen blir det galt.

7.0 DLD I STRID MED ANNEN LOVGIVNING OG RETTSPRINSIPPER

7.1 GRUNNLOVEN

Privatlivets fred har en relativt svak beskyttelse i norsk lov, også hva angår Grunnloven, i alle fall når det gjelder de faktorene som i dag etter EFNs mening er noen av de største truslene mot folks privatliv og personvern. I Grunnloven finnes riktignok en viss beskyttelse i og med paragraf 102, som slår fast at "Hus-Inkvisitioner maa ikke finde Sted, uden i kriminelle Tilfælde". Denne bestemmelsen kunne imidlertid ikke forhindre at det norske Stortinget i 2005 vedtok et tillegg i Politilovens paragraf 17d om vilkår for bruk av tvangsmidler i forebyggende øyemed. Det nye var at loven åpnet for at Politiets sikkerhetstjeneste fra da av legalt kunne iverksette blant annet romavlytting, telefonavlytting, brev- og e-postkontroll, uten skjellig grunn til mistanke om noe kriminelt som forutsetning. Loven ble møtt med sterk kritikk, blant annet av førstestatsadvokat Lasse Qvigstad, som i sin kritikk trakk frem Grunnlovens paragraf 102 som en bestemmelse han mente burde vært med i avveiningene da Politiloven ble revidert i 2005.

Man skulle også kunne tenke seg at inngrep som Datalagringsdirektivet kan vurderes i lys av det absolutte prinsippet om at husundersøkelser ikke må finne sted uten i tilfeller av kriminalitet, særlig ettersom elektronisk overvåkning og kommunikasjonskontroll med langvarig innsamling av private opplysninger og overskuddsinformasjon kan sies å være "vesentlig mer inngripende" enn en målrettet ransakning. Dette er i det minste hva Lasse Qvigstad mente og ga uttrykk for i en kronikk i Aftenposten[11] den 28.04.2008. Da skulle man kanskje kunne forvente at den normative retningslinje vedrørende privatlivets fred som unektelig ligger i Grunnlovens paragraf 102 også kunne være med i bildet når Datalagringsdirektivet vurderes.

Her kan også nevnes at justisminister Knut Storberget fortjenstfullt i juli 2009 ga direkte ordre til Politiets sikkerhetstjeneste (PST) om stans i all avlytting av private hjem i tilfeller der det ikke er bevist at noe kriminelt er skjedd[12]. Ordlyden gikk ut på "straks å suspendere eventuelle pågående forebyggende romavlyttingssaker av privat bolig som det er gitt tillatelse til å iverksette og heller ikke fremme nye begjæringer om bruk av slik metode". Bakgrunnen for justisminister Storbergets ordre, var at det regjeringsoppnevnte Metodekontrollutvalget fastslo at den daværende praksis som PST tillempet faktisk var i strid med Grunnloven og dermed helt ulovlig.

Vi ser altså at samfunnet i så stor grad finner at inngrep i private hjem uten at noe kriminelt er skjedd er uakseptabelt at landets justisminister stopper en praksis som PST allerede hadde innarbeidet. Da synes det sterkt urimelig å gå inn for en pliktmessig lagring av opplysningene om samtlige borgeres elektroniske kontakter og bevegelser, når slik lagring skjer med den hensikt å legge til rette for mulig etterforskning. EFNs syn er at på samme måte som private hjem bør være omfattet av privatlivet inntil noe kriminelt har blitt påvist, bør også menneskers private kommunikasjon og nettbruk være noe som tilhører privatlivet inntil noe kriminelt er blitt påvist. Vi konstaterer også at eksemplet viser hvorfor det aldri kan godtas at statens maktapparat får definere rammene for sin virksomhet. Politiet er statens maktapparat, og i en rettsstat skal ikke politiet legge premissene for sin oppgave. Her synes det å være behov for en tydelig grenseoppgang.

7.2 METODEUTVALGET OM DATAAVLESING

Metodeutvalget slår fast[13] at det ikke kan plasseres utstyr for å gjennomføre dataavlesing hos

folk flest. Dette i følge avsnitt 2.12 Dataavlesing (NOU 2009:15):

Når det gjelder dataavlesing i forbindelse med hemmelig ransaking og beslag innebærer forslaget at ransaking kan skje uten politiets fysiske tilstedeværelse. Slik gjennomføring vil kunne være mindre integritetskrenkende enn tradisjonell hemmelig ransaking, som krever at politiet skaffer seg fysisk tilgang til anlegget, typisk ved innbrudd i en privat bolig. Utvalget finner ikke at det foreligger tilstrekkelige tungtveiende grunner til å åpne for at retten kan gi tillatelse til gjentatt eller fortløpende hemmelig ransaking.

De samme utfordringene som gjør seg gjeldende på etterforskningsstadiet med hensyn til den teknologiske utvikling, gjør seg også gjeldende på forebyggingsstadiet. Utvalget tilrår derfor en tilsvarende utvidelse for PSTs forebyggende tvangsmiddelbruk, likevel slik at utvalgets flertall mener Grunnloven § 102 innebærer at det på det forebyggende stadiet ikke kan gis adgang til å gå inn i privat bolig for å plassere utstyr for å gjennomføre dataavlesingen.

Metodeutvalget foreslår også å frata muligheten Post- og teletilsynet har til å pålegge teletilbydere å utlevere trafikkdata til politiet. Vi viser til kapittel 2.10 om Innhenting av trafikkdata (NOU 2009:15):

I dag er den enkelte teletilbyders praksis 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, og det foreslås derfor at innhenting bare skal kunne skje etter beslutning om utleveringspålegg fattet av retten, eventuelt i kombinasjon med utsatt underretning om dette. Fordi Post- og teletilsynet som regel vil ha mangelfull tilgang til faktum i saken og fordi tilsynets vurdering ikke anses nødvendig når utlevering etter utvalgets forslag uansett skal besluttes av domstolen, foreslås at Post- og teletilsynet fratras denne oppgaven. Dette foreslås gjort ved at trafikkdata unntas fra teletilbyders taushetsplikt etter Ekomloven § 29 dersom det foreligger beslutning om utleveringspålegg.

Metodeutvalget har følgende konklusjon om Grunnloven § 102 og avvergende og forebyggende tvangsmiddelbruk:

Ut fra flertallets forståelse av Grunnloven § 102 foreslås det å utvide forbudet mot ransaking av private hjem i politiloven § 17d til også å gjelde romavlytting og innbrudd (i forbindelse med dataavlesing) i privat bolig. Mindretallet går derimot inn for at alle metodene i politiloven § 17d skal være tillatt for forebyggende formål også i private boliger.

7.3 EMK OG DLD

En direkte relevant bestemmelse i forhold til spørsmålet om Datalagringsdirektivet er Den europeiske menneskerettighetskonvensjon (EMK), og da især denne konvensjonens artikkel 8. EMK er innlemmet i norsk rett, gjennom menneskerettsloven av 1999, og vi er dermed bundet av den, spesielt når menneskerettighetskonvensjonens bestemmelser skal gis forrang dersom det oppstår motstrid til andre deler av norsk lovgivning.

EMK artikkel 8 sier følgende[14]:

Art 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.

Det synes ikke tvilsomt at den registreringen og lagringen som Datalagringsdirektivet krever, bryter mot artikkel 8.1. Hva som da blir spørsmålet, er hvorvidt vilkårene i artikkel 8.2 kan sies å være oppfylt. Kjernen her blir nødvendighetskravet "er nødvendig i et demokratisk samfunn...". I den juridiske fortolkning er dette et absolutt krav om at tiltaket må springe ut av en tvingende nødvendighet. På hvilken måte kan tiltakene i DLD sies å være tvingende nødvendig i den norske rettsstaten?

Departementenes høringsnotat er ikke i stand til å peke på at noen nødvendighet foreligger, og en proporsjonalitetsvurdering i det norske samfunnet tilsier etter vår mening ikke at det på noe vis foreligger en situasjon som gjør det berettiget å bryte mot artikkel 8.1, men det er hva en massiv lagring av elektroniske kommunikasjoner og elektroniske bevegelser gjør. EFN kan vanskelig se noe annet enn at Datalagringsdirektivet innebærer et klart brudd mot de relevante bestemmelser i EMK. Dette poenget blir spesielt tydelig ettersom det foreligger rettsavgjørelser i Europa som konkluderer med at bare registrering og lagring av slike data som det er snakk om i regi av offentlig myndighet har direkte inngripende virkning på individets privatliv, og dette uavhengig av hvorvidt dataene senere brukes. Uten at tvingende nødvendighet foreligger, er det mer enn tvilsomt å introdusere denne typen invaderende tiltak overfor hele befolkningen. Her foreligger ingen forholdsmessighet mellom tiltaket og følgene ved at alle borgeres rett til privatliv og privat kommunikasjon overkjøres.

7.4 USKYLDSPRESUMPSJONENS PRINSIPELLE OG PRAKTISKE RELEVANS

I en rettsstat er et annet viktig prinsipp uskyldspresumpsjonen - en borger har rett til å bli betraktet som uskyldig inntil noe annet er bevist gjennom forsvarlig rettsavgjørelse. Dette impliserer at det ikke er borgerens uskyld som skal bevises dersom denne blir gjenstand for rettslig forfølgelse, det er vedkommendes skyld som må bevises for at straff eller andre former for reaksjon skal kunne idømmes. Siden den ekte rettsstaten må ha som et ufravikelig prinsipp at det alltid og bare er skylden som skal bevises, er det oppsiktsvekkende at det i departementenes høringsbrev legges vekt på å argumentere for Datalagringsdirektivet ut fra at datalagring også omfatter bevismateriale i data som taler for siktedes uskyld. Vi frykter at vektleggingen reflekterer en økende tendens til å umerkelig gli vekk fra uskyldspresumpsjonen, ved å introdusere resonnementet om at en siktets uskyld skal være gjenstand for bevisførsel. At det fra en del hold er blitt argumentert til fordel for lagring av den type data som det her er tale om gjennom at angivelig behov for å bevise uskyld, er i realiteten enda et moment som taler for at dette er en vei vi bør unngå å gå inn på. Igjen må vi bare henviser til at dersom man ikke er under mistanke om noe kriminelt, så skal man få lov til å bevege seg og kommunisere med hvem man vil uten at dette skal kunne spores i ettertid. Slik må det være i en rettsstat, det er politistaten som krever å kontrollere alle.

8.0 SAMMENFATNING OM TILLIT OG KONTROLL, MAKTBALANSENS BETYDNING, OG KONKLUSJONEN PÅ EFN SIN HØRINGSUTTALELSE

8.1 KONTROLLSAMFUNNETS NEDBRYTENDE SOSIALE EFFEKTER

I et scenario der myndighetene gjør krav på å gjøre alle borgere sporbare ved å gjennom lov hindre dem i å kommunisere sporfritt, og i verste fall kartlegge de fleste av deres elektroniske og fysiske bevegelser, vil tillitsforholdet mellom myndigheter og borgere svekkes. Dette er en effekt som er umulig å unngå dersom noen krever å få vite hvem du har kontakt med eller hvor du befinner deg. Om staten med loven i hånd gjør krav på å vite hvem du har kontakt med og/eller hvor du beveger deg, er dette derfor uforenlig med tillit og jevnbyrdighet. Det er utvilsomt at effekten blir at den enkelte borgers samfunnsbevissthet og vilje til å være en "god" samfunnsborger da vil reduseres, fordi den som blir møtt med mangel på tillit gradvis mister respekten for den som viser mistillit.

Her er det nødvendig å ha en realistisk holdning. Det hjelper ikke å forskjønne et slikt scenario ved å si at "det er ikke overvåkning, materialet skal bare benyttes hvis du gjør noe galt". Overvåkning er selvsagt en innsamling av opplysninger. Videre er det nytteløst å si at "materialet skal bare benyttes hvis du gjør noe galt", ettersom det i en rettsstat ikke skal samles inn informasjon om hva borgerne foretar seg i etterforskningsøyemed i forbindelse med kriminalitet. Å registrere og lagre opplysninger om hva mennesker gjør for å kunne bruke det "i tilfelle" man skulle gjøre noe kriminelt, eller noe som staten anser det som nødvendig å reagere mot, innebærer en uttalt men bakenforliggende formodning om at vi alle er potensielle forbrytere som må kontrolleres. Mennesker er ikke dummere enn at de forstår dette, og instinktivt vil de aller fleste mennesker som har et modent selvbilde miste tilliten til de som møter dem med mistro og kontroll.

Imidlertid er det ikke bare tillitsforholdet mellom staten, myndighetsorganene og borgerne som vil ta skade av at staten gjør krav på å få mulighet til innblikk i menneskers privatliv og kontrollere hva de foretar seg. **Når det fra enkelte hold er blitt hevdet at det er en motsetning mellom det individuelle personvernet og samfunnets behov, så bygger dette synet på en feilslutning og en manglende forståelse for betydningen av sporfri kontakt mellom mennesker. Dersom det skal være slik at man ikke kan ha kontakt med andre mennesker uten at det skal kunne spores i lang ettertid, kan følgen bli en høyere terskel for "vanlige mennesker" mot å ha kontakt med individer som er blant de sosialt belastede i samfunnet. Resultatet kan da være at de vanlige borgerne blir mer reserverte mot å vise sosial aksept overfor tidligere straffedømte, eller andre mennesker som av en eller annen årsak betraktes som "tvilsomme" eller "suspekter". Det kan bidra til øke risikoen for at marginaliserte grupper i samfunnet kan bli mer isolert og utvikle destruktive holdninger og aggressiv atferd, dersom vanlige borgere tar enda mer sosial avstand fra dem fordi de frykter at de selv kan komme i mistankens søkelys ved å ha kontakt med mennesker eller grupper av mennesker som kan antas å være under oppsikt.**

Privatliv, i betydningen mulighet til å etablere kontakter med medmennesker uten at staten skal ha innsyn i hva som har skjedd, er også en nødvendighet for å etablere genuine vennskap og nære relasjoner. Det er i privatsfæren at den enkelte møter sine medmennesker i fortrolighet og lærer seg å bryne egne følelser, oppfatninger og holdninger mot den andres. Derfor er det uomgjengelig nødvendig at det private rom får lov til å være nettopp privat, ved at myndighetene holdes unna privatsfæren. **I et fritt samfunn må det være slik at hvem du har kontakt med og er sammen med tilhører privatlivet. Hvis myndighetene etter nærmere bestemte regler har muligheten til å nøste opp dine kontakter og omstendighetene rundt dem i lang ettertid, så ødelegges dette private rommet i stor grad.** Bare gjennom å dele ditt sinns hemmeligheter med Den Andre kan det enkelte individ selv utvikle den tilliten til seg selv, som deretter også omfatter de andre, og som gjennom personlig følt erfaring gjør individet til en altruistisk samfunnsborger med evne til omtanke og solidaritet. **Et privatliv som beholdes**

privat er således også en nødvendighet for å utvikle de personlighetsegenskapene som gjør oss i stand til å knytte bånd til andre mennesker, og å være en "god" samfunnsborger.

8.2 HVORFOR ER MAKTBALANSEN SÅ VIKTIG?

Nøkkelen til en forståelse av hvorfor balansen mellom myndighetenes makt og borgernes makt er en så avgjørende faktor i demokratiets overlevelse, ligger i å forstå at det politiske system vi kaller "demokratiet" ikke er og aldri kan være en vaksine mot at noe samfunn utvikler seg fra å være folkestyrt og preget av menneskers medbestemmelse over eget liv og egen hverdag til å bli autoritært og begrensende for menneskenes bevegelsesfrihet, valgmulighet og i siste instans også selve den subjektive og objektive tryggheten i hverdagen. Alt som forrykker maktbalansen for meget i borgernes disfavør, setter demokratiet og rettsstaten i fare.

Å gjøre alle borgere sporbare i deres kommunikasjon, innebærer å gi myndighetene en tidligere ukjent grad av kontroll med hva folk flest foretar seg, og slik kunnskap om enkeltindividene vil gi myndighetene et uforholdsmessig maktmiddel. Menneskers kontaktmønster forteller veldig mye om hvem man er, og det er et stort inngrep i privatlivet dersom noen gjør krav på å få kartlegge det. Ettersom de aller fleste av oss har eller vil komme til å bære mobilt kommunikasjonsutstyr, vil den enkeltes fysiske posisjon og tilholdssted ofte kunne fastslås med ned til noen hundretall meters nøyaktighet. Dermed er også retten til anonym ferdsel truet.

Et negativt menneskesyn som går ut på at "du må kontrolleres, for det tilfelle at du gjør noe galt" er premissleverandør for at en slik kontroll er nødvendig. Dessverre er et slikt menneskesyn selvoppfyllende, i den forstand at mennesker gjerne lever opp til de forventninger som stilles til dem. **At et lands myndigheter gjennom lovverk og ledsagende praksis formidler en slik mangel på tillit at de gjør krav på å gjøre alle mennesker sporbare, må føre til en gradvis, umerkelig, men uunngåelig ødeleggelse av tillitsforholdet mellom myndigheter og borgere. Tragisk nok er det sannsynlig at den tradisjonelle aktelsen for lov og rett er noe av det første som går tapt hvis man ikke nå snur i tide. Legalitet skaper aldri i seg selv legitimitet.** Fenomener som Datalagringsdirektivet er en av et stort antall faktorer i samtidens dagligliv som setter privatlivet og personvernet under press, så det er mye å ta tak i for de som ønsker å forsvare vanlige menneskers rett til å ha sitt privatliv i fred. Hvilket bare er nok et moment som tilsier at vi gjør klokt i å si nei til Datalagringsdirektivet.

De politiske krefter som har ønsket overvåkning av samtlige av statens innbyggere har hevdet at den er nødvendig for tryggheten i samfunnet, og de har videre hevdet at det faktum at vi lever i en globalisert verden der også kriminaliteten overskrider landegrensene innebærer at omfattende kontrolltiltak som Datalagringsdirektivet er blitt nødvendige. **Vi mener derimot at nettopp globaliseringen kanskje sterkere enn noen annen faktor gjør at personvernets og privatlivets interesser for enkeltindividet sammenfaller med hele samfunnets interesser, fordi muligheten for hver enkelt til å beskytte privatsfæren gjennom å etter eget valg kunne bevare sin kommunikasjon og sine bevegelser privat er en sentral faktor for å skape trygghet.**

Det er nettopp i en globalisert og derfor kompleks og risikofylt verden at de frie borgere mer enn noensinne har behov for mulighet til selvvalgt anonymitet og rett til den kommunikasjonsfriheten som er en av de viktigste kjennetegnene på et fritt samfunn. Dette er et ansvar som den enkelte i siste instans må få lov å ivareta, ved at frie borgere som ikke er under mistanke eller etterforskning for noe kriminelt i størst mulig utstrekning får lov til selv å trekke grensene for sitt privatliv og sine bevegelser.

Et viktig stikkord her er begrepet "rettsstat". Som tidligere poengtert, legalitet er ikke det samme

som legitimitet, og denne subtile distinksjonen kan det være klokt å bevare i bakhodet. I en rettsstat er det ikke betraktet som legitimt å underkaste alle borgere en overvåkning og registrering av våre bevegelser ut fra den tanke at borgerne må kontrolleres mest mulig og helst kontinuerlig for å hindre at de begår ulovlige eller uønskede handlinger.

Dette mønsteret, hvor alle i utgangspunktet behandles med det for øye at de er potensielle lovbrutere, er karakteristisk for politistaten. Vissheten om dette er trolig årsaken til de bestrebelse vi har vært vitne til for å overbevise det norske folk om at den innsamling av opplysninger som Datalagringsdirektivet påbyr, likevel ikke er overvåkning. Det er et faresignal når slike feilfremstillinger skjer bevisst.

For borgerne er det da avgjørende viktig å vedlikeholde bevisstheten om at demokratiet i seg selv aldri er noen vaksine. De som gjør seg til tilhengere av Datalagringsdirektivet, bruker mye energi på å forsikre om at tiltak som Datalagringsdirektivet ikke er farlige, så lenge de gjennomføres i et demokrati. Resonnementet er forståelig, men feilaktig. Forståelig fordi demokratiets tendens til å trene mennesker opp til å søke kompromiss og konsensus også der kompromisser er lite å anbefale, disponerer for en type tenkning hvor mange finner det vanskelig å ta klare standpunkter. Feilaktig, fordi det ikke er slik at demokratiet etableres eller opprettholdes som et resultat av den gode viljes vedtak.

Demokratiet er resultatet av maktbalanse i samfunnet, og har historisk måttet kjempes igjennom under motstand mot de som til enhver tid har hatt mye makt i samfunnet. Skritt for skritt har mennesker, først og fremst som en følge av utdanning og kunnskap sett fordelene forbundet med åpenhet, medbestemmelse og balansering av maktforholdene. Vil vi bevare denne samfunnsformen, bør vi vokte oss vel for med tilsvarende mange små skritt nedbygge folkestyret og slik gjøre det mer autoritært, mer straffende, mindre fritt og dermed automatisk mer preget av maktkonsentrasjon på myndighetenes hender og dermed uunngåelig større risiko for og større forekomst av maktmisbruk.

8.3 KONKLUSJON

EFN mener at det i en rettsstat ikke kan være akseptabelt at et lands myndigheter i lang ettertid skal kunne komme til kunnskap om lovlydige borgeres bruk av telefon, e-post, SMS/MMS-meldinger og eventuelt nettbruk, ved å kreve at det skal lagres detaljerte opplysninger om hvem og med hva borgerne kommuniserte og om når disse kommunikasjonshandlingene fant sted. Det lar seg ikke gjøre å utpeke en enkeltfaktor som alene ødelegger rettsstaten, og vårt samfunn er under press fra utallige gode formål som spenner fra kriminalitetsbekjempelse til velmenende tiltak for å sørge for at syke mennesker får behandling og andre former for støtte etter behov.

Like fullt representerer Datalagringsdirektivet ett av de mange skritt som fører samfunnet i en retning med større kontroll og flere inngrep i den enkeltes liv, og korresponderende mindre bevegelsesfrihet i samfunnet. Dertil kommer at tillitsforholdet både mellom borgere og myndigheter og mellom samtlige medlemmer i samfunnet uunngåelig vil lide og bli preget av større mistro, dersom staten ved lov skal hindre borgerne i å kommunisere og bevege seg sporfritt. Vi mener at dette er en tendens som kan og bør reverseres, og det gjøres blant annet ved at vi sier nei til uforholdsmessig inngripende tiltak som i de gode hensiktens navn belaster menneskers privatliv, går på tvers av hensynet til personvern og øker risikoen for utilbørlig maktbruk.

Derfor blir vår konklusjon at vi på det sterkeste fraråder at Datalagringsdirektivet innlemmes i norsk lov.

9.0 KILDEHENVISNINGER

- [1] Høring - datalagring
<http://www.regjeringen.no/nb/dep/sd/dok/hoeringer/hoeringsdok/2010/horing---datalagring.html?id=590001>
- [2] Storebror har fått ufortjent dårlig rykte
<http://tinyurl.com/storebror-erik>
- [3] 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565
- [4] Referat fra møte om Datalagringsdirektivet i Oslo 07.03.2008
<http://efn.no/dld-noseminar2008-referat.txt>
- [5] PST: Høring om datalagring
http://www.pst.politiet.no/System/Norsk/20100412_dld_hu.pdf
- [6] Datalagring er ikke overvåking
<http://www.bt.no/meninger/kronikk/Datalagring-er-ikke-overvaaking-985954.html>
https://www.politi.no/politidirektoratet/aktuelt/nyhetsarkiv/2009_12/Nyhet_8002.xml
- [7] Trafikkdatas betydning
<http://www.aftenposten.no/nyheter/iriks/article3569530.ece>
- [8] Lite sannsynlig at Kristiansen har ringt fra åstedet
<http://www.nrk.no/nyheter/1.522225>
- [9] http://en.wikipedia.org/wiki/Data_mining
- [10] <http://no.wikipedia.org/wiki/Justismord>
- [11] Utenfor enhver mistanke
<http://www.aftenposten.no/meninger/kronikker/article2394305.ece>
- [12] Forbyr romavlytting
<http://www.aftenposten.no/nyheter/iriks/politikk/article3159092.ece>
- [13] NOU 2009: 15 Skjult informasjon - åpen kontroll
<http://www.regjeringen.no/nb/dep/jd/dok/nouer/2009/nou-2009-15/>
- [14] LOV 1999-05-21 nr 30: Lov om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven).
<http://www.lovdatab.no/all/hl-19990521-030.html#EMKN-A8>

10.0 FORFATTERE, KREDITERING OG KONTAKT-INFORMASJON

EFNs høringsuttalelse om Datalagringsdirektivet er skrevet og redigert av Per Inge Østmoen, med bidrag fra Knut Yrvin (bl.a. del 5, 7.1-2), Tom Fredrik B. Klaussen, Thomas Gramstad og Bjørn Remseth.

Kontaktinformasjon:

styret@efn.no
mobil: 4817 6875 / 4735 2097

EFN er en elektronisk rettighetsorganisasjon som jobber med medborgerskap og juridiske rettigheter i IT-samfunnet. www.efn.no

Med vennlig hilsen på vegne av EFN,

Per Inge Østmoen og Thomas Gramstad

Oslo, 12. april 2010

Dette dokumentets nettsadresse er
<http://efn.no/dld-hoeringsuttalelse2010.html>
<http://efn.no/pdf/dld-hoeringsuttalelse2010.pdf>

Dette dokumentets adresse:
<http://www.efn.no/dld-hoeringsuttalelse2010.html>

Elektronisk Forpost Norge er en rettighetsorganisasjon som jobber med medborgerskap og juridiske rettigheter i IT-samfunnet.
www.efn.no

Sist oppdatert av [Thomas Gramstad](#) 12. april 2010.

