Samferdselsdepartementet
Postboks 8010 Dep
0030 OSLO

12.april 2010

Høring om datalagringsdirektivet

1. SAMMENDRAG

Stopp Datalagringsdirektivet[1] (Stopp DLD) er en partipolitisk uavhengig kampanjeorganisasjon. Over 8000 personer fra ulike samfunnslag har sluttet seg til organisasjonen siden stiftelsesmøtet 3.november 2009.

Stopp DLD mener datalagringsdirektivet er mer et politisk veiskille enn en enkeltsak. Det grunnleggende spørsmålet som skal tas stilling til er hvor grensen skal gå for statlig kontroll over lovlydige borgeres liv. Stopp DLD aksepterer derfor ikke høringsuttalelsens forsøk på å redusere debatten om datalagringsdirektivet til en pragmatisk debatt om lagringstid og lagringsmåte.

Stopp DLD vil med følgende hovedargumenter advare Stortinget mot å implementere datalagringsdirektivet i norsk rett:

- **Datalagringsdirektivet representerer Norgeshistoriens største enkeltinngrep i lovlydige borgeres privatliv**. Ikke bare vil direktivet lagre opplysninger om når, hvor, hvordan og med hvem vi kommuniserer elektronisk. Direktivet vil også gjøre en økende andel av befolkningen som har mobiltelefoner med kontinuerlig nettilgang (f.eks. iPhone) sporbar 24 timer i døgnet.

- **Datalagringsdirektivet svekker rettssikkerheten til borgerne.** Direktivet skiller nemlig ikke mellom uskyldige og mistenkte og representerer med det en helt ny måte å bekjempe kriminalitet på i Norge som vi vil advare mot på det sterkeste. Å innføre datalagringsdirektivet er å kaste det demokratiske rettsprinsippet om at enhver er uskyldig inntil det motsatte er bevist (uskyldspresumpsjonen) over bord.

- **Datalagringsdirektivet gir borgerne falsk trygghet**. Selv om direktivet pålegger omfattende lagring av trafikk- og lokasjonsdata er det enkelt for kriminelle å slippe unna. Man kan for eksempel surfe via et åpent trådløst nettverk, ta i bruk

1 http://stoppdld.no/

anonymiseringstjenester som TOR eller kommunisere ved hjelp av Skype, Gmail, MSN eller andre internettbaserte kommunikasjonstjenester. Nettopp den type avanserte kriminelle direktivet angir som hovedmål vil lett tilpasse seg direktivets virkeområde. Dermed er det lovlydige borgere som rammes av direktivet og ikke de det er ment for.

Datalagringsdirektivet er et ektefødt barn av *krigen mot terrorisme*. Terrorisme er det svake og marginale mindretalls strategi mot et større og sterkere storsamfunn. Den marginale størrelsen gjør de vanskelige å fange og deres taktikk effektiv. Å ikke vite hvem de er eller hvor de er, gjør at de er vanskelig å stoppe. Og det er denne usikkerheten som er deres mål. Ikke selve aksjonene. Og gjennom å spre frykt, få storsamfunnet til å overreagere og endre sin adferd. Vi mener datalagringsdirektivet representerer en slik overreaksjon.

2. PROSESS

Et urovekkende mønster i høringsnotatet at det lider av manglende utredninger. Særlig skuffende er det at man ikke har utredet de personvernmessige konsekvensene av datalagringsdirektivet på en grundig måte, eller forsøkt å dokumentere politiets faktiske behov for direktivet. Det siste var noe en samlet personvernkommisjon i juni 2008 uttalte som en forutsetning for å i det hele tatt å kunne *starte en diskusjon* om en eventuell implementering av direktivet i norsk rett.

Mens svenske myndigheter har gjennomført en over 300 sider lang utredning av datalagringsdirektivets konsekvenser for Sverige, har norske myndigheter nøyet seg med et 60 siders langt høringsnotat som ikke bare mangler utredninger, men gir minst like mange spørsmål som svar.

3. PERSONVERNET OVERKJØRES

Et demokrati er avhengig av et gjensidig og godt tillitsforhold mellom borger og stat. Om borgernes friheter innskrenkes for mye til fordel for økt statlig kontroll vil tilliten, og med det også demokratiet, svekkes.

I debatten om datalagringsdirektivet hevdes til stadighet argumentet om at den som ikke har noe å skjule heller ikke har noe å frykte. Et slikt argument undergraver borgernes privatliv både som egenverdi og som forutsetning for et demokrati.

3.1. Sporbar døgnet rundt

En stor svakhet med høringsnotatet er at det tar utgangspunkt i en teknologisk virkelighet som for lengst er utgått på dato. Hvilke opplysninger som kan hentes fra lagrede trafikk- og lokasjonsdata fra borgernes elektroniske kommunikasjon er helt avhengig av de teknologiske vanene som borgerne til enhver tid har. Vi vil her peke på to relevante endringer som har skjedd siden direktivet ble vedtatt i 2006, og som har mye å si for de personvernmessige konsekvensene av direktivet:

1. De fleste går i dag rundt med en mobil i lommen/vesken som brukes like mye til mediebruk som til å ringe og sende meldinger med. For eksempel har 600.000 nordmenn blitt brukere av musikktjenesten Spotify det siste året[2]. I tiden som kommer vil flere bli brukere denne og lignede streamingtjenester, og dette vil få store konsekvenser for personvernet fordi tjenestene legger igjen elektroniske spor hver gang den brukes.

2. I 2009 ble det solgt 2,3 mill mobiltelefoner i Norge. Av disse var 63 prosent 3G-tlf og 30 prosent var smarttelefoner.[3] Det betyr at stadig flere har mobiltelefoner som kobler seg automatisk til nettet for å oppdatere telefonens programvarer, noe som etterlater elektroniske spor også når telefonen ikke er i bruk. Datalagringsdirektivet vil dermed også gi staten kunnskap om hvor vi tilbringer nettene, om vi var hjemme, hos svigermor, elskeren eller kanskje på et nachspiel.

Blir datalagringsdirektivet innført vil staten ikke bare vite med hvem, hvor, når og hvordan vi kommuniserer med andre mennesker elektronisk. Direktivet vil også gi staten informasjon om hvor vi befinner oss når vi lytter til musikk på mobilen og hvor vi befinner oss når mobilens programvarer automatisk oppdateres. Borgere flest vil på grunn av datalagringsdirektivet bli sporbare døgnet rundt, og det er med dagens teknologiske virkelighet. Hvordan teknologien ser ut i morgen, og hvilke konsekvenser lagring av trafikk- og lokasjonsdata vil få for personvernet da, er det ingen som vet.

I Soria Mora 2 heter det at *"Arbeiderpartiet vil implementere datalagringsdirektivet forutsatt at det i utredningen ikke framkommer klare negative konsekvenser for personvernet"*. Utsagnet er uforståelig. Om ikke det å innføre et direktiv som vil gi staten nok data til å rekonstruere hverdagen til hver enkelt av oss er klart negativt for personvernet, ja hva er det da? Utsagnet er også tegn på en betydelig maktarroganse – hvis direktivets mulige negative personvernkonsekvenser er avgjørende, hvorfor har da ikke regjeringen utredet om slike finnes?

3.2. Åpner for enda mer overvåkning

All erfaring tilsier at jo mer informasjon som kan hentes ut fra de lagrede trafikk- og lokasjonsdata, jo flere vil gjøre krav om å få bruke dem. Da øker også sannsynligheten for misbruk eller at data kommer på avveie. I England, der direktivet er implementert, har til sammen mer enn 600 forskjellige myndighetsinstitusjoner tilgang til de data som direktivet pålegger å lagre. Selv om man i høringsnotatet slår fast at bare politiet skal ha tilgang til de lagrede dataene er dette ingen garanti for at det ikke vil skje en formålsglidning i fremtiden. Det er for eksempel nok å forestille seg at andre enn politiet ber om tilgang til de lagrede dataene for å oppklare ulovlig fildeling, innsidehandel eller utroskap.

3.3. Overvåkning påvirker adferden?

2 http://www.aftenposten.no/kul_und/musikk/article3583606.ece
3 Kilde Elektronikkbransjen.

Etter at direktivet ble innført i Tyskland ble i 2008 gjort en undersøkelse[4] som viste at datalagringsdirektivet hadde endret den tyske borgers oppførsel. Det hadde bidratt til en "chilling effect":

Undersøkelsen, utført blant et representativt utvalg på 1002 personer viste følgende skremmende resultat

- **73%** kjente til datalagring
- **11%** sa at de allerede hadde avstått fra å bruke telefon, mobiltelefon eller e-post ved spesielle anledninger
- **6%** opplevde å motta mindre kommunikasjon etter implementering av direktivet b
- **52%** sa at de sannsynligvis ikke vill bruke telekommunikasjon til kontakt med f. eks. narkotikarådgivning, ved psykoterapi eller ved ekteskapsrådgivning, på grunn av datalagringsdirektivet.

Dette viser at innføring av datalagringsdirektivet kan ha en stor grad av påvirkning av hvordan borgerne oppfatter direktivet som en opplevd trussel mot deres ønske om å kunne kommunisere uten fare for at denne kommunikasjonen kan misbrukes.

Personvernkommisjonen har også vært inne på dette da de i en uttalelse om datalagringsdirektivet[5] fra Juni 2008, sier:

> *Allerede vissheten av at noen kan lete seg fram til dine kontakter og dine bevegelser, både i det virkelige rommet og på Internett, kan være nok til å hemme borgere i utøvelsen av sine friheter til å samles, til å ytre seg og til å søke opplysninger. Dette er grunnleggende rettigheter i et demokrati, som kommer til uttrykk både i norsk lovgivning og i Den Europeiske Menneskerettskonvensjon (EMK). Etter kommisjonens oppfatning vil innføring av direktivet kunne svekke opplevelsen av privatliv og privat kommunikasjon.*

4. RETTSSIKKERHETEN SVEKKES

Det prinsipielt banebrytende med datalagringsdirektivet er den bakenforliggende tankegang at vi alle er potensielle lovbrytere som må overvåkes. Direktivet retter seg mot hele befolkningen, og skiller ikke, slik andre integritetskrenkende politimetoder gjør, mellom mistenkte og uskyldige borgere.

Stopp DLD synes det er oppsiktsvekkende at det i høringsnotatets argumenteres med at datalagringsdirektivet kan bidra til å frikjenne personer som er ubegrunnet mistenkt for kriminelle handlinger. Et slikt argument tilsier, om en tar det på alvor, at enhver overvåkning, uansett hvor inngripende den måtte være, er av det gode. Det snur også opp-ned på det grunnleggende rettsstatlige prinsipp om at enhver borger er uskyldig inntil det motsatte er bevist (uskyldspresumsjonen). Det burde være unødvendig å minne om at det i en rettsstat er borgernes skyld, og ikke uskyld, som skal bevises.

4 http://www.kreativrauschen.com/blog/2008/06/04/data-retention-effectively-changes-the-behavior-of-citizens-in-germany/

5 http://www.regjeringen.no/nb/dep/fad/dok/nouer/2009/nou-2009-1/24.html?id=542291

5. FALSK TRYGGHET

Det ser ut som om de fleste har glemt hvorfor datalagringsdirektivet ble etablert. Høringsnotatet viderefører en merkverdig taushet om direktivets opprinnelige begrunnelse. Det var terroraksjonene i Madrid og London som bidro til at direktivet i sin tid ble innført, og den bærende rasjonale bak det er kampen mot ekstreme terrorhandlinger.

Direktivet er altså ment å gi justismyndighetene et verktøy til å avdekke, etterforske og rettsforfølge terrorisme og alvorlig kriminalitet. Dets bidrag til det moderne samfunn er å gi muligheten for å oppklare alvorlige forbrytelser *etter de har skjedd*. Det vil i altså i liten grad forhindre alvorlig kriminalitet eller terroraksjoner, men skal brukes i etterkant.

5.1. Politiets tilgang til trafikkdata i dag

Når tilhengere av datalagringsdirektivet hevder at Norge kan bli en kriminell frihavn dersom ikke datalagringsdirektivet innføres, kan man få inntrykk av at politiet ikke har tilgang til trafikkdata i dag. Det er ikke riktig, noe som omtales i høringsnotatet.[6] I tillegg er det også verdt å merke seg vi faktisk har en generell lovbestemmelse som gir påtalemyndigheten adgang til å kreve tvungen datalagring; den finnes i straffeprosessloven § 215a.[7]

Høringsnotatet vurderer heller ikke endringer av reglene i straffeprosessloven og politiloven om bruk av tvangsmidler som ble gjennomført i 2005.

Det ble åpnet for bruk av romavlytting som etterforskingsmetode, samt for bruk av tvangsmidler i avvergende og forebyggende øyemed. Videre ble politiet gitt adgang til å identifisere mobiltelefoner og andre kommunikasjonsanlegg ved hjelp av teknisk utstyr. Det ble gjort mindre endringer i reglene om hemmelig ransaking, kommunikasjonskontroll, teknisk sporing, utleveringspålegg fremover i tid og avlytting og opptak av samtale med samtykke fra en av samtalepartene.

Siden datalagringsdirektivet har sin bakgrunn i å bekjempe terrorisme er det underlig at høringsnotatet heller ikke nevner de verktøy som f. eks. PST allerede har fått tilgang til, både i form av romavlytting og forebyggende tvangsmidler. Vi mener det er avgjørende å se den betydelige økningen i omfanget av statlige overvåkningsmuligheter i sammenheng når man etter så kort tid vurderer å innføre så omgripende virkemidler som direktivet er.

Det er også verdt å merke seg at Metodekontrollutvalget mener at de ikke hadde grunnlag nok til å gjøre en kvalitativ god vurdering av de endringer som ble innført i 2005[8]

> *"Reglene som ble vedtatt i 2005 hadde imidlertid bare vært i bruk i under tre år da utvalget startet sitt arbeid. Reglene åpner for bruk av romavlytting i etterforsking av saker om svært alvorlige typer kriminalitet, samt bruk av tvangsmidler for å avverge og forebygge alvorlige straffbare handlinger. Som Justiskomiteen pekte på i uttalelsen ovenfor, er reglenes anvendelsesområde lite, og statistikk utvalget har fått tilgang til viser at bruken av reglene ikke har vært omfattende. Grunnlaget for en evaluering er*

6 Høringsnotatet punkt 2.4
7 http://www.uhuru.biz/?p=28
8 http://www.regjeringen.no/nb/dep/jd/dok/nouer/2009/nou-2009-15/10.html?id=569467

derfor begrenset. Det faktum at utvalget heller ikke er blitt innvilget innsyn i opplysninger fra enkeltsaker har ytterligere svekket utvalgets forutsetninger for å gjennomføre en slik evaluering."

Politiet har altså fått utvidede fullmakter som viser seg lite brukt. I tillegg vil man altså innføre datalagringsdirektivet med de negative konsekvenser det innebærer for personvernet. Uten at man har en fullgod evaluering av de verktøy man råder over.

Kriminelle tilpasser seg veldig raskt til de endringer både når det gjelder politiets metoder og ikke minst teknologiutviklingen. Dette innså politiet allerede i 2005 da de i en høring om forebyggende politimetoder[9] mente at andre metoder enn romavlytting ikke ville fungere.

Professor Petter Gottschalk ved Handelshøgskolen BI som også har vært foreleser ved Politihøgskolen og konsulent for politiet, mener at politiet ikke trenger datalagringsdirektivet:[10]

"- Politiet har i dag ekstremt mange gode datakilder til rådighet. Samkjøring av registre, analyseverktøy og bedre metodebruk er veien å gå. Jeg synes det nærmest er en fallitterklæring når Politiet sier de trenger datalagringsdirektivet, sier Gottschalk"

Også siv.ing og ph.d. Svein Willassen har, i en grundig utredning på oppdrag fra Datatilsynet konkludert med at hoveddelen av de data direktivet pålegger lagring av ikke, eller i liten grad, er nødvendige for politiet.[11]

Vi i Stopp Datalagringsdirektivet ikke bare innser, men støtter fullt ut politiets behov for gode virkemidler i kampen mot kriminelle. Vi mener imidlertid disse allerede finnes gjennom de metoder som har blitt innført etter 2005. Skulle det være mangler, så bør de eventuelt diskuteres endringer av disse. Å innføre datalagringsdirektivet vil ikke være et virkemiddel som forholdsmessig kan anbefales. Det bryter mot den liberale rettstatens grunnlag.

5.2. Lett for kriminelle å omgås direktivet

Det er liten grunn til å tro at datalagringsdirektivet vil ramme de som har til hensikt å begå terrorisme eller alvorlig kriminalitet særlig hardt. Dette har også presidenten i EuroCop (European Confederation of Police), Heinz Kiefer, innsett. Før datalagringsdirektivet ble vedtatt av EU uttalte han følgende i en pressemelding:

"It remains easy for criminals to avoid detection through fairly simple means, for example mobile phone cards can be purchased from foreign providers and frequently switched. The result would be that a vast effort is made with little more effect on criminals and terrorists than to slightly irritate them.".[12]

Hvor enkelt det er for kriminelle å unngå å bli overvåket av datalagringsdirektivet er nok et tema som er underkommunisert i høringsnotatet. Vi har her listet opp ni måter som kriminelle, amatører så vel som profesjonelle, kan benytte for å unngå direktivet:

9 http://pf.no/asset/2092/2/2092_2.doc
10 http://www.idg.no/computerworld/article161438.ece
11 Svein Willassen, Datalagringsdirektivet – Verdi i etterforskning og risikofaktorer for personvern, utredning 7.4.2010
12 http://www.eurocop-police.org/pressreleases/2005/05-06-02%20PRESS%20JHA%20Council_E.pdf

Unngåelsesmulighet 1: The Onion Router (TOR)
The Onion Router (TOR) er et nettverk av der vanlige nettbrukere kan stille sin datamaskin til rådighet for andre[13]. Kommunikasjonen er kryptert, distribuert og indirekte tilknyttet mellom endepunktene. Dette innebærer at tilkoblingen til en nettside for eksempel vil gå gjennom en rekke datamaskiner før den når sluttpunktet, og sendes tilbake samme vei gjennom nettverket – uten at hver enkelt maskin vet hva som ble forespurt eller hvem som gjorde forespørselen. Nettverket forhindrer noen som overvåker brukerens nettilkobling fra innsyn i hvilke nettsteder som besøkes, samtidig som det hindrer nettstedene som besøkes fra å vite hvilken maskin (IP-adresse) forespørselen i utgangspunktet kom fra. Dette gjør IP-adressen verdiløs som informasjon.

TOR brukes blant annet av bloggere som har behov for anonymisering når de publiserer informasjon fra totalitære regimer som Kina og Iran.

Unngåelsesmulighet 2: Kontantkort for mobiltelefoner
Med et kontaktkort kjøpt i utlandet kan man foreta telefonsamtaler og sende SMS uten at teleoperatørene har tilgang til informasjon om hvem som i utgangspunktet gjennomfører kommunikasjonen. Dette gjør informasjon om telefontilkobling verdiløst.

Unngåelsesmulighet 3: Nettelefontjenester
Med Skype og andre nettelefontjenester er det mulig å kommunisere muntlig uten å bruke det analoge telefonnettet. Disse tjenestene fungerer på mange ulike måter, hvor enkelte bruker direkte kommunikasjon (såkalt «peer-to-peer») og andre benytter seg av en sentral server. Med sistnevnte kjenner ikke brukerne til hverandres IP-adresser. Nettelefontjenester kan også benyttes i kombinasjon med anonymiseringsnettverk som TOR.

Unngåelsesmulighet 4: VPN og Proxy
Med virtuelle private nettverk (VPN) og proxyer kan brukeren utføre kommunikasjon via en betalt eller åpen server på Internett. Et søk på nettet etter «Free proxy server» gir flere tusen resultater som tilbyr anonymisert tilkobling til ressurser på nettet. Dette er en mindre avansert form for anonymisering sammenlignet med nettverk som Tor, men likevel et system som i de fleste tilfeller gjør IP-adressen verdiløs.

Unngåelsesmulighet 5: Hurtigmeldingstjenester
Hurtigmeldingstjenester («Instant messaging services») brukes av mange for å kommunisere på nettet i dag. Dette fungerer på mange måter som nettelefonitjenester, men i hovedsak med tekst. Eksempler på slike tjenester er MSN, IRC, AIM, XMPP, Spin m.fl.. Kommunikasjonen foregår enten direkte mellom brukerne eller via en sentral server. Slike tjenester kan også brukes i forbindelse med kryptering og anonymiseringsnettverk som Tor[14].

Unngåelsesmulighet 6: Hurtigmeldinger i onlinespill og andre applikasjoner
Det er ikke bare de større og mer tradisjonelle hurtigmeldingstjenestene som MSN, Skype, IRC osv. som benyttes av nettbrukere i dag. I nesten alle onlinespill, slik som World of Warcraft, er det mulig å kommunisere direkte med andre brukere eller via en

13 http://www.torproject.org/overview.html.en
14 http://www.torproject.org/overview.html.en#hiddenservices

sentral server. Det er også mulig å programmere eller modifisere egne applikasjoner som kan fungere som hurtigmeldingstjenester – om nødvendig kan slik kommunikasjon kamufleres som normale web-forespørsler[15].

Unngåelsesmulighet 7: Offentlige internetterminaler
På stadig flere steder kan man i dag koble seg til nettet med åpent tilgjengelige datamaskiner. Slike maskiner finnes på bibliotek, internettkafeer, universiteter m.m. og gjør at koblingen mellom bruker og IP-adresse forsvinner.

Unngåelsesmulighet 8: Åpne nettverk
Svært mange husholdninger bruker i dag ingen beskyttelse på sine nettverk. Dette gjør det mulig for andre personer å benytte nettverkene og dermed skjule hvem som egentlig står bak kommunikasjonen. Mange steder finner man også offentlig tilgjengelige nettverk (kaféer, bibliotek m.m.) i tillegg til at det finnes organisasjoner som jobber for å opprettholde åpen nettilgang i urbane områder[16].

Unngåelsesmulighet 9: Endre IMEI-koden til mobiltelefonen
Mobiltelefonens IMEI-kode er en kode som blant annet brukes til å spore telefonen tilbake til eier/produsent og til å kontrollere hvor telefonen er solgt. IMEI-koden skal lagres etter datalagringsdirektivet, men fordi denne koden ikke er en fysisk unik kode for hver telefon er det fint mulig for kriminelle med litt teknisk innsikt å endre denne koden.

Totalt er det så mange hull i direktivet at det nærmest er å anse som åpne låvedør for kriminelle. Dermed er det lovlydige borgere som først og fremst vil bli rammet av direktivet.

Samtidig er det viktig for Stopp Datalagringsdirektivet å understreke å det er verken mulig eller ønskelig å lage et vanntett direktiv. Flere av unngåelsesteknologiene som kan brukes for å unngå datalagringsdirektivet er nemlig de samme teknologiene som i andre sammenhenger brukes helt lovlig for å oppnå økt sikkerhet. For eksempel er VPN (se unngåelsesmulighet 4) en teknologi som Post- og Teletilsynets Nettvettkampanje anbefaler for å oppnå sikre kommunikasjonsforbindelser mellom hjemmekontor og arbeidsplass[17]. Å erklære krig mot disse teknologiene er som å be folk om å ferdes på nettet uten noen form for beskyttelse.

6. Motstanden mot direktivet er ikke et særnorsk fenomen

Mer enn fire år etter at datalagringsdirektivet formelt ble vedtatt av EU, er direktivet fremdeles kontroversielt i Europa. Vårt naboland Sverige er ett av i alt fire land som ikke har implementert direktivet overhodet. Selv om landet har blitt idømt en bot på ca 30 millioner svenske kroner for manglende implementering, vil direktivet ikke bli politisk behandlet før tidligst etter Riksdagsvalget 19.september.

Mer interessant er Datalagringsdirektivets møte med rettsvesenet i Europa. I Romania slo grunnlovsdomstolen fast 8.oktober 2009 at datalagringsdirektivet er i strid mot den rumenske grunnloven og Den Europeiske Menneskerettighetskonvensjonen (EMK). 2.mars 2010 avsa

15 http://en.wikipedia.org/wiki/Tunneling_protocol
16 http://en.wikipedia.org/wiki/Wireless_community_network
17 http://www.nettvett.no/ikbViewer/page/nettvett/tema/artikkel?p_document_id=113327&tema=63128

den tyske forfatningsdomstolen kjennelse om at Tysklands implementering av direktivet, som blant annet innebar minimums lagringstid på seks måneder, er i strid med den tyske grunnloven. Domstolen påla også operatørene å slette alle lagrede data med umiddelbar virkning.

Det er underlig at norske myndigheter legger til grunn for høringsnotatet at direktivet er i tråd med menneskerettighetene når omfanget av direktivets personvernutfordringer prinsipielt er underkjent i begge de land der direktivet faktisk har vært prøvet for domstolene At direktivet er i strid med EMK er også fremholdt i flere juridiske artikler.

Hva EUs egen evaluering vil munne ut i er uklart. Kommisjonen skal levere en rapport til Europaparlamentet innen 15.september i år. Fagkommisær Cecilia Malmstrøm, som selv stemte imot datalagringsdirektivet som Europaparlamentariker i 2006, skrev følgende på sin blogg 6.mars I år:

> *"Jag har för avsikt att göra en översyn av lagen – dess effektivitet, proportionalitet, dataskydd, kostnad mm. Detta planerar jag att genomföra i slutet på året".*

Debatten om datalagringsdirektivet lever fortsatt i hele Europa, noe som i seg selv er et argument for at Norge ikke bør vedta direktivet. Direktivet vil ramme de lovlydige, men ikke de kriminelle det er ment for. Det er allerede før implementering, utgått på dato og vil med stor sannsynlighet bli endret. Tiden vil vise hvordan.

Med vennlig hilsen
for Stopp Datalagringsdirektivet

Lars-Henrik Parup Michelsen
Leder

***Nestleder*:**
Heidi Nordby Lunde

Nestleder:
Ida Jackson,

Styremedlemmer:

Audhild Gregoriusdotter Rotevatn

Heidi Austlid

Linn Hemmingsen

Hallstein Bjercke

Knut Johannessen

Erlend Sand

Tale Marte Dæhlen

Per Aage Pleym Christensen

Carl Christian Grøndahl

Geir Pollestad

Ingeborg Steinholt

Svenn-Arne Dragly

Guro Fjellanger

Hanna E. Marcussen

Ulf Leirstein

Hans Felix

Anine Kierulf

Torgeir Waterhouse

Snorre Valen

Thor Bjarne Bore

Tonje Brenna

Vedlegg 1:

Eksempel: Slik overvåker datalagringsdirektivet

Navn: Gro Grolsen
Stilling: Mellomleder i bedrift
Bosted: Bærum
Arbeid: Oslo
IKT: Bredbånd hjemme og på jobb, mobilt bedriftsabonnement

Hverdagslige hendelser som registreres gjennom datalagringsdirektivet, står med **uthevet skrift**:

07:00: Synkronisering av e-post og outlook hver 4. time i fritida, i mobil-nettet. Registrerer hvor hun befinner seg.

07:45: Passerer bomring på Lysaker, brikken i bilen, registret på ham, registreres med tidspunkt

07:55: Passerer bomring på Skøyen, brikken registreres

08:04: På vei fra parkeringsplassen til arbeidsplassen i sentrum snakker hun i mobiltelefonen med en kunde, og krysser mellom forskjellige basestasjoner, og dermed er det logget hvor hun var 08:04 da samtalen startet, samt hvor hun var 08:09 da samtalen ble avsluttet

08:12: Hun stopper i en minibank for å ta ut penger, og legger dermed igjen spor i form av korttransaksjonen, med info om navn, kortnummer og tidspunkt

08:15: Hun går inn på sin arbeidsplass og drar adgangskortet for å komme inn; dermed er det sannsynligvis registrert klokkeslettet hun kom inn

08:30 – 16:00: Hun sender e-post; hver av disse legger igjen elektroniske spor i form av IP-adressen huns, tidspunkt, hvem hun sendte til, hvilken adresse hun sendte fra (slik at man for eksempel kan se at hun sendte e-post fra sin private adresse, eller til venner og kjente), hun snakker i mobiltelefonen, og legger igjen spor i form av hvem hun ringte når, og lokasjon.

09:00: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobil-nettet. Registrerer hvor hun befinner seg.

09:15: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobil-nettet. Registrerer hvor hun befinner seg.

09:30: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobil-nettet. Registrerer hvor hun befinner seg.

09:45: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobil-nettet. Registrerer hvor hun befinner seg.

10:00: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobil-nettet. Registrerer hvor hun befinner seg.

10:15: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

10:30: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

10:45: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

11:00: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

11:15: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

11:30: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

11:34 Hun kjøper lunsjen sin på kafeen på hjørnet, og betaler med bank accept, kortnummer og tidspunkt er registrert

11:45: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

12:00: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

12:05 Hun passerer inn gjennom adgangskontrollen igjen, og trekker kortet sitt, og legger igjen spor

12:10: SMS fra Amnesty International (1960) med oppfordring om å kreve løslatelse av politiske fanger. Registrerer tid og sted for hvor hun befant seg.

12:15: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

12:30: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Rsgistrerer hvor hun befinner seg.

12:30 Hun drar på møte hos en kunde et annet sted i byen; tar taxi og snakker i mobiltelefonen på vei til møtet. Det er da registrert lokasjonsdata, dvs når samtalen fant sted, samt hvor hun var ved samtalens start og slutt

12:45: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

12:48: Hun betaler med kredittkort, og legger igjen informasjon om kort og tidspunkt (kombinert med GPS-systemet til Oslo Taxi har man muligens også posisjon for start og stopp for turen)

12:57: Hun logger seg på internett hos kunden, som ikke har et tilgjengelig trådløst gjestenett. Hun benytter derfor mobilt bredbånd, og det registreres da hvor hun logger seg på fra, samt når hun logger seg på og av.

13:00: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

13:15: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

13:30: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

13:45: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

14:00: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

14:15: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

14:30: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Rsgistrerer hvor hun befinner seg.

14:45: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

15:00: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

15:05 Hun tar taxi tilbake til jobben, og legger igjen informasjon om kort og tidspunkt (kombinert med GPS-systemet til Oslo Taxi har man muligens også posisjon for start og stopp for turen)

15:15: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

15:30: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

15:30: Hun passerer gjennom adgangskontrollen igjen, og trekker kortet sitt, og legger igjen spor

15:45: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

16:00: Synkronisering av e-post og outlook hver 15. minutt i arbeidstida, i mobilnettet. Registrerer hvor hun befinner seg.

16:15: SMS fra samboeren hjemme, med spørsmål om når hun kommer hjem i dag. Registreres tid og sted.

16:20: Hun drar fra jobb, og drar for å møte en kamerat. Underveis ringer hun hjem, og dermed er det igjen registrert hvor hun har befunnet seg ved start og avslutning av samtalen

18:30: Datteren på 4 ringer for å si god natt; det er nok en gang registrert hvor hun befant seg

20:00: Synkronisering av e-post og outlook hver 4. time i fritida, i mobil-nettet. Registrerer hvor hun befinner seg.

20:30 : Hun kjører hjemover, og passerer en bomring på veien, og brikken er da registrert igjen

21:15: Hun kommer hjem, setter seg ned og logger seg på internett, noe som logges. Hun sjekker e-posten sin, sender et par eposter, disse logges også.

24:00: Synkronisering av e-post og outlook hver 4. time i fritida, i mobil-nettet. Registrerer hvor hun befinner seg.

Inklusive alle e-postene i arbeidstida, er dette 50+ elektroniske spor på en helt vanlig dag. Med 50 e-poster blir det f.eks 100 spor. Av disse er det bare 10 spor som skyldes annen innsamling enn det som følger av datalagringsdirektivet.