Datalagringsdirektivets innvirkning på samfunnet

Kristoffer Johannesen, Øyvind Julsrud og Emil Andreassen

19.09.2011 Høgskolen i Østfold

Datalagringsdirektivets innvirkning på samfunnet

Kristoffer Johannesen, Øyvind Julsrud og Emil Andreassen

«En teknikk for innlemmelse og utelukkelse og en maktmekanisme som i våre dager gjennomsyrer store deler av samfunnet.»

(Michel Foucault)

Sammendrag

I teksten skal vi ta for oss hvordan datalagring strider med rettstatens prinsipper samt hvordan det påvirker mennesker mentalt. Vi tar også for oss hvordan datalagring kan bli brukt som bevis og hvordan informasjonen blir brukt til å kartlegge befolkningens nettrafikk.

Med hensyn til at data over nettrafikk og andre kommunikasjonsmetoder blir lagret vil det skape stridigheter og spørsmål om dette er forsvarlig og etisk riktig. Vil det gi vise seg å gi flere positive enn negative sider, og hvor mye vil dette koste? Når det gjelder å bruke informasjonen som bevis gjenstår det å se om det faktisk vil gjøre politiets arbeid lettere, selv om dataovervåkning tidligere har gitt resultater. Slik som strategisk informasjonsanalyse vil gi politiet en mulighet til å overvåke all trafikk som foregår, selv om de overvåkede ikke har direkte tilknytning til noen form for kriminelle handlinger, og er dette da riktig å gjøre?

Vi vil i denne teksten legge frem uttalelser om datalagringsdirektivet og deres intensjoner, med tanke på å opplyse leseren om direktivets innførings problem i et samfunn.

Innledning

Datalagringsdirektivet er et EU-direktiv om lagring av abonnements-, lokaliserings- og trafikkdata. Direktivet ble vedtatt i Norge 4. april 2001. Dette direktivet er en direkte reaksjon mot terrorangrepene 11. september 2001 i New York, 11. mars 2004 i Madrid og 7. juli i London. Direktivet handler i utgangspunktet om å lagre og loggføre alle våre bevegelser i den digitale verden. På denne måten kan det, ved mistanke om kriminalitet og andre ugjerninger, uthentes informasjon fra direktivet. Hensikten er å bekjempe terrorisme, kriminalitet og andre ugjerninger.

For å sette datalagringsdirektivet i et annet perspektiv, er det mulig å sammenlikne det med hvordan direktivet ville vært i en verden uten det digitale. Om forfedrene våres skulle sende et brev, så kunne det nye direktivet sammenliknes med at det alltid stod en mann ved postkassene og noterte til hvem du sender brev, fra hvem, når du sendte det og hvor du sendte det i fra. Det samme gjelder ved telekommunikasjon; hver gang du går til en telefonkiosk og ringer, står det en mann og registrer når du ringer, til hvem, nummeret du ringer til og fra, og hvem som ringer. Dette ville vært brudd på privatlivet til de som sendte brev og ringte, og det vil det i dag også være.

Det er ikke bare brudd på personvernet som gjør det kontroversielt, men også kostnadene av å utvikle, opprettholde system og ikke minst sikkerheten rundt lagringen. Direktivet må nemlig ha en utrolig god sikkerhet rundt seg. Pentagon har blitt hacket flere ganger, hva er det som hindrer hackere og andre kriminelle fra å hacke et direktiv som lagrer alt av lokaliseringer? Om dette blir gjort, gjør det jobben for kriminelle mye enklere. Mange voksne personer mener at; "Om datalagringsdirektivet kan hindre terrorisme og kirminelle handlinger, er det verdt å innføre det". Spørsmålet er; vil det faktisk det? Hvilke terrorister sender e-mail til sin medhjelper om hvor og når de skal foreta sitt neste oppdrag? De fleste kriminelle vil være oppmerksomme på datalagringsdirektivet, og bruke omveier

for å unngå dette. Det vil ende med at uskyldighetsprinsippet blir snudd på hodet. Det vil gå fra «Alle er uskyldige til det motsatte er bevist» til «Alle er potensielle kriminelle». Det går dermed i mot demokratiets prinsipper.

Datalagringsdirektivet er derfor et kontroversielt tema, ikke bare i Norge, men også flere EU-land. Det er mange som er i mot, og samtidig mange som er for at dette nye direktivet skal innføres i Norge. Hvordan vil innføringen av datalagringsdirektivet påvirke vårt samfunns hverdag på nett?

Rettsstatens prinsipper

I 1975 utga den franske filosofen og psykologen Michel Foucault verket «Overvåking og straff.» Foucault regnes som en 1900-tallets viktigste tenkere, der hans filosofiske undersøkelser av makt og kunnskap, og forholdet mellom makt og kunnskap, har hatt stor innflytelse på tvers av faglige disipliner. I verket «Overvåkning og straff» tar han for seg maktens rolle i framveksten av det moderne fengselssystemet. Foucault ser på fengselet som et uttrykk for overvåknings- og disiplinærteknikken. Han forklarer det som: «en teknikk for innlemmelse og utelukkelse og en maktmekanisme som i våre dager gjennomsyrer store deler av samfunnet» (Michel Foucaults "Overvåkning og Straff" 1975).

I dette verket skriver han om panoptikon («se alt»). Dette er en overvåkningsordning som ble designet av Jeremy Bentham i 1791 til bruk i fengsler. Dette designet gikk ut på at fengselscellene var plassert i en sirkel, med et tårn i midten. Denne arkitekturen gjør at de innsatte alltid er eksponert for tårnets blikkpunkt. Tårnet er et altseende øye. De innsatte kan alltid se tårnet, men aldri vokterne som skjules av tårnets lyskastere. I tårnet kan man se alt, uten noen gang å bli sett.
Den overvåkede merker til alle tider tårnets usynlige blikk som en oppmerksomhet man ikke unnslipper, uansett hva.

Illustrasjon: http://www.webpsykologen.no/innhold/Panoptikon-300x179.jpg

Samfunnets individer vil hele tiden fornemme overvåkningen, og vil bli mer selvbevisste. Mange, spesielt eldre generasjoner som ikke er oppvokst med den nyeste tekonologien, er usikre på retningslinjene og reglene i den digitale verden. Dette kan videre anstifte en ubegrunnet underliggende skyldfølelse. På denne måten får man, uten gyldig grunn, grobunn for en diffus skyldfølelse. Psykologisk sett er dette en av hovedinnvendingene mot datalagringsdirektivet.

In dubio pro reo

Datalagringsdirektivet vil ikke bare overvåke samfunnet; direktivet vil også utfordre et av de grunnlegende prinsippene i en rettsstat – nemlig uskyldspresumpsjonen. «In dubio pro reo» (latin for: I tvil for den anklagede) er nemlig prinsippet om at tvil om den faktiske siden ved et eller flere av straffbarhetsvilkårene, skal komme den tiltalte til gode. Ved innføringen av datalagringsdirektivet vil det gå fra uskyldspresumsjonen, der alle er uskyldige til det motsatte er bevist, til at alle er potensielt kriminelle.

I Norge har det politiske partiet Høyre hatt lange tradisjoner for å styrke personvernet. I denne saken ble deres ideologi satt på prøve.

9.4 For å sikre personvern og ytringsfrihet vil Høyre:
- Utrede grunnlovsfesting av personvernet
- Styrke datatilsynet
- Redusere overvåkningen i samferdselssektoren
- Stille seg kritisk til innføringen av nye lover som øker adgangen til, eller omfanget av, overvåkning i samfunnet.

(Nevnt av Martin Bekkelund i "Politisk Syretest" 26.januar 2011, hentet av Bekkelund fra Høyres program "Kapittel 9 - Trygge lokalsamfunn")

Her sier Høyre at de vil styrke datatilsynet og stille seg kritisk til innføringen av nye lover som øker adgangen til, eller omfanget av, overvåkning i samfunnet. Ved at Høyre stemte for datalagringsdirektivet, forkastet de nemlig sin 127 år gamle tradisjon. Høyre satt på makten til innføringen av datalagringsdirektivet. Et ja fra Høyre ville føre til en innføring, mens et nei ville avkaste det. Det var dermed overraskende at et parti som er for personvern og mindre overvåking stemte for.

Overvåkning og den psykologiske opplevelsesverden

Foucault trekker sine idéer om et overvåkningssamfunn til opplevelser forbundet med alvorlig psykopatologi, og da spesielt schizofreni. En schizofren pasient uttrykker ofte følelsen av å bli overvåket. Den finnes mennesker som påstår at de har implantater i hodet som styrer de og overvåker tankene deres. Noen mener det er utenomjordiske som kontrollerer dem, andre mener det er KGB, Pentagon, FBI eller frimurerlosjen.

En følelse av at samfunnet overåker sine borgere, kan føre til at individet overvåker seg selv. Dette kan føre til grubling og stadig undersøkelser av egene tanker og følelser, noe som vil føre til at noen vil installere sitt eget overvåkningsorgan. Dette krever mye mental energi. Alle handlinger og impulser gjøres til gjenstand for tvil, og man ender opp i sitt eget tankespinn. Vi blir både den som tenker og observerer våre egne tanker. Hos schizofrene skaper dette en stor avstand og indre splid, og de vil da oppleve at det er noen utenfor deres egen kropp som hele tiden overvåker og dømmer alle handlinger. Underkastelsesaspektet i forholdet mellom å overvåke og bli overvåket illustrerer i følge Foucault ulike sider ved en gjennomgripende skam- og skyldfølelse som hjemsøker mange schizofrene.

Vi ser også likhetstrekk med den religiøse instansen. For religiøse mennesker har Gud vært en skikkelse som ser og vet alt. Ikke bare gode handlinger, men også alle syndige impulser. De fleste religioner og gamle visdomstradisjoner inneholder mye kunnskap om mennesket og ikke minst menneskets mulighet for selvutvikling. Mange av disse elementene har blitt undergravd på grunn av monoteistiske underkastelsesideer og gudfryktige forestillinger i hendene på herskesyke prester opp gjennom historien.

Her kan vi trekke paralleller til datalagringsdirektivet. Datalagringsdirektivet er ingen Gud, men kan potensielt «se alt» vi foretar oss i den digitale verden. Om vi tar bakgrunn i dette, kan vi forestille DLD som et vedtak som representerer en usynlig overmakt, som kan skape indre uro med innflytelse på samfunnets individers privatliv.

Som bevis

Det hevdes i datalagringsdirektivets høringsnotater (Samferdselesdepartementet, høringsnotat - datalagring, 2010) at trafikkdataene kan eller har vært viktige bevis for behandlingen av flere kriminalsaker. Et eksempel er en operasjon som politiet har foretatt seg, hvor de benyttet seg av slik teknologi, er Operasjon ENEA, som ble gjennomført i 2004. Dette var en omfattende operasjon som de gjennomførte sammen med politiet i Danmark hvor målet var å finne og stoppe personer som delte bilder av overgrep mot barn. De som delte filer i fildelingsnettverket vil angi ip-adressen sin når de overfører filene. Slik kunne politiet lett finne disse personene ved å gå inn i abonnentregisteret og få ut hvilke datamaskiner som hadde blitt brukt til fildelingen.

Dette er allikevel et eksempel som viker noe fra datalagringsdirektivets intensjoner da det under ENEA operasjonen ble overvåket ip-adresser i sann tid. Datalagringsdirektivet vil i motsetning lagre denne informasjonen til alle nettverksbrukere, slik at de kan hente opp denne informasjonen senere.

Også i NOKAS-saken var politiets bruk av trafikkdata en viktig faktor i arbeidet med saken(Samferdselsdepartementet, høringsnotat – datalagring, 2010). Når det gjelder denne hendelsen var de skyldige forutinntatt med at politiet hadde anledning til å benytte seg av datatrafikk fra mobiltelefoner til å angi eventuelle bevegelsesmønstre. Derfor hadde de isteden anvendt sosiale nettverk på nett for å kommunisere med hverandre. Det de ikke viste var at politiet også her hadde mulighet for overvåkning, og kunne finne de skyldige ved hjelp trafikkdata fra telenor og netcom.

Det er klart at slike metoder for å oppklare slike saker har vært til god hjelp. Spørsmålet er bare om denne metoden vil være like effektiv i fremtiden da det viser seg at de kriminelle nå etter vert har begynt å lære seg å unngå politiets systemer ved å kommunisere på andre måter. Dette kan vi allerede se på NOKAS-saken hvor de mistenkte var klar over at politiet hadde tilgang til å bruke lokasjonsdata fra mobiltelefoner og hadde ingen direkte kommunikasjon vi telefoner. Det de ikke visste var at politiet også kunne overvåke de på sosiale nettverk som ranerne benyttet seg av.

Fortsatt var dette informasjon som var plukket opp i sann tid og politiet har i dag rett til å bruke kommunikasjonskontroll når det er grunn til mistanke. Dette har altså egentlig ikke noe direkte tilknytning til datalagringsdirektivet da de brukte informasjon som de innhentet under sann tid overvåkning. Det er altså ikke noe som tilsier at lagring av data slik som datalagringsdirektivet vil gi noen større hjelp i å løse kriminalsaker som dette, sammenlignet med de midlene de allerede har tilgang til utenom denne ekstrainformasjonen.

Det vil koste samfunnet mange millioner å innføre en slik ordning og spørsmålet om nytteverdien av denne informasjonen er veldig relevant. De midlene som blir brukt på lagring av nettverkstrafikk kunne også ha bli brukt på organisere, samordne og søke i spor de allerede samler inn, og allikevel få like gode resultater i bekjempelsen av kriminalitet.

Det finnes også eksempler hvor det har vært behov for mer effektive dataverktøy for å systematisere bevismateriale, som kommer frem i behandlingen av flere alvorlige saker. Med Lommemannsaken som eksempel skal det ha kommet frem at saken hadde blitt oppklart raskere dersom politiet hadde hatt tilgang til slik overvåkning som datalagringsdirektivet tilbyr.

Personvernkommisjonen skal i sin tur ha etterlyst i en sluttrapport, en grundig klargjøring av behovet for lagring av datatrafikk, og viste til dokumentasjonskravet om nødvendigheten av inngrepet som følger av artikkel 8 i Den europeiske menneskerettskonvensjonen. Instituttet for informatikk hevder at det i høringsnotatene om datalagringsdirektivet ikke blir tatt stilling til denne etterlysningen på en seriøs måte utover fire eksempelsaker, hvor av tre av dem er misvisende referert til. Følgelig viser høringsnotatet at personvernskommisjonens inntrykk av at nødvendigheten for datalagring for bekjempelse av kriminalitet ikke er tilstrekkelig dokumentert.

Strategisk informasjonsanalyse

Politiet kan få tilgang til lagrede trafikkdata dersom det finnes grunn for mistanke, uavhengig om mistanken kan stilles til en spesiell person. høringsnotater (Samferdselesdepartementet, høringsnotat - datalagring, 2010) Dermed kan man ved hjelp av denne informasjonen gjøre strategisk informasjonsanalyse. Dette går ut på at man samler inn store mengder data som behandles og søkes i for å finne gjennomgående mønstre slik at de kan avsløre eventuelle lovstridige.

Slik informasjonsanalyse vil kunne være veldig nyttig for politiet i deres arbeid om å oppklare kriminelle forhold. Selv om dette blir brukt i god hensikt er det samtidig svært motstridene personvernets prinsipper. Dette fordi alle som har tilknytning den eventuelle dataen vil bli trukket inn i etterforskningen. De vil også de få tilgang til overflødig informasjon som kan omhandle annen sensitiv personinformasjon som ikke angår etterforskningen. Allikevel har høyesterett i sammenheng med flere saker stadfestet at politiet skal kunne få benytte seg av denne informasjonen.

Å gi politiet tilgang til informasjon om datatrafikk som de kan benytte seg av i kriminalsaker vil gjøre at flere personer kan bli trukket inn i en eventuell sak og kan avsløre mer sensitiv informasjon om personene involvert. Dette kan være en stor belastning for uskyldig mistenkte å bli trukket inn i en saksbehandling de ikke har noe med og unødvendig informasjon om den mistenkte skal komme frem. At politiet for eksempel tar i bruk overvåkningsvideoer vil ligge nærmere personvernets idealer da dette vil i motsetning til trafikkdata, omfatte et mindre antall personer og vil avsløre mindre unødvendig sensitiv informasjon om personer som blir trukket inn i en eventuell saksbehandling og vil også gi politiet mulighet til å identifisere mulige vitner og gjerningsmenn. Når det gjelder strategisk informasjonsanalyse av trafikkdata vil det stride mer mot personvernet da all kommunikasjon mellom norske borgere vil bli tatt vare på som igjen vil føre til at enda flere personer blir lagt under analyse av politiet. Man vil også få tilgang til å kartlegge personers aktivitet på sosiale nettverk og da kan få tilgang til høyt sensitiv informasjon. Denne metoden vil også svekke pressens kildevern da det er mulig å finne ut hvilke personer som har kontaktet hverandre eller hvor personer skal ha befunnet seg til spesielle tider.

Konklusjon

Er eventuelt datalagringen en så god resurs i forhold til andre metoder at det vil gjøre politiets arbeid så mye lettere i anskaffelsen av bevismateriale at det vil lønne seg? Det vises til flere eksempler hvor informasjon av datatrafikk er benyttet for å fremme datalagringsdirektivets hensikter. Det som gjenstår er om dette vil lønne seg i lengden og om det gir den ønskede effekten da vi ser at tidligere metoder har hatt gode resultater. Videre, er det riktig å drive analyse av datatrafikk som også angår uskyldige mennesker. Dette kan virke både krenkende og respektløst overfor personers privatliv, selv om det gjøres med de beste hensikter. Allikevel kan dette også være en god ting da politiet da lettere kan kjenne igjen og avsløre suspekte mønstre i en lett tilgjengelig database, som igjen vil komme til fordel for de lovlydige borgerne.

KILDER OG REFERANSER

NOU. (2010). Høringsnotat: Datalagring. Oslo: Samferdselsdepartementet. http://www.regjeringen.no/pages/2281081/hnotat_datalagring.pdf

In dubio pro reo. (2011). Hentet 17. september 2011 fra http://no.wikipedia.org/wiki/In_dubio_pro_reo

Bekkelund, Martin. (2011). *Politisk syretest.* Hentet 17. september 2011 fra http://www.bekkelund.net/2011/01/26/politisk-syretest/

Foucault, Michael. (1975). *Overvåkning og straff: Det moderne fengsels historie.* Hentet 15. september 2011 fra http://www.bokkilden.no/SamboWeb/produkt.do?produktId=104301&rom=MP

Liverød, Risholm Sondre. (2011). *Psykoanalyse av datalagring (DLD).* Hentet 15. september 2011 fra http://www.webpsykologen.no/artikler/psykoanalyse-av-datalagringsdirektivet/

NOU. (utdatert). *Trygge lokalsamfunn.* Oslo: Høyre. http://www.hoyre.no/www/politikk/hoyres_programmer/hoyres_stortingsprogram_2009-2013/hoyres_stortingsprogram_2009-2013_html/Kapittel+9+-+Trygge+lokalsamfunn.d25-ThlbW1Q.ips