INTERNATIONAL COMMISSION OF JURISTS ICJ-Norge – Den internasjonale juristkommisjon, norsk avdeling

Samferdselsdepartementet

Postboks 8010 Dep.

0030 Oslo

HØRINGSUTTALELSE – DATALAGRINGSDIREKTIVET

INNLEDNING

Det vises til regjeringens (v/henholdsvis Samferdsels-, Justis- og Fornyings, administrasjons- og kirkedepartementet) høringsnotat av 08.01.10, med høringsfrist satt til i dag, 12.04.10.

Med dette inngis høringsuttalelse fra ICJ-Norge – Den internasjonale juristkommisjon, norsk avdeling.

ICJ-Norges hovedformål er i foreningens vedtekter beskrevet slik: "å fremme og beskytte menneskerettigheter og rettstatlige prinsipper, herunder styrke individets grunnleggende rettigheter og friheter og fremme domstolsvesenets og advokatyrkets uavhengighet og Norges gjennomføring av internasjonale standarder." Ytterligere informasjon om ICJ-Norge finnes på vår nettside www.icj.no.

I samsvar med dette har ICJ-Norge i flere sammenhenger offentlig advart mot implementering av Datalagringsdirektivet (DLD), på prinsipielt grunnlag – under henvisning til balansen i en liberal, demokratisk rettstat mellom statlig kontroll med borgerne og borgernes grunnleggende, demokratiske friheter som privatlivets fred, retten til fortrolig kommunikasjon og generell ytrings-, informasjons- og organisasjonsfrihet. Vi viser blant annet til ICJ-Norges likelydende brev av juni 2009 til henholdsvis Statsministeren, justisministeren, samferdselsministeren samt Stortingets justiskomité og samferdselskomité (*vedlegg 1*).

ICJ-Norge
Postadresse: c/o Ketil Lund, Postboks 1148 Sentrum, 0104 Oslo
E-post: post@icj.no **Nettside:** www.icj.no

ICJ-Norges syn, slik det kommer til uttrykk i ovennevnte brev, står uendret. I nærværende uttalelse vil dette utdypes.

OM REGJERINGENS HØRINGSNOTAT - GENERELT

DLD innebærer en statspålagt kontinuerlig, automatisk, systematisk og unntaksfri registrering og lagring (i minst seks måneder) av alle borgeres trafikk- og lokasjonsdata i forbindelse med bruk av elektroniske kommunikasjonsmidler, som dokumenterer hver enkelt borgers private kommunikasjonsmønstre og -nettverk, samt i stor utstrekning fysiske bevegelser og bevegelsesmønstre (jf blant annet utbredelsen av smarttelefoner) – helt uavhengig av og løsrevet fra noen individuell vurdering av relevansen av registreringen og lagringen for den enkelte som rammes av inngrepet

I lys av de alvorlige, prinsipielle spørsmålene som en slik overvåkning åpenbart reiser – og som ICJ-Norge har i fokus – er en generell observasjon at høringsnotatet behandler disse på en særdeles overfladisk måte, i den grad de overhodet behandles. Dette gjelder blant annet behandlingen av et slikt tiltaks forenlighet med Den europeiske menneskerettighetskonvensjon (EMK) Høringsnotatet viser ikke at regjeringen har foretatt en reell vurdering ac spørsmålet i henhold til de kriterier som følger av praksis fra Den europeiske menneskerettighetsdomstolen (EMD). En slik vurdering kommer ikke til uttrykk i notatet.

Vi konstaterer videre at notatet – på en måte som er egnet til å villede– utelater opplysninger om på hvilke vilkår og i hvilke sammenhenger politi og andre utenforstående vil kunne få tilgang til de lagrende trafikkdata. I høringsnotatet – og i regjeringens offentlige utspill for øvrig – er det gjort til et stort poeng at det *kun* er politiet som skal kunne få tilgang til data som lagres i henhold til det foreslåtte lagringskrav, og at slik tilgang vil forutsette kjennelse fra retten og at det i det minste foreligger *skjellig grunn til mistanke* om straffbart forhold, rettet *mot noen*.

Begge forutsetninger er feilaktige:

For det første vil det i henhold til Regjeringens forslag fremdeles være adgang for statlige og/eller private parter i *sivile søksmål* til å kreve utlevert trafikkdata etter tvistelovens regler, jf tvisteloven § 22-3, jf § 21-5.

For det annet vil Politiets sikkerhetstjeneste (PST) kunne få utlevert historiske trafikkdata etter straffeprosessloven § 216b, jf politiloven § 17d, i *rent forebyggende øyemed*, når det er "grunn til å undersøke" om noen forbereder en av de der nevnte straffbare handlinger. PSTs fullmakter etter politiloven § 17d kan dessuten benyttes *uten forutgående kjennelse fra retten*, dersom PSTs sjef eller assisterende sjef mener at det haster.

Høringsnotatet berører heller ikke den *utlevering* av lagrede trafikkdata som vil skje til *utenlandske myndigheters politi og etterretningstjenester*, til tross for at det åpenbart vil skje – også i hemmelighet, uten at de som rammes vil ha eller få kunnskap om det. Så sent som i går kveld, 11.04.10, publiserte aftenposten.no en artikkel hvor PST-sjef Janne Kristiansen i

forbindelse med høringen om DLD, gjengis med blant annet følgende grunner til at hun ønsker DLD innført i Norge:[1]

> *"Norge fortsatt står på sidelinjen når det gjelder ordningen med fri flyt av bevis mellom EU-landene. [...] PST er helt avhengig av å utveksle informasjon. Hvis ikke vi kan gi gjenytelser, vil de ikke være interessert i å samarbeide med oss."*

Fra et rettstatsperspektiv er det mildt sagt lite tillitsvekkende at sjefen for det politiorgan som har de videste og mest integritetsinngripende fullmakter til å bedrive hemmelig overvåkning av egne borgere, omtaler forvaltning av våre personopplysninger i nærmest merkantile vendinger.

Når høringsnotatet overhodet ikke berører disse problemstillingene, er det i det minste prisverdig oppklarende at PST-sjefen er så vidt tydelig om de hemmelige tjenestenes motiver.

Disse generelle kommentarene til høringsnotatet, illustrerer hvorfor ICJ-Norge ser det som nødvendig med en mer grunnleggende gjennomgang av de prinsipielle spørsmålene et kontroll- og overvåkningstiltak som DLD reiser for samfunnet. Dette begrunner også hvorfor vi i det følgende fremfører våre synspunkter på selvstendig grunnlag, uten at systematikk eller tema knyttes direkte opp til høringsnotatets disposisjon.

DET BREDERE PERSPEKTIV – SAMMENHENGEN

Da en av de mest kjente varslerne i nyere vestlig historie, amerikaneren Daniel Ellsberg, i 1971 begynte å lekke fra de hemmeligstemplede "Pentagon Papers", utløste det et skremmende eksempel på hva statlige myndigheter, herunder selve regjeringen, i et av verdens mest avanserte demokratier kan få seg til å benytte av midler i forsøke på å kneble kritikk for å beskytte sin politiske makt – i fullstendig forakt for alle spilleregler i en liberal, demokratisk rettstat.

Her så man blant annet forsøk på sensur av pressen, ulovlig avlytting og innsyn i psykiske helseopplysninger til bruk i kampanjer for å sverte eller undergrave troverdighet, sjikanøs straffeforfølgning og til og med forsøk på utilbørlig påvirkning av dommere. Alt med god hjelp fra statens egne jurister. Regjeringens innenrikspolitiske makt ble forsøkt beskyttet under merkelappen "Rikets sikkerhet" – en fristende, men demokratisk meget farlig øvelse – som vi som jurister har en plikt til å advare mot og begrense mulighetene for.

Historien nevnes her fordi den samtidig illustrerer hvor essensielt både personvernet, ytringsfriheten og rettstatens prinsipper er for opprettholdelse av demokratiet – og ikke minst hvor grunnleggende viktig det er at disse prinsippene kan håndheves som overordnet den utøvende (og om nødvendig den lovgivende) makts vilje, av uavhengige domstoler.

Rettsstaten er ryggraden i et fungerende demokrati. Varsleren Ellsberg gikk juridisk, om ikke personlig, skadefri fra prosessen. Ytringsfriheten fikk en av sine viktigste seiere i amerikansk rettshistorie, i den berømte høyesterettsavgjørelsen *New York Times Co v United States*. Og den offentliggjorte informasjonen bidro vesentlig til USAs avslutning av Vietnamkrigen. Alt fordi noen mennesker var utover normalt modige, og trosset både statsmakten og dens

---

[11] "Mener Norge vil bli mer utsatt for terror", Aftenpostens nettutgave 11.04.10 http://www.aftenposten.no/nyheter/iriks/article3601417.ece (lastet ned 12.04.10)

jurister, og fordi rettsvesenet opptrådte uavhengig av den utøvende makt, og håndhevet konstitusjonens prinsipper.

Det er bare få år siden avisen Verdens Gang avslørte at daværende forsvarsminister Anne-Grete Strøm-Erichsen hadde bedt PST om å etterforske avisens anonyme kilder, etter avsløring av de reelle kostnadene forbundet med flytting av Fellesoperativt hovedkvarter fra Stavanger til Bodø.[2]

Verken USAs, Europas eller våre hjemlige politikere later å ha lært av slike og andre, senere eksempler. Det pågår for tiden en sterk utvikling – i akademiske kretser ofte betegnet som et paradigmeskifte – i europeisk lovgivertenkning når det gjelder villighet til å la normale rettsstatsprinsipper og hevdvunne liberale rettigheter innskrenkes til fordel for en mer preaktiv strafferett og innføring av sterkere kontroll- og tvangsmidler for staten i kriminalitetsbekjempelsens navn. En bevegelse på skalaen mellom den liberale rettsstat og politistaten, i retning av sistnevnte.

Det skjer nærmest uten større offentlig debatt – og gjennomgående i strid med anbefalinger og advarsler fra uavhengige ekspertorganer og akademikere innenfor feltene menneskerettigheter og strafferett. Denne utviklingen har skutt fart etter terrorhandlingene i USA i 2001, og senere i Madrid og London. DLD er direkte foranlediget av disse hendelsene, jf direktivets fortale.

Det dreier seg dels om kriminalisering av handlinger langt utenfor det tradisjonelt straffverdige, hvor gjerningspersonens subjektive hensikt (tanker) blir avgjørende for handlingens objektive straffbarhet (straffelegging av ulike typer forberedelseshandlinger, blant annet terrorfinansiering). Dels om innføring av "skyldpresumsjoner" som utgangspunkt for statens mulighet til å benytte inngripende, preaktive tiltak mot personer hvis forbindelser oppfyller visse objektive vilkår (FNs terrorlister og frysing av økonomiske verdier). Og om utvidelser av de hemmelige tjenesters fullmakter til å bruke skjulte tvangsmidler (kommunikasjonskontroll, avlytting og annen innsamling av personopplysninger) før det foreligger mistanke om straffbart forhold – såkalte "undersøkelser i forebyggende øyemed".

I Norge i dag skal det meget lite til før PST formelt vil ha adgang til i hemmelighet å foreta kommunikasjonskontroll (tilgang til trafikkdata fra teletilbydere, avlytting av kommunikasjon, osv) og andre personundersøkelser av en bestemt borger eller gruppe av borgere, registrere opplysningene og løpende holde vedkommende under oppsikt – i rent "forebyggende øyemed", uten at det noensinne tas ut siktelse for straffbart forhold.

I prinsippet er det nok at en person forsøker å samle inn eller låne penger til en person eller organisasjon som anses å være kontrollert av noen som (uten judisiell prøving, og nærmest uten mulighet til å bestride oppføringen) er oppført på FNs sikkerhetsråds terrorlister, eller noen som forsøker å "forberede" en vagt definert terrorhandling, ved å forsøke å inngå "forbund" med andre om å planlegge slike handlinger. Objektivt sett kan dette ramme arrangøren av et lokalt kakelotteri, dersom pengene er ment å gå til en motstandsbevegelse i en diktaturstat et sted i verden, hvis bevegelsen anses å ha forbindelser til internasjonal terrorvirksomhet.

---

[2] "Hysjen beordret på kildejakt etter VG-avsløring", vg.no 26.06.08: http://www.vg.no/nyheter/innenriks/artikkel.php?artid=501063 (lastet ned 12.04.10)

Dette illustrerer hvorfor det er essensielt å se flere tiltak i sammenheng når man skal vurdere det totale kontroll- og overvåkningstrykket i samfunnet. Skal man kunne overskue for eksempel effekten av slik tvungen masseregistrering og -lagring av personopplysinger som DLD forutsetter, kan det ikke gjøres uten at man samtidig ser på vilkårene for politiets (og PSTs) og samarbeidende utenlandske myndigheters tilgang til opplysningene. Vilkårene for tilgang kan ikke vurderes uten at man samtidig analyserer hvilke handlinger som er definert som kriminelle – fordi de prosessuelle reglene om bruk av kommunikasjonskontroll og liknende jo knyttes til etterforskning, eventuelt forebygging, av bestemte handlinger. Jo videre de straffbare handlinger er definert, jo videre blir for eksempel PSTs fullmakter til å overvåke borgerne og/eller gi fremmede etterretningstjenester tilgang til opplysninger.

Det primære formål med svært mange straffebestemmelser som rammer forberedelser er i virkeligheten ikke å straffe – det vil ytterst sjelden kunne skje på grunn av bevisvansker, i sær med å påvise forbryters sinnelag , men å å kunne iverksette hemmelige undersøkelser og kontroll av personer og miljøer som myndighetene for eksempel mener det er grunn til å tro at forbereder å forbryte seg mot rikets sikkerhet eller å inngå avtale om en senere terrorhandling. Grensen mot ren politisk overvåkning kan bli meget diffus, og misbrukspotensialet er iøynefallende. Dette er påpekt av blant andre professor Erling Johannes Husabø i problemnotat om kriminalisering av forberedelseshandlinger, utarbeidet som ledd i forarbeidene til våre nye terrorbestemmelser i straffeloven §§ 147a og 147b.[3] Fra notatet hitsettes følgende:

> *"I kva grad ei kriminalisering vil medføra auka politikontroll og inngrep i uskuldige sin «private sfære», er likevel avhengig av fleire faktorar. Ein viktig faktor er naturlegvis kva ressursar overvakingstenesta og politiet elles har å setja inn på telefonavlytting o l. Ein annan viktig faktor er utforminga av det enkelte straffebodet. Faren for unødige inngrep i folk sitt privatliv synest å vera særleg stor dersom det aktuelle straffebodet er vagt formulert. Då er det grunn til å tru at domstolane vil ha vanskelegare for å overprøva påtalemakta sine ønskjemål og vurderingar. I denne samanheng kan det vera grunn til å nemna at § 104a andre ledd blir forholdsvis mykje nytta som grunnlag for telefonavlytting og andre tvangsmidlar, endå det visstnok enno ikkje har skjedd noko domfelling etter denne regelen.*
>
> *Ein tredje faktor er kva tersklar som vert sett for å ta i bruk ulike typar tvangsmidlar. Slik som reglane om tvangsmidlar i dag er utforma, er det ei kopling mellom straffebodet si strafferamme og kva tvangsmidlar som kan nyttast. Denne koplinga kan lovgivar likevel velja å bryta. Eit forslag om å utvida tilgangen på etterforskingsmetodar i saker om strl. kap. 8 og 9, er sett fram i høyringsnotatet om terrortiltak. Som kjent drøftar eit eige utval dessutan bruken av særskilte etterforskingsmetodar på breiare grunnlag. Her nøyer eg meg difor med å peika på behovet for å sjå dei materielle og prosessuelle reglane i samanheng når ein skal finna ein rimeleg balanse mellom omsynet til effektivitet og rettstryggleik."*

---

[3] Erling Johannes Husabø, "Problemnotat til revisjonen av straffelova kap. 8 og 9 mv.", inntatt i NOU 2003:18 Rikest sikkerhet

På et mer generelt plan – helt uten de rettssikkerhetsgarantier som tross alt finnes i straffeprosessen – kombineres slike tiltak på europeisk nivå med utvikling av mer generelle og avanserte overvåkningssystemer (på internett og på offentlige steder), samt kobling av slike systemer og andre systemer for masseinnsamling av personopplysninger (flypassasjerlister og lignende), hvor hensikten generelt er sosial kontroll og spesielt å kunne fange opp såkalt "abnormal behaviour". Eksempler er EU-prosjektene INDECT – Intelligent information system supporting observation, searching and detection for security of citizens in urban environment, og ADABTS – Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces).

Eksemplene er mange. Og gjennom blant annet Schengen-, Prüm- og Europol-samarbeidet er tanken at alle disse systemer og registre med personopplysninger i så stor grad som mulig skal kunne kobles og være gjenstand for utveksling mellom politi og hemmelig tjenester over landegrensene. At DLD ses i dette perspektivet, bekreftes av PST-sjefens uttalelser til Aftenposten i går, gjengitt ovenfor.

Det er i det hele tatt snakk om utviklingen av et felleseuropeisk kontrollregime, hvor statens kontroll med borgerne, deres bevegelser og nettverk, settes i hovedsetet, av diverse trygghets- og sikkerhetshensyn. Hensynet til liberale rettstatsverdier som rettssikkerhet, personvern og kommunikasjonsfrihet blir – i den grad de vies oppmerksomhet overhodet i dette mildt sagt uoversiktlige totalbildet – behandlet som om de er begreper som det er nok å henvise til, for at de skal være ivaretatt. En hovedfaktor bak denne utviklingen er krigsretorikken som benyttes i forbindelse med bekjempelse av terror og annen organisert kriminalitet, som tilsynelatende skal forsvare innføring av lovgivning som man ellers forbinder med akutte unntakstilstander hvor nasjonens liv er truet. Også på dette punkt gir professor Husabø viktige betraktninger i tidligere refererte problemnotat:

> *"I dag er det ikkje minst terrortrusselen som gjer det nødvendig med ei ny gjennomtenking av korleis situasjonsavgrensinga til dei ulike reglane bør utformast. I denne samanhengen må ein drøfta om det er treffande å hevda at vi går inn i ein periode av «kronisk unntakstilstand». Med dette siktar ein vel til at reglar og verkemiddel som før berre vart nytta i unntakssituasjonar, no må nyttast meir permanent. Med ein slik tenkjemåte vil ein viska ut skiljet mellom reglar for normalsituasjonar og reglar for unntakssituasjonar.*
>
> *Som utvalet sin formann peika på i ein kronikk i Aftenposten i fjor haust, er det lang tradisjon for å ha særreglar for krig og andre unntakssituasjonar. Også menneskerettskonvensjonane har reglar om unntakssituasjonar, jf EMK art. 15 om «krig eller annen nødstilstand som truer nasjonens liv». I slike tilfelle tillet EMK innskrenkingar i t d ytringsfridomen og privatlivet som normalt ikkje vil stå seg mot menneskerettane.*
>
> *Den prinsipielle tenkinga bak dette er viktig, og har samanheng med synet på ein rettsstat og kva grunnleggjande verdiar staten skal verna. Kanskje kan vi seia det slik at i denne typen «skjebnetider for landet» er dei mest sentrale verdiane (liv, fridom m v) trua på brei front. Då må staten også, for å verja om desse verdiane og gjenoppretta ein normalsituasjon, kunna stilla særlege krav til kva folket må tola og yta. Dersom vi let tanken om ein «kronisk» unntakstilstand få gjennomslag, endrar samtidig relasjonen mellom individ og stat karakter. Målet om eit «fritt» samfunn*

vert forlate, og fridomen i den «private sfære» må permanent vika plass for statleg kontroll og overvaking.

Etter mitt syn er det særs viktig å unngå at redsla for krig og terror skal unødig svekkja folket sin fridom og rettstryggleik i meir normale tider. Sjølv om utfordringa er stor, bør utvalet difor gjera det tydeleg kva som skal vera reglar for unntakssituasjonar og kva reglar som skal gjelda meir generelt. Dette er også av stor betydning for å imøtekoma det «Bestimmtheitsgebot» som ligg i legalitetsprinsippet."[4]

Dette er også påpekt av mange uavhengige ekspertorganer, herunder i den omfattende rapporten "Assessing damage, urging action" fra februar 2009, initiert av Den internasjonale juristkommisjon – som da den ble publisert ble gjenstand for fyldig omtale i verdenspressen (men knapt ble nevnt i Norge).[5] Også FNs spesialrapportør innenfor feltet terrorbekjempelse og menneskerettigheter, Martin Scheinin, har blant andre påpekt og advart mot denne utviklingen i sine rapporter til FNs menneskerettighetskomité. I sin seneste rapport til komitéen i desember 2009 nevner han blant annet særskilt Datalagringsdirektvet.

Også europeiske domstoler har gjennom enkeltavgjørelser satt til side og/eller sterkt begrenset flere av de anti-terrorlover som er innført i Europa de seneste ti årene. Et fellesbudskap i flere av disse avgjørelsene er at det ikke er unntakstilstand i Europa, og at det heller ikke kan fires på de alminnelige kravene til rettssikkerhet og proporsjonalitet når staten skal gjøre inngrep i borgernes grunnleggende, demokratiske friheter. Menneskerettsdomstolen har tvert om gjentatte ganger understreket at selv om visse kontroll- og overvåkningstiltak kan være nødvendige for å sikre samfunnet og demokratiet mot angrep på dets institusjoner, vil de som typiske elementer i en politistat snarere kunne bidra til "undermining or even destroying democracy on the ground of defending it". I en av de britiske høyesterettsavgjørelser som har satt til side anti-terrorlover, ordla Lord Hoffmann seg slik:

"Of course the government has a duty to protect the lives and property of its citizens. But that is a duty which it owes all the time and which it must discharge without destroying our constitutional freedoms. I do not underestimate the ability of fanatical groups of terrorists to kill and destroy, but they do not threaten the life of the nation. Whether we would survive Hitler hung in the balance, but there is no doubt that we shall survive Al-Qaeda (...) Terrorist violence, serious as it is, does not threaten our institutions of government or our existence as a civil community. The real threat to the life of the nation, in the sense of a people living in accordance with its traditional laws and political values, comes not from terrorism but from laws such as these. That is the true measure of what terrorism may achieve."[6]

Alle disse klare meldingene fra uavhengige jurister, herunder i domstolene – rettsstatens voktere – til tross: De politiske myndighetene synes å jobbe ufortrødent videre på sitt (og, paradoksalt nok, terroristenes) prosjekt med sakte, men sikkert å omdanne det Europa som i

---

[4] Husabø, op. cit.

[5] Kan lastes ned via ICJs nettsider her http://icj.org/news.php3?id_article=4453_〈=en

[6] House of Lords, *A and others vs Secretary of State for the Home Department,* dom av 16.12.04

et halvt århundre har vært modellen for den liberale, demokratiske rettsstat, til et repressivt kontrollsamfunn som vi aldri ville ha kunnet vedkjenne oss for bare få år siden. [7]

Når endog dagligdagse handlinger og forbindelser er gjort potensielt straffbare, og de som foretar dem til potensielle overvåkningsobjekter, blir det desto mer usikkert for borgerne hva som av myndighetene legges i ikke-rettslige begreper som "abnormal oppførsel" – som kan medføre at grenseoverskridende, automatiserte overvåkningssystemer peiler en inn for nærmere analyse, på en eller annen myndighets kontor, et sted i Europa.

At Justisdepartementet og andre som støtter innføringen av DLD, på denne bakgrunn anser det som uproblematisk at opplysninger om alle vår kommunikasjonsmønstre og -nettverk skal tvangslagres for politiformål, vitner dessverre om en stat som later til å ha glemt hvilke prinsipper som har hittil vært gjeldende for statlig innsamling, registrering og lagring av personopplysinger i europeisk og norsk rett – og da særlig etter EMK, slik konvensjonen er håndhevet av EMD. Vi finner grunn til å minne om disse:

DLD OG MENNESKERETTIGHETENE

Hovedprinsipper om lagring av personopplysninger i Europeisk rett – særlig om trafikkdata

En vesentlig bakgrunn for å forstå hvordan innsamling, registrering og lagring av personopplysninger vurderes etter EMK, er utformingen av de øvrige felleseuropeiske konvensjoner og direktiver som hittil har regulert spørsmålene.

De viktigste av disse er:

- Europarådets konvensjon av 20. januar 1981 nr. 108 om personvern i forbindelse med elektronisk behandling av personopplysninger (persondatakonvensjonen)
- EU-direktiv 1995/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger (personopplysningsdirektivet)
- EU-direktiv 2002/58/EF om behandling av personopplysninger og beskyttelse av privatlivets fred i den elektroniske kommunikasjonssektor (kommunikasjonsdirektivet)

Innenfor Europarådet er persondatakonvensjonen senere fulgt opp med en særlig anbefaling fra ministerkomiteen om bruk av persondata i politisektoren.[8] Anbefalingen inneholder detaljerte prinsipper om vilkår for innsamling, lagring, sikring samt bruk av personopplysninger for kriminalitetsbekjempelse, og ikke minst sletting av slike personopplysninger. Det går tydelig frem av disse at man her har hatt for øye det alminnelige etterforskningsprinsipp – at det skal foreligge en konkret mistanke og en

---

[7] I norsk/nordisk sammenheng kan det henvises generelt til artikler av blant andre professor i strafferett ved Københavns Universitet, Vagn Greve, Riksadvokat Tor-Aksel Busch og høyesterettsdommer Ketil Lund i den nylig utgitte boken *"Til forsvar for personvernet"*, Kristin Clemet og John O. Egeland (red.) (Universitetsforlaget 2010) – som alle advarer mot den omtalte utviklingen.

[8] Recommendation No R (87) 15 – Regulating the use of personal data in the police sector, som er forankret i både persondatakonvensjonen og EMK artikkel 8, listet opp en rekke prinsipper for innsamling, lagring og håndtering av personopplysninger for politiformål.

relevant og forholdsmessig begrunnelse for registrering av den enkelte personopplysning, og videre at opplysninger skal slettes så snart disse vilkårene ikke lenger er tilstede.

EMD refererer selv regelmessig til så vel persondatakonvensjonen som til ministerkomiteens anbefaling, i saker som angår statenes håndtering av persondata.[9]

Grunnprinsippene i de nevnte EU-direktivene er de samme, om enn utpenslet i større detalj når det gjelder særlig persondata fra elektroniske kommunikasjonssystemer (naturlig nok, da de er vedtatt langt senere).

Felles for disse internasjonale regelsettene er at de alle – blant annet under henvisning til EMK – bygger på utgangspunktet om vern av personopplysninger og av privatlivets fred – herunder kommunikasjonsfortroligheten.

Videre forutsetter de at selve registreringen og lagringen av personopplysninger – selv når det skjer i henhold til avtale mellom vedkommende person og for eksempel tilbyder av teletjenester – skal begrenses i omfang og tid til det som er strengt nødvendig for gjennomføring av tjenesten og administrasjon av kundeforholdet. Deretter skal opplysningene slettes.

For trafikkdata går dette uttrykkelig frem av kommunikasjonsdirektivet artikkel 6. I direktivets fortale avsnitt 30 understrekes generelt at:

" [S]ystemer til levering af elektroniske kommunikationsnet og kommunikationstjenester bør konstrueres, så de begrænser mængden af nødvendige personoplysninger til et absolut minimum."

Etter kommunikasjonsdirektivet og de øvrige direktiver og konvensjoner nevnt ovenfor, er altså registrering og lagring av personopplysningeret eventuelt nødvendig onde som bør begrenses i størst mulig grad. Ministerkomiteens anbefaling angående innsamling m.v. av personopplysninger til politiformål, presiserer disse prinsippenes anvendelse i kriminalitetsbekjempelsen. Kommunikasjonsdirektivets artikkel 15 nr 1 sier at selv om dens regler om bl.a. trafikkdata ikke er til hinder for bruk av lagrede opplysninger til kriminalitetsbekjempelse, skal slik bruk være "nødvendig, passende og forholdsmæssig i et demokratisk samfund".

At EU selv erkjenner at den tvangsmessige masselagring av trafikkdata til politiformål som DLD krever, innebærer et klart brudd med disse grunnprinsippene, fremgår av DLDs egne bestemmelser:

DLD artikkel 3 nr 1 fraviker uttykkelig kommunikasjonsdirektivets regler om lagring og sletting av blant annet trafikkdata, jf. kommunikasjonsdirektivet artikkel 6. Og DLD artikkel 11 innfører et nytt ledd 1 a til kommunikasjonsdirektivet artikkel 15, hvor det sies at artikkel 15 nr 1 (jf. ovenfor) ikke gjelder for data som lagres i henhold til DLD. Ingen av disse bestemmelsene hadde vært nødvendige, dersom DLD hadde kunnet vedtas innenfor rammen av kommunikasjonsdirektivet.

Det er også interessant å se hvordan Europarådet og norsk lovgiver i nyere tid, avveide hensynet til på den ene siden behovet for ytterligere sikring av trafikkdata i

[9] Se eksempelvis *S og Marper mot Storbritannia*, dom 4. desember 2008.

kriminalitetsbekjempelsen og respekt for personvern og kommunikasjonsfrihet på den annen side.

Europarådets konvensjon av 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (Datakriminalitetskonvensjonen), ble utarbeidet og vedtatt nettopp med henblikk på å effektivisere kriminalitetsbekjempelsen i forhold til utviklingen av elektroniske kommunikasjonsmedier.

Datakriminalitetskonvensjonen pålegger konvensjonsstatene å innføre en rekke strafferettslige og straffeprosessuelle tiltak for bedre å kunne bekjempe alvorlige kriminalitet som enten skjer ved bruk av elektronisk kommunikasjon, eller slik at elektroniske spor er viktige for etterforskningen av forholdene. Konvensjonens artikkel 16 pålegger statene å ha regler som muliggjør *midlertidig sikring av blant annet trafikkdata* som antas å kunne ha betydning som bevis i en konkret straffesak.

Det er altså ikke snakk om generell plikt til lagring trafikkdata, men om målrettet bevissikring som tvangsmiddel under etterforskning. Konvensjonsforpliktelsen ble i norsk rett gjennomført ved vedtagelsen av straffeprosessloven § 215 a, hvoretter påtalemyndigheten som ledd i etterforskning kan "gi pålegg om sikring av elektronisk lagrede data som antas å ha betydning som bevis", jf første ledd.

Av forarbeidene til bestemmelsen fremgår at det var diskusjon om det burde stilles strengere vilkår for et slikt sikringspålegg, for eksempel krav om skjellig grunn til mistanke.[10] Under henvisning til at sikringspålegg ikke innebar at politiet fikk tilgang til de sikrede data, og at politiet burde ha mulighet til å sikre lagring av data på et så tidlig stadium av etterforskningen som mulig, valgte Justisdepartementet den vedtatte løsningen. Det ble i den forbindelse vist til at de personvern- og rettssikkerhetsmessige betenkeligheter forbundet med å tillate en så vid ramme for sikringspålegg,, til en viss grad ville kunne avhjelpes ved forholdsmessighetsvilkåret i straffeprosessloven § 170a.

Denne gjennomgangen av grunnprinsippene i europeisk personvernrett frem til DLD, viser to vesentlige poenger:

1) at selve innsamlingen og lagringen av personopplysninger, herunder trafikkdata, regnes som et selvstendig inngrep som må kunne forsvares som nødvendig og forholdsmessig, uavhengig av vilkårene for myndighetenes eventuelle tilgang til opplysningene, og 2) at Europarådet og senere norsk lovgiver så sent som i 2005, mente at den midlertidige tvangslagring av trafikkdata hjemlet i straffeprosessloven § 215a, var så langt det var nødvendig og forholdsmessig å gjøre inngrep i personvernet.

DLD som vilkårlig massebevissikring – forholdet til EMK

EUs Datalagringsdirektiv kan – og bør etter ICJ-Norges syn – i et norsk perspektiv sees på som en massiv utvidelse av den form for bevissikring av trafikkdata som straffeprosessloven § 215a i dag gir adgang til.

Selv om dagens regel kan medføre tvangslagring av forholdsvis store mengder trafikkdata om kommunikasjon mellom mange uskyldige mennesker, begrenses som nevnt likevel

[10] Ot prp nr 40 (2004-2005) kapittel 4.2

adgangen av at sikringspålegget må relatere seg til en *konkret etterforskning*, og av at de trafikkdata som sikres antas å ha betydning som bevis i denne – i tillegg til det alminnelige forholdsmessighetsprinsipp i straffeprosessen.

DLD innebærer at alle borgernes trafikkdata skal lagres i minst et halvt år – helt uavhengig av slike krav og vilkår som gjelder for sikringspålegg etter dagens system.

Spørsmålet er om slik tvangsregistrering og -lagring er forenlig med EMKs krav til respekt for særlig personvernet/retten til privat kommunikasjon, jf EMK artikkel 8.

At blant annet trafikkdata omfattes av den typen personopplysninger som er beskyttet av EMK artikkel 8 er sikker rett, noe som ble slått fast allerede i 1984 i EMDs avgjørelse i saken *Malone mot Storbritannia*. Dette er bekreftet i en rekke senere avgjørelser.

Videre er det slått fast av EMD at *selve lagringen* av slike opplysninger utgjør et inngrep i artikkel 8, når det skjer uten borgernes samtykke, *uavhengig* av om og på hvilke vilkår staten senere kan få tilgang til/bruke de lagrede opplysningene, jf for eksempel EMDs avgjørelser i sakene *Leander mot Sverige* og *Amann mot Sveits*.

Ettersom den lagringen som DLD forutsetter, utvilsomt utgjør et inngrep i artikkel 8 (1), er spørsmålet om inngrepsvilkårene i artikkel 8 (2) er oppfylt.

For at inngrep skal kunne aksepteres, kreves at 1) inngrepet er hjemlet i nasjonal lovgivning på en tilstrekkelig klar måte, 2) at inngrepet er begrunnet i de opplistede samfunnsmessige hensyn – i dette tilfellet typisk nasjonal sikkerhet, forebygging av kriminalitet og/eller beskyttelse av andres rettigheter – og 3) at inngrepet er nødvendig i et demokratisk samfunn for å ivareta de anførte hensynene.

De to første vilkårene vil neppe volde problemer, dersom direktivet implementeres på en alminnelig, oversiktlig måte i norsk lovgivning. Kjernespørsmålet blir derfor om det tredje vilkåret – *nødvendighetskravet* – kan anses oppfylt.

Nødvendighetskravet er av EMD presisert slik at det fra statens side må godtgjøres at det foreligger et *presserende samfunnsmessig behov* (pressing social need) for inngrepet, overfor det enkelte individ som rammes. Det er ikke tilstrekkelig at inngrepet er nyttig eller hensiktsmessig – det skal være nødvendig. Det må påvises at inngrepet er egnet til å ivareta de hensyn som begrunner det, at de samme hensyn ikke kan ivaretas på alternative, mindre inngripende måter og at det alt i alt er proporsjonalitet mellom "mål og middel".

EMD har hittil aldri tatt stilling til en helt parallell sak – altså om tvangsmessig masselagring av trafikkdata til politiformål, men uavhengig av konkret etterforskning.

EMD har imidlertid tatt stilling til flere tilfeller av bruk av straffeprosessuell kommunikasjonskontroll – noe som prinsipielt er godtatt som virkemiddel i kriminalitetsbekjempelse, når kontrollen skjer som ledd i etterforskning av konkrete saker eller målrettet etterretning, og de nødvendige rettssikkerhetsgarantiene er på plass, både i forhold til forutberegnelighet og proporsjonalitet.

Videre har EMD tatt stilling til tilfeller av såkalt "strategisk overvåkning" av elektroniske kommunikasjonsnettverk. Konkret har dette dreid seg om henholdsvis Tysklands og Storbritannias etterretningstjenesters systemer for overvåkning av i prinsippet all elektronisk

kommunikasjon som passerer statsgrensene, jf EMDs avgjørelser i sakene henholdsvis *Weber og Saravia mot Tyskland* og *Liberty m fl mot Storbritannia.* Formålet med begge systemene var å forebygge og bekjempe terrorisme og annen, alvorlig og grenseoverskridende kriminalitet som kunne true rikets sikkerhet eller sentrale samfunnsinstitusjoner.

EMD godtar i prinsippet slike systemer, men stiller strenge krav til gode og effektive garantier mot misbruk. Det som skiller disse sakene fra den typen lagring som DLD legger opp til, er at det allerede i overvåkningsteknologien lå en filtreringsmekanisme, ved at det kun er kommunikasjon som tilfredsstiller bestemte søkekriterier, som i det hele tatt fanges opp og kan bli gjenstand for nærmere bearbeiding, analyse og lagring. Det var derfor ikke slik at all kommunikasjonen, verken trafikkdataene eller innholdet i utgangspunktet blir registrert/lagret. Av de nevnte avgjørelsene fremgår tvert om at EMD stilte ganske strenge vilkår til hvordan søkekriteriene ble valgt ut og til hvilken kontroll som eksisterte med også denne delen av systemet. Av de opplysningene som ble fanget opp for videre behandling, stilte EMD dessuten strenge krav til både kriteriene for at trafikkdata/kommunikasjonsinnhold kunne bli gjenstand for videre granskning og/eller lagring – samt til sletting av informasjon som ikke var relevant i forhold til å avdekke slik kriminell virksomhet som hjemlet overvåkningen. I sum, ble det stilt slike krav til systemet at innsamlingen, bearbeidingen og lagringen av blant annet trafikkdata ble så målrettet som mulig. Her sviktet det i Storbritannias tilfelle, og det ble derfor konstatert krenkelse av EMK.

Den eneste EMD-avgjørelsen som behandler et tilfelle med klare paralleller til den typen preaktiv masselagring som DLD legger opp til, er dommen fra 2008 i saken *S. og Marper mot Storbritannia*.

I den saken var det snakk om registrering og lagring av fingeravtrykk, celleprøver og DNA-profiler av personer som hadde vært mistenkt, men ikke dømt for straffbare forhold. Formålet med å beholde opplysningene registrert var utelukkende å bidra til å bygge opp en database over slike opplysninger, til bruk i fremtidig kriminalitetsbekjempelse. Slik at fingeravtrykk og/eller DNA-spor som ble funnet under etterforskning av fremtidige straffesaker, kunne sjekkes mot registeret. Opplysningene ville aldri bli brukt, med mindre vedkommende person ble involvert som mistenkt i et fremtidig straffbart forhold

EMD aksepterte ikke denne registreringen som nødvendig i et demokratisk samfunn, selv om den aksepterte at de registrerte opplysningene ville kunne effektivisere kriminalitetsbekjempelsen

EMD slo for det første fast – under henvisning til tidligere praksis – at lagring av personopplysninger utgjorde et inngrep i seg selv, uavhengig av eventuell bruk av de lagrede opplysningene. Dermed avviste EMD statens anførsel om at borgerne hvis opplysninger var lagret, ikke ble utsatt for noe nevneverdig inngrep så lenge opplysningene aldri ville bli brukt med mindre deres fingeravtrykk eller DNA knyttet dem til fremtidige straffbare handlinger.

For øvrig la EMD vekt på lagringens helt generelle karakter, at den skjedde uavhengig av hva den enkelte hadde vært mistenkt for eller av andre utvelgelseskriterier, at lagringen var tidsubestemt og at lagring av ikke-dømte personers opplysninger i et slikt register, også støtet an mot uskyldspresumsjonen. Det siste momentet gjorde seg særskilt gjeldende når

de registrerte enten aldri var blitt tiltalt eller hadde blitt frifunnet. De burde ha krav på å behandles likt med andre uskyldige borgere.

Kombinasjonen av denne avgjørelsen og EMDs praksis vedrørende diverse former for kommunikasjonskontroll og annen behandling av kommunikasjonsdata, viser at ikke-målrettet, tvangsmessig og generell masselagring av alminnelige borgeres personopplysninger, uavhengig av noen konkret etterforskning, vil ha store problemer med å passere EMDs normale krav til proporsjonalitet.

Dersom man skulle akseptere slik masselagring så lenge de prosessuelle vilkårene for bruk av opplysningene var strenge nok, ville den logiske konsekvensen fort bli at staten kunne kreve generell tvangslagring av en rekke opplysninger om oss og vår gjøren og laden på flere livsområder som anses som nyttige i kriminalitetsbekjempelse og/eller andre viktige samfunnsoppgaver.

Dette synes umulig å forene med den grunnholdning EMD har gitt uttrykk for i alle slike saker, hvor den som vist har presisert at lagring i seg selv utgjør et inngrep som må kunne forsvares som nødvendig i et demokratisk samfunn.

EMD vil derfor måtte overbevises om at verden har forandret seg ganske drastisk de seneste årene – som nevnt ovenfor, mot en slags kronisk unntakstilstand – dersom en konvensjonsstat skal kunne vinne frem med at slik registrering og lagring som DLD krever, skal ha håp om å passere proporsjonalitetstesten i EMK artikkel 8 (2).[11]

I Romania har forfatningsdomstolen allerede slått fast at implementeringen av direktivet i rumensk rett er i strid med rumensk grunnlov og med Romanias forpliktelser etter EMK artikkel 8 (dom av 08.10.09). I Tyskland har forfatningsdomstolen (dom av 02.03.10) slått fast at implementeringen av direktivet i tysk rett er grunnlovstridig – og selv om den sier at lagring av trafikkdata *kan* være grunnlovsmessig, stiller den i realiteten så vidt strenge krav at en full implementering blir krevende å gjennomføre for tysk lovgiver. Forfatningsdomstolen tok *ikke* stilling til forholdet til EMK.

Forholdet til ytringsfriheten – særlig om vernet for varslere og pressens kilder

Som vist foran, er personvernet, herunder vernet om retten til fortrolig, privat kommunikasjon, nært forbundet med ytringsfriheten – på flere måter.

For det første er borgernes rett til å kommunisere fritt seg imellom i fortrolighet både med hensyn til innhold og til tid, sted og mønster for kommunikasjonen, en fortsetning for den enkeltes selvutfoldelse som individ.

Følelsen av å være overvåket – ved at slike opplysninger kontinuerlig registreres og lagres – virker dokumentert hemmende på mange. I Tyskland ble det publisert en undersøkelse som bekreftet at betydelige andeler av referansegruppen endret adferdsmønster i sin bruk av elektronisk kommunikasjon, etter at DLD var innført.[12] Det gikk blant annet frem at over halvparten av dem uttrykte skepsis til å kommunisere med for eksempel sine psykologer

---

[11] Se også Jon Wessel-Aas, "Datalagringsdirektivet og EMK – kommentarer til Ingvild Bruce", *Lov og Rett nr 3 2010 s 154-164*, med nærmere analyse og henvisninger.

[12] http://www.kreativrauschen.com/blog/2008/06/04/data-retention-effectively-changes-the-behavior-of-citizens-in-germany/ (lastet ned 12.04.10)

eller med eventuelle rusrådgivere via elektroniske medier – av frykt for at lagrede data om slik kommunikasjon kunne komme uvedkommende i hende. Slike undersøkelser bekrefter at slike virkninger ikke bare er teoretiske, selv om det nødvendigvis er vanskelig å måle slikt.

Retten til fortrolig privatkommunikasjon og tilliten til at den er reell, er også en forutsetning for den enkeltes mulighet til å prøve ut sine meninger og sine tanker i private sammenhenger, for derved å kunne danne seg et grunnlag for å kunne delta i den offentlige debatt om samfunnsspørsmål, uten å måtte frykte at privat prøving og feiling blir brukt mot en i uvedkommende sammenhenger.

Videre er den en forutsetning for at enkeltindivider kan knyttes sammen i diskusjonsfora og eventuelt etablere tettere forbindelser som politiske grupperinger som ønsker å utfordre det regjerende politiske flertallet på demokratisk vis – uten at myndighetene har innsyn i disse private forbindelsene, og i tillit til at myndighetene eller andre uvedkommende heller ikke kan få innsyn i dem. Dette er en forutsetning for at samfunnet løpende kan utvikle og vedlikeholde en levende og kritisk opposisjon til den til enhver tid regjerende flertallsmakten. Hvis tilliten til at disse forutsetningene ikke er til stede – fordi den enkelte har eller opplever å ha manglende kontroll over hvem som har tilgang til opplysninger om sine private forbindelser og bevegelsesmønstre – skaper mistilliten en naturlig demping av den enkeltes frimodighet. Dermed reduseres også vekstvilkårene for nettopp den kritiske opposisjon som er nødvendig for å bevare dynamikken i selve demokratiet.

Illustrerende i den sammenhengen er betydningen av vernet for varslere og for pressens kilder, når disse bringer ut opplysninger om kritikkverdige eller andre forhold ved statlige eller private aktørers forvaltning av sin samfunnsmakt.

Eksempelet som ble trukket frem ovenfor, om varsleren Daniel Ellsberg og "The Pentagon Papers", fra 1970-årenes USA, er høyst aktuelt i dag, i 2010. Varslere er ikke blitt mindre viktige for den demokratiske kontrollen med myndighetene.

På grunn av faren for at rettmessig varsling, ofte i "strid" med formell taushetsplikt, kan føre til formelle og uformelle sanksjoner mot varsleren fra den statlige eller private institusjonen som varslingen "går ut over", er det viktig med rettslig beskyttelse av slik virksomhet. Til en viss grad har norsk lovgivning tatt dette til etterretning, blant annet gjennom reglene om pressens kildevern, eksempelvis i straffeprosessloven § 125. I nyere tid har vi også fått regler i arbeidsmiljøloven 2-4 og 2-5 – hvor henholdsvis arbeidstagers varslingsrett og forbud mot gjengjeldelser fra arbeidsgiver er lovfestet. Som det fremgår av bestemmelsenes forarbeider, er bestemmelsene nettopp begrunnet i ytringsfriheten og hensynet til "Sandhedssøgen" og "Demokrati", jf Grunnloven § 100, slik den lyder etter revisjonen i 2004.[13]

Kildevernet generelt er selvfølgelig også begrunnet i de samme hensyn, og det er håndhevet tydelig av EMD i flere avgjørelser over årene (jf særlig *Goodwin mot Storbritannia* og *Financial Times m fl mot Storbritannia*). At kildevernet også rammes av tiltak hvor lagring av blant annet trafikkdata fra kommunikasjon mellom pressens kilder og pressen, fremgår av dommen i *Weber og Saravia mot Tyskland:* Alene *muligheten* for at myndighetene kan avsløre hvem kildene er, utgjør et inngrep i ytringsfriheten, på grunn av den "chilling effect" dette kan ha på kildenes motivasjon for å bidra med informasjon.

---

[13] Ot prp nr 84 (2005-2006)

Ellsberg var nettopp en slik varsler, og bestemmelser om "rikets sikkerhet" ble forsøkt brukt mot både ham og mot pressen som han var kilde for. Tilsvarende bestemmelser har vi i dag i Norge i straffelovens kapittel 8. Forholdet mellom disse og ytringsfriheten er behandlet blant annet i NOU 2003:18 Rikets sikkerhet, særlig i punkt 6.2.3.5.

Forebygging og etterforskning av overtredelser av disse bestemmelsene ligger – naturlig nok – i kjernen av PSTs mandat, og som omtalt ovenfor, gir politiloven § 17d PST meget vide fullmakter til hemmelig overvåkning og andre inngripende tiltak i forebyggende øyemed på dette området.

Det derfor innlysende at praktiseringen av henholdsvis reglene om rettmessig varsling, ytringsfrihet og pressens kildevern på den ene side, og reglene om rikets sikkerhet og PSTs fullmakter til å forebygge og forfølge handlinger som *etter statens oppfatning,* utgjør en trussel mot rikets sikkerhet, står i et klart spenningsforhold til hverandre. Eksempelet om "The Pentagon Papers" illustrerer hvordan dette kan misbrukes. Det tidligere refererte eksempelet fra saken i VG i 2008, viser at også dagens norske regjering kan falle for fristelsen til – i beste fall – å tøye fullmaktene som finnes i dagens lovgivning, for å beskytte ikke rikets sikkerhet, men egen politisk makt.

At dette er en høyst aktuell problemstilling, og at den tankegangen som førte til at USAs myndigheter grovt misbrukte hensynet til rikets sikkerhet på 1970-tallet, slett ikke er forlatt, fikk vi et ferskt eksempel på i mars i år:

"Varslerinformasjonsnettstedet" Wikileaks, som tidligere har sørget for at dokumenter blant annet om ulovlig bruk av tortur som avhørsmetode overfor terrormistenkte i Guantanamo, la nylig ut en hemmeligstemplet, amerikansk Pentagon-rapport – hvor nettopp Wikileaks' virksomhet diskuteres, og hvor det fremgår hvordan amerikansk etterretning har vurdert og vurderer å stanse denne muligheten for varslere til å få ut informasjon anonymt.[14][15]

For det første illustrerer flere avsnitt i rapporten hvordan amerikansk etterretning ganske aggressivt tenker på å benytte nettopp tilsvarende metoder som overfor Ellsberg, for å skape hva man kan kalle en "chilling effect", for å skremme eventuelle varslere fra å gi ut informasjon via Wikileaks. Her er et eksempel:

> *"Web sites such as Wikileaks.org use trust as a center of gravity by protecting the anonymity and identity of the insiders, leakers, or whistleblowers. The identification, exposure, termination of employment, criminal prosecution, legal action against current or former insiders, leakers, or whistleblowers could potentially damage or destroy this center of gravity and deter others considering similar actions from using the Wikileaks.org Web site."*

Videre fremgår det at det vurderes hvilke tekniske muligheter som finnes for å "hacke" systemet, for å avsløre kildene m v, slik at ovennevnte metoder for å skremme folk fra å varsle kan anvendes:

> *"The obscurification technology used by Wikileaks.org has exploitable vulnerabilities. Organizations with properly trained cyber technicians, the proper equipment, and the*

---

[14] Se Wikileaks nettside: http://wikileaks.org

[15] Rapporten kan også lastes direkte ned her: https://docs.google.com/fileview?id=0B2Rh7x7YpF3KMGM5YTlkMTctNjliOC00YmEzLWE3NmEtMTE5OGM3ODliMzM2&hl=en

proper technical software could most likely conduct computer network exploitation (CNE) operations or use cyber tradecraft to obtain access to Wikileaks.org's Web site, information systems, or networks that may assist in identifying those persons supplying the data and the means by which they transmitted the data to Wikileaks.org."

Her diskuteres det med andre regelrett å skremme potensielle varslere fra å benytte seg av det som i utgangspunktet er deres *rett*, ved bevisst å ødelegge tilliten til at varslervern/kildevern vil respekteres, for derved å skape nettopp den "chilling effekt" som domstolene i så vel USA og Europa har understreket som en krenkelse av ytringsfriheten. Og i den grad det ikke hjelper, diskuteres muligheten for å bryte seg inn i de aktuelle databasene, for å få avslørt kildene til informasjon om statens egne menneskerettsbrudd.

Så vel vår norske, militære etterretning – E-tjenesten – som vår sivile etterretning – PST – arbeider tett med amerikansk etterretning, både direkte og via andre, europeiske stater. Det er både selvfølgelig og erkjent, jf blant annet PST-sjefens uttalelser til Aftenposten.no i går. Det er imidlertid også bekymringsfullt, når man ser at de holdninger som preget skandalen i Ellsberg-saken, lever i beste velgående i dag. Én sak er at tilgang til all informasjon som lagres om norske borgeres kommunikasjon, i tilfeller som objektivt sett dekkes av PSTs fullmakter til å foreta hemmelig overvåkning og kommunikasjonskontroll (herunder innhenting av trafikkdata), lovlig kan innhentes også etter forespørsel fra blant annet amerikanske etterretning. En annen sak, som bør bekymre, er at i alle fall amerikanske tjenester åpenbart ikke lar seg hindre av straffeprosessuelle begrensninger, når det gjelder å beskytte "rikets sikkerhet"; de er villige til å begå hva som ellers vil anses som regelrette datainnbrudd, for å avdekke hvem som er kilder for pressen og/eller organisasjoner som Wikileaks. Enhver database som inneholder slik informasjon – jf de enorme basene over trafikkdata som DLD krever, og som etter høringsnotatet skal ligge hos de enkelte teleselskapene og ISP'ene – vil derfor også være "fritt vilt" for slike, aggressive etterretningstjenester som USAs. Man kan bare tenke seg til hva andre, mer repressive regimers etterretningstjenester eller ikke-statlige agenter, vil kunne ønske å gjøre med slike databaser.

Det må på denne bakgrunn av helt ferske eksempler, kunne slås fast at det ikke er fraværet av et tiltak som DLD, men innføring av det, som utgjør en trussel mot vårt demokrati, jf sitatet fra den britiske høyesterettsdommer Lord Hoffmanns votum ovenfor.

DLDs manglende effektivitet i forhold til dets anførte formål

Etter ICJ-Norges oppfatning er det massive inngrep som et tiltak som DLD vil gjøre i personvernet og i ytringsfriheten, tilstrekkelig alvorlig til å konstatere at tiltaket er hindsides alle normale krav til proporsjonalitet – uavhengig av i hvilken grad slik registrering og lagring måtte bidra til økt avverging og/eller oppklaring av kriminalitet.

Enhver økning av statlig kontroll med og/eller overvåkning av borgernes privatliv og handlinger, vil selvsagt kunne bidra til at staten enklere vil kunne kontrollere borgernes adferd – og derved også kunne bidra til kriminalitetsbekjempelsen. Men i det perspektivet som er fremstilt ovenfor, kan dette i seg selv aldri bli styrende for hvilke inngrep som skal gjøres i borgernes rettssikkerhet eller grunnleggende friheter.

I dette tilfellet har verken EU eller den norske regjeringen bidratt med noen dokumentasjon for den reelle effekten av slik masseregistrering og lagring som foreslått. Norske myndigheter har simpelthen ikke sørget for å føre noen som helst objektiv statistikk over bruken av eller dokumentert nytte av den typen data i forbygging av eller generell bekjempelse av terror eller annen alvorlig, organisert kriminalitet som tiltaket er begrunnet i. Det ble til fulle bekreftet av Regjeringens eget oppnevnte utvalg som skulle evaluere bruk av eksisterende skjulte tvangsmidler; Metodekontrollutvalget (jf NOU 2009:15 Skjult informasjon – åpen kontroll). Utredningens tittel er i den sammenheng ikke uten ironisk valør, all den tid utvalget verken hadde statistikk å bygge på, eller fikk innsyn i råmaterialet, konkrete saksdokumenter, som kunne ha gitt dem de nødvendige data – heller ikke etter at utvalget gjorde Justisdepartementet oppmerksom på dette formelle hinderet for dets arbeid (se NOU'ens pkt 9.4.4).

Det må under enhver omstendighet karakteriseres som uforsvarlig å innføre et så dramatisk tiltak basert på udokumentert faktisk grunnlag – ikke minst når heller ikke EU-kommisjonen kunne vise til dokumenterte resultater den gang DLD ble hastevedtatt i kjølvannet av bombingene i henholdsvis London og Madrid - for øvrig i strid med alle anbefalinger fra Europas datatilsynsorganer og personvernmyndigheter. EU er først nå i en prosess med evaluering, basert på det som leveres av medlemsstatene av statistikk fra de første årenes erfaring. Vi er kjent med at den norske Regjeringens bidrag – naturlig nok – stort sett består av svar om at man i Norge overhodet ikke har sikre tall eller annen systematisk statistikk om hvorledes politiets bruk av trafikkdata egentlig skjer eller bidrar til kriminalitetsbekjempelsen.

Det som imidlertid er klart, er at DLD inneholder store "hull", i form av uttallige og til dels meget enkle omgåelsesmetoder, for den som ikke ønsker at trafikkdata fra sin bruk av telefoni, e-post eller andre internettbaserte tjenester skal registreres/lagres.

Dette fremgår dels av Regjeringens eget høringsnotat, jf notatets pkt 7, særlig nederst på side 56 – hvor en rekke nettverk m m unntas.

Dels oppstår det "hull" ved at borgere (og da ikke minst de profesjonelle, organiserte kriminelle som jo er målet for tiltaket), enten velger å kommunisere via tjenester som ikke omfattes av lagringsplikten, eller benytter seg av teknologi som gjør kommunikasjonen ikke-sporbar. Dette har vært påpekt fra flere teknisk kyndige hold i den offentlige debatten, og forklares også nærmere i flere høringsinstansers uttalelser. Vi viser blant annet til høringsuttalelsen fra organisasjonen Stopp Datalagringsdirektivet, hvor det i pkt 5.2 gis en god og oversiklig fremstilling av dette.

I den nødvendighetsvurderingen som foretas etter EMK, jf ovenfor, inngår som et sentralt element spørsmål om et inngrep rent faktisk er *egnet* til å realisere det anførte samfunnsmessige formål. Med de enkle omgåelsesmulighetene som er avdekket så langt, synes det ganske åpenbart at det kan stilles store spørsmål ved dette for DLDs vedkommende. Det var blant annet noen av disse omgåelsesmulighetene som gjorde at daværende president i European Confederation of Police, Heinz Kiefer, i 2005 uttalte følgende:

> *"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."[16]

Det synes derfor som om Regjeringen ønsker å innføre et massivt inngripende tiltak overfor hele den lovlydige befolkningen, som i stor grad vil kunne omgås av dem som tiltaket søker å ramme – samtidig som man nærmest henviser alle som har legitime og menneskerettighets beskyttede krav på fortrolig kommunikasjon (varslere/kilder-journalister, klienter-advokater, pasienter-leger, sosialklienter-hjelpeapparater m v), til å oppføre seg som de kriminelle, for å unngå at deres rettmessige interesser blir kompromittert – av staten eller av andre uvedkommende.

ENKELTE ANDRE FORHOLD

Kort om utlevering av lagrede trafikkdata i sivile søksmål

Som nevnt i de innledende kommentarene til Regjeringens høringsnotat, nevner Regjeringen overhodet ikke den adgang som finnes til å kreve trafikkdata utlevert som bevis i sivile søksmål, jf tvisteloven § 22-3, jf § 21-5.

Med hensynet til varsler-/kildevernet som illustrasjon, kan det nemlig ikke sees at lagrede kommunikasjonsdata som avslører pressens kilder prinsipielt vil være trygget mot utlevering i sivile søksmål. Man kan tenke seg at en arbeidsgiver (statlig eller privat) går til arbeidsrettlig oppsigelses- og/eller avskjedssak mot en ansatt som mistenkes for å ha lekket taushetsbelagt/fortrolig informasjon, til pressen og/eller andre, , eventuelt går til erstatningssak. Da kan utlevering av kommunikasjonsdata som kan bidra til å bekrefte og/eller avkrefte om vedkommende har kommunisert med en journalist eller andre i det aktuelle tidsrom, være et aktuelt bevismiddel. At også statlige/kommunale myndigheter vil/kan benytte seg av dette i sivilrettslige arbeidsrettssaker, finner man eksempel på blant annet i Oslo tingretts avgjørelse fra 2006 (TOSLO-2005-166823) mellom Oslo kommune og en ansatt.

Det kan ellers tenkes et utall variasjoner. Blant dem kan man heller ikke se bort fra tilfeller hvor sivilrettslige skritt benyttes som et rent påskudd for "fiske" etter pressens kilder eller varslere generelt, under dekke av å forfølge helt andre rettslige interesser.

I slike sammenhenger er det ikke praktisk for den det gjelder – kilden/varsleren – å protestere mot en provokasjon om utlevering og/eller et utleveringspålegg, ved å vise til kilde-/varslervernet. En slik anførsel vil i seg selv avsløre vedkommende som kilde.

Uansett om man vurderer de formelt tilgjengelige straffe- eller sivilprosessuelle rettsmidlene som faktisk kan benyttes for å få tilgang til trafikkdata som avslører pressens kilder, enten det har vært formålet eller ei – er det sentralt å peke på at det i denne sammenheng *ikke* hjelper om domstoler eller andre myndigheter på et senere stadium slår ned på tilgang som ikke burde ha funnet sted. Skaden overfor kildevernet (eller andre former for kommunikasjon som har krav på fortrolighet) oppstår allerede når kilden er avslørt, og her kan det være nok at det kan konstateres at kommunikasjon har funnet sted mellom A og B på et gitt tidspunkt.

---

[16] http://www.eurocop-police.org/pressreleases/2005/05-06-02%20PRESS%20JHA%20Council_E.pdf

Med mindre Regjeringen vurderer et uttrykkelig totalforbud mot utlevering av lagrende trafikkdata som bevis i sivile søksmål, er derfor dette nok et inngrep blant annet i varsler- og kildevernet.

Om risikoen for lekkasjer og/eller tyveri av lagrende trafikkdata

Slik lagringen er foreslått, hos den enkelte private teletilbyder og/eller ISP på vegne av staten, vil det, uavhengig av de formelle krav til lagringssikkerhet, alltid være en risiko for lekkasjer og/eller tyveri av de lagrede data. Det er ikke mangel på dokumentasjon av dette, og det gjelder både fra elektroniske baser hos private aktører og fra offentlige aktører. Risikoen blir ikke mindre av at det innenfor EU-området og innenfor ytterligere utvidede frihandlesområder som Norge er del i, vil være fritt for norske tele- og internettilbydere å velge å kjøpe lagringstjenester i andre land, hvor norske myndigheter har liten eller ingen kontroll med verken krav til lagringssikkerhet eller nasjonale regler om tilgang til lagrede data. Dette er nok et åpenbart problemområde som heller ikke synes tilstrekkelig problematisert i høringsnotatet.

OPPSUMMERING – KONKLUSJON

Etter gjennomgangen ovenfor, mener ICJ-Norge å ha vist at en gjennomføring av DLD representerer en logikk og et inngrep som vil ha dramatiske – og dels uoverskuelige – konsekvenser for flere av våre grunnleggende, demokratiske friheter og for den liberale rettstat som samfunnsform. Tiltaket vil heller ikke være egnet til å nå de mål det er begrunnet i. Implementeringen vil dessuten etter ICJ-Norges oppfatning krenke den enkelte borgers rettigheter etter EMK på flere punkter

De færreste av de sentrale problemene som er påpekt her – og som stor grad sammenfaller med hva som blir påpekt av uavhengige jurister og institusjoner som har beskyttelse av rettsstaten og menneskerettighetene som anliggende, herunder de uavhengige domstoler som har uttalt seg hittil – er berørt eller av Regjeringen i debatten eller i høringsnotatet. Det kan derfor synes som om Regjeringen ikke fullt ut har evnet å se implikasjonene av et slikt tiltak..

ICJ-Norge gjentar derfor, med økt styrke, sin oppfordring til Stortinget og Regjeringen til å tenke nok en gang gjennom følgende:

Ønsker Norge å implementere et direktiv som:

1. Innebærer krav til oppbygging av databaser over hele befolkningens – barns som voksnes – kontaktnett og kommunikasjonsmønstre?
2. Muliggjør kartlegging og overvåkning av hvor borgerne til enhver tid befinner seg – og hvilke geografiske bevegelsesmønstre de har?
3. Aksepterer en uspesifisert og generell frykt som tilstrekkelig grunnlag for inngrep i hver enkelt borgers personvern og kommunikasjonsfrihet?
4. Er rettet mot befolkningen generelt og derfor vil ha negative folepsykologiske virkninger utover tiltak som baseres på konkret mistanke. Det gjelder ikke bare frykt for misbruk, men også utvikling av ødeleggende rykter og spekulasjoner, nettopp slike negative konsekvenser for tilliten i samfunnet som i sin tid nødvendiggjorde granskingen av de hemmelige tjenestene.

ICJ-Norges klare råd til Regjeringen og Stortinget er at et slikt direktiv ikke bør implementeres i Norge.

***

Oslo, 12. april 2010

For ICJ-Norge

Ketil Lund

Jon Wessel-Aas