KROM – Norsk forening for kriminalreform
Postboks 6740 St. Olavs plass
0130 Oslo
Tel. 22 36 21 87
e-post: krom@krom.no
Forfattet av Professor Thomas Mathiesen;
henvendelser tel. 22850116; thomas.mathiesen@jus.uio.no

Oslo, 12. april 2010

Samferdselsdepartementet m. fl.
postmottak@sd.dep.no

DATALAGRINGSDIREKTIVET, DIREKTIV 2006/24/EF AV 15. MARS 2006. HØRING MED FRIST 12. APRIL 2010.

KROM ønsker å avgi følgende høringsuttalelse om ovennevnte direktiv:

Omfattende debatt

Normalt medfører direktiv og ordninger som har å gjøre med datalagring av den typen Datalagringsdirektivet gjelder, liten debatt i vårt land. Norsk gjennomføring av Schengenavtalen samt Schengen informasjonssystem, SIS, ble opprinnelig møtt med en del diskusjon i form av mediainnlegg, møter og annet.[1] Senere har imidlertid debatten om Schengen (SIS II) stort sett dødd ut, og de øvrige systemene som etter hvert ble aktuelle – *The Europol Information Systems* eller TECS, *The European Asylum System* eller EURODAC, osv. - har møtt liten interesse i offentligheten. Dette er beklagelig.

Datalagringsdirektivet har på den annen side vakt relativt stor interesse i offentligheten. Etter hvert, og særlig etter at det 3. november 2009 ble dannet en opinionsgruppe, *Stopp Datalagringsdirektivet*, mot innføring av direktivet, har det vært skrevet en rekke innlegg for og imot direktivet i store aviser. Det har meldt seg stor interesse på Internett, særlig i de såkalte sosiale medier som Facebook, og de politiske partier har delvis engasjert seg sterkt. Senest 10. april 2010 holdt Stopp Datalagringsdirektivet en en stor demonstrasjon mot

[1] For informasjon om dette, Thomas Mathiesen: *Politisamarbeid, overvåking og rettssikkerhet i Europa. Nytt oppl. med etterord om Schengensakens videre utvikling.* Oslo: Spartacus forlag 1997.

direktivet foran Stortinget, med en rekke appellanter fra de forskjellige partier. Debatten om Datalagringsdirektivet har vært omfattende.

Oppvåkningen av offentlig debatt er bra. Man kan spørre seg hva den skyldes. Vi tror en vesentlig årsak er at i motsetning til de andre informasjonssystemene, dekker Datalagringsdirektivet privatsfæren til *alle* personer i vårt land, og *alle* personer i andre land som implementerer direktivet. Det gjør direktivet aktuelt for alle og enhver, ikke bare for mer eller mindre spesielle grupper som man ofte distanserer seg fra.

Paradigmeskifte

I en viss forstand kan man si at Datalagringsdirektivet danner et paradigmeskifte i norsk overvåking. Andre systemer i utlandet gjelder også *tilnærmet alle* i en stat eller et område, som den svenske FRA-loven[2] eller det europeisk-amerikanske passasjerliste-systemet,[3] som også har vært sterkt kritisert offentlig.

Debatten om Datalagringsdirektivet er tydelig påvirkbar av mektige krefter i samfunnet. Opprinnelig, da opinionsgruppen *Stopp Datalagringsdirektivet* ble dannet, var nær sagt samtlige politiske partier på Stortinget representert på møtet, og alle partier unntatt Arbeiderpartiet hadde sterke motforestillinger. Høyre var i tvil og i vippeposisjon. Senere, etter at politiet kom på banen i Aftenposten med sine sterkt formulerte interesser (Aftenposten m.nr. 18. mars 2010; se også stort oppslått intervju med PST-lederen Janne Kristiansen i Aftenposten på dagen for høringsfristen for direktivet 12. april d.å.), ble en del meninger endret. Fremskrittspartiet begynte å vakle. Vi vil fremholde at politiets krav om sterkere virkemidler i sin kamp mot kriminalitet er umettelige. Flere ganger har politiets metodearsenal blitt utvidet nasjonalt og internasjonalt. Internasjonalt er det nylig blitt utvidet

[2] Den svenske såkalte FRA-loven gir FRA (Försvarets Radioanstalt) rett til å overvåke telefon- og internettrafikk som passerer Sveriges grenser. En betydelig del av norsk internettrafikk passerer Sverige grenser, også norsk trafikk som har norsk endepunkt.

[3] PNRA – *Passenger Name Record Agreement*, refererer til overenskomsten mellom EU og USA om elektronisk overføring av data om alle passasjerer og flypersonale til myndigheter i USA før flyet tar av. Europa-parliamentet, har vært i opposisjon på et menneskerettlig grunnlag. Se Richard M. Spooner: "Freedom, Security, and Democracy in the European Union; the intervention of the European Parliament in the negotiation of the Passenger Name Record Agreement*", King College London*, September 2007. Det er Spooners oppfatning at EU-parliamentet ikke har klart å beskytte individet fra innsamling og vidtgående spredning av personlige data, noe om har åpnet for omfattende misbruk. Grunnen til dette er, sier Spooner, den svake posisjon som EU-parliamentet har.

gjennom Norges tiltredelse til den såkalte Prüm-avtalen, som vi kommer tilbake til nedenfor. Ofte om ikke alltid er det blitt sagt at nå er det nok, politiet får nå vise at metodene duger. Ved neste korsvei, som nå, har politiet imidlertid sagt at det ikke vil *klare seg* og er avgjørende svekket uten det nye virkemidlet som er i emning.

I lys av Maktens betydning for retningen i debatten – når politiet rykker ut, får det jevnlig gehør hos politikerne – krever vi at dette blir tatt hensyn til under departementets behandling av Datalagringsdirektivet. Det er ikke makt, men argumenter som teller i denne sak.

Vi mener at kritikerne av Datalagringsdirektivet har meget sterke argumenter for sitt standpunkt.[4]

Hva saken gjelder

Dypest sett gjelder debatten om Datalagringsdirektivet grensen for privatlivets fred. Vi tror det er dette som engasjerer folk når de hører om Datalagringsdirektivet.

For det første: Selv om ikke innholdet i kommunikasjonen på fasttelefon, mobiltelefon og Internett skal kunne registreres og avlyttes, skal type kommunikasjonsmiddel (hvorvidt det dreier seg om fasttelefon, mobiltelefon, eller Internett), hvem som er eier av kommunikasjonsmidlene som brukes, tidspunkt for når kommunikasjon opprettes og når den avsluttes, lengden av kommunikasjonen, antallet kontakter som tas og mye annet registreres. Det som skal lagres er *trafikkdata, lokaliseringsdata og abonnements/brukerdata* som fremkommer ved bruk av offentlig elektronisk kommunikasjon. Dette er meget sensitiv informasjon, fordi det innebærer at man kan ”tegne” hele ”kart” over personers kommunikasjonsnett over tid.

For det andre: Selv om ikke slik overvåking av enhver persons kommunikasjonsnett skal skje *til enhver tid*, skal all slik informasjon om kommunikasjon lagres, og informasjonen skal kunne tas frem av rette vedkommende og studeres ved behov. Noen regner ikke slik lagring av informasjon for overvåking. Vi ser dette som et urimelig standpunkt som skjuler realiteten.

[4] Bestrebelser i retning av overvåking av telekommunikasjon har en meget lang historie i EU, i hvert fall til første del av 1990-tallet. Se Thomas Mathiesen: *Siste ord er ikke sagt. Schengen og globaliseringen av kontroll,* Oslo: Pax Forlag 2000, s. 88-89. Det endelige støtet i retning av Datalagringsdirektivet kom etter bombeanfallet i London i 2005. Se også Ronald Bye og Finn Sjue: *Overvåket,* Oslo: Gyldendal Norsk Forlag 2008.

Overvåking vil ikke si at alle til enhver tid nødvendigvis *skal* være under lupen, men at alle på grunnlag av foregående lagring av informasjon om dem til enhver tid *kan* være under lupen. Derfor bruker vi i det følgende begrepet "overvåking" om slik lagring av informasjon som *kan* bli brukt.

Det betyr at alle *alle i Norge blir overvåket dersom direktivet blir en realitet hos oss.*

Momenter av særlig betydning

Noen momenter er av særlig betydning i Justisdepartementets høringsnotat (bl.a. s. 7-8):

- Direktivet fastlegger som nevnt en plikt til å lagre trafikkdata, lokaliseringsdata og abonnements/brukerdata som er fremkommet ved bruk av elektronisk kommunikasjon som fasttelefoni, mobiltelefoni, internettaksess, e-post og bredbåndstelefoni.
- Lagringsplikten foreslås å gjelde for tilbydere av offentlig elektronisk kommunikasjonsnett.
- Det drøftes hvilke modeller for lagringssted som kan eller skal brukes – lagring hos tilbyder, lagring i en sentral database og mellomløsninger. Man mener personvernhensyn taler mot en sentral løsning.
- Lagringstiden er i direktivet stipulert til mellom seks måneder og to år. Spørsmålet står åpent i høringsnotatet.
- Man foreslår at utlevering av lagret informasjon bare skal skje til politiet etter avgjørelse av retten. Utlevering skal bare kunne pålegges i saker av en viss grovhet, dvs. handlinger som kan straffes med fengsel i 3 år eller mer, samt i andre saker som vurderes som "særlige saker" (uttømmende liste over slike straffebestemmelser i kap. 4.12).
- Regjeringens forslag legger opp til at det skal stilles krav til at "noen med skjellig grunn kan mistenkes" for et bestemt straffbart forhold før politiet kan få innsyn. Andre alternativer nevnes også (høringsnotatet s. 48-49; sml. Afftenposten 20. mars 2010 og Aftenposten 12. april 2010).
- Dagens tilsynsordning med delt tilsynsansvar mellom Post- og teletilsynet og Datatilsynet foreslås videreført.

Vi vil påpeke at representanter for politiet motsetter seg en ordning som har innbakt flere av ovennevnte punkter – som at

- ”skjellig grunn til mistanke” til konkrete personer skal være et grunnkrav for at politiet skal kunne få innsyn (se Aftenposten 20. mars 2010 samt PST-lederen Janne Kristiansen i Aftenposten 12. april s.å.), og at
- forslaget ikke legger opp til at politiet skal få såkalt hastekompetanse dersom etterforskningen vil lide vesentlig hvis man må vente på kjennelse fra en domstol (se Aftenposten 20. mars s.å.).

Begge deler er vesentlige rettssikkerhetsmomenter.

Av en bestemt grunn ønsker vi imidlertid ikke å gå inn i en debatt om slike detaljerte punkter i Datalagringsdirektivet:

Inviterende retorikk

Direktivets, og særlig høringsbrevets, formuleringer har nemlig det vi vil kalle en *”inviterende retorikk”*. Det vil si at formuleringene innebærer at man må velge mellom en ”streng” og en ”snill” tolkning eller ytterlighet. Eksempler:

- En ”snill” løsning vil for eksempel innbefatte kortest mulig lagringstid for informasjon. Direktivet stipulerer som nevnt 6 måneder, i realiteten en meget lang periode, som nedre grense.
- La oss si at man stilles overfor den ”snille” opsjon å fastholde et grunnkrav om ”skjellig grunn til mistanke” til konkrete personer (som sagt skisseres flere altgernativer på s. 48-49). ”Skjellig grunn til mistanke” er nok snevrere og mer begrensende enn det helt åpne ”grunn til mistanke”, men er likevel i seg selv og i praksis et meget tøyelig begrep.

På en inviterende måte presses man derved til å godta direktivet i en eller annen form, for oss den ”snille” formen. *Men den ”snille” formen er ikke ”snillere” enn at personvernet og privatlivets fred trues på en helt fundamental måte*.

Slik er høringsnotater om mange saker om overvåking så vel som andre saker formulert. Man inviteres til å begi seg inn i detaljspørsmål hvor man presenteres for alternative løsninger som i realiteten står nær hverandre. Ut fra en logikk som innebærer at "det beste må ikke bli det godes fiende" velger man den "gode" løsningen, som i realiteten innebærer at man godtar helheten.

Vi presiserer: Noen ganger, kanskje mange ganger, må man tross dette gå inn i detaljene og argumentere for den beste av dårlige (eller relativt dårlige) løsninger. Men noen ganger, som i nærværende sak, blir dette galt eller direkte farlig: Selv en løsning som representerer *alle de "snille" alternativer som er mulig* vil, som sagt, fundamentalt true personvernet og privatlivets fred.

Vi mener at tre momenter er vesentlige:

Invadering av privatlivet

For det første følger vi i all hovedsak høyesterettsdommer Ketil Lunds resonnement om personvern, som følger innenfor dette sitatet fra Aftenposten (9. januar 2010):

> *"...Også på flere andre "kritiske" områder, for eksempel lagringstid, unnlater Regjeringen å ta stilling. [Justisminister] Storberget la i går vekt på at det av personvernhensyn legges opp til strengere rutiner enn i dag for at politiet skal få tilgang til datatrafikk. Han ramset opp tre endringer i favør av personvernet.*
> - *Domstolskontroll*
> - *Krav om "skjellig grunn til mistanke" til konkrete personer*
> - *Minimum tre års strafferamme [for lovbrudd begått eller sannsynligvis begått av personer man vil hente ut lagrede data om]*
>
> *Ketil Lund er langt fra imponert. Han sier de skjerpede kravene lang på vei ikke vil gjelde for Politiets sikkerhetstjeneste (PST) som både skal forhindre og etterforske den type kriminalitet direktivet i hovedsak er myntet på. – PST er unntatt og vil kunne benytte seg av mulighetene som direktivet åpner for. Lund påpeker at PST etter de nye terrorlovene har anledning til å kunne iverksette avlytting selv om man bare har 'grunn til å tro' at noe alvorlig kan skje. PST må heller ikke vente til det har skjedd en forbrytelse. PST skal forebygge og kan dermed bruke de nye virkemidlene i forebyggende øyemed. 'Grunn til å*

tro' er vesentlig lavere beviskrav enn kravet om at det skal være 'skjellig grunn til mistanke'. Det siste vil gjelde for det ordinære politiet, ikke for PST. ... - Dette er en ekspropriering – en invadering – av privatlivet og må absolutt ikke bli gjeldende rett. Vi må si nei til en generell overvåking av hele befolkningen, sier Lund. ..."(vår utheving).

"Invadering av privatlivet" er et godt begrep, som passer på realiteten. Vi deler Ketil Lunds generelle syn, og vi mener det gjelder selv om PST skulle bli fratatt noen av sine myndigheter (hvilket naturligvis ikke vil skje). Vi *avviser vedtakelsen av Datalagringsdirektivet i Norge som en invadering av privatlivet*. Selv "snille" løsninger som domstolskontroll, krav om skjellig grunn til mistanke og tre års strafferamme gjør direktivet til en invadering av privatlivet, fordi:

- Historisk erfaring har vist at domstolskontroll lett kan bli *en overflatisk "sandpåstrøing"*.
- "Skjellig grunn til mistanke" er som nevnt i realiteten *et meget tøyelig begrep*.
- Minimum tre års strafferamme er i praksis et spørsmål som man lett kan komme rundt ved *det vi vil kalle "oversubsumsjon"* – man legge til grunn en påstand som i utgangspunktet ligger over nivået på tre års strafferamme.

Ekspansjonsfaren

For det andre er det vi vil kalle "ekspansjonsfaren" knyttet til Datalagringsdirektivet nok en generell grunn til å gå imot innføring av det.

Vårt samfunn er et samfunn i endring, som hyppig er utsatt for risiki og hendelser som er definert som større eller mindre katastrofer. Katastrofene kan ta form av kriminalitet som vi ikke ville si er så alvorlig men som er store nok for enkeltmennesket. Katastrofene kan også ta form av større og mer eller mindre alvorlig kriminalitet som ses som trusler også på samfunnsplan, og de kan ta form de rene terrorangrep som innebærer store angrep på sivilbefolkningen og død for mange mennesker. Vi ser det trusselsbildet som dermed melder seg dels som "objektivt" – bomber eksploderer og uskyldige mennesker dør. Men i vårt samfunn er heldigvis slike hendelser meget sjeldne, og trusselsbildet er også "konstruksjoner" – menneskeskapt av medier og myndigheter. Frykten og angsten som følger er tilsvarende laget av mennesker.

Trusselsbildene som melder seg er egnet til å skape situasjoner der virkemidler mot truslene, virkemidler som opprinnelig er relativt forsiktige og snille, raskt transformeres til mye mer inngripende og farlige redskaper. *Dette er "ekspansjonsfaren*".

Et virkemiddel som Datalagringsdirektivet har stor ekspansjonsfare knyttet til seg.

Det tar tid å utvikle et slikt direktiv. Det må vedtas i forskjellige organer og spres til ulike stater. Ulike formuleringer må finslipes. Dette er viktig tid, som kan komme godt med i mer eller mindre paniske situasjoner. Tiden roer gemyttene. *Annerledes er det når virkemidlet, som Datalagringsdirektivet, er fikst ferdig og vedtatt*. Kommer man da opp i en panisk situasjon, kan virkemidlet – igjen som Datalagringsdirektivet – raskt tas frem og børstes støv av. Er panikken stor nok kan et allerede foreliggende virkemiddel som Datalagringsdirektivet meget raskt endres på helt vesentlige punkter som gjør det langt farligere enn opprinnelig tenkt. For et Storting er det for eksempel raskt gjort og endre tidsrammen for lagring på 6 måneder til 1 år, endre "skjellig grunn til mistanke" til "grunn til å tro" og endre 3 års-rammen for lovbrudd til noe atskillig mindre.

"Ekspansjonsfaren" knyttet til Datalagringsdirektivet *kan* føre vårt rimelig demokratiske samfunn over kanten til et mer eller mindre totalitært samfunn. Dette er ikke å male fanden på veggen. Det er å ta i bruk historien. Etter 11. september 2001 var det nettopp slik den betydelige overvåkingskapasiteten som allerede var til stede i USA og EU raskt kunne benyttes til å skru skruen kraftig om og gi samfunnene flere klart totalitære striper. Det relative fravær av modeller som fantes i Norge gjorde at man måtte bruke noe mer tid, som roet gemyttene og førte noe mer begrensede virkemidler.

Vi avviser også på dette grunnlag at Datalagringsdirektivet innføres i Norge.

Integrering av overvåkingsystemer

Det tredje grunnlaget som gjør at vi avviser Datalagringsdirektivet, er den plass det vil kunne få i et integrert nettverk av overvåkingssystemer i Europa.

Vi gir to eksempler på integrasjon generelt og av overvåkingssystemer spesielt fra EUs nylige historie. Begge eksempler gir godt grunnlag for å vente at liknende integrasjon vil finne sted på datalagringsområdet.[5]

Haag-programmet

Av avgjørende betydning er det såkalte Haag-programmet, antatt 5. november 2004, der det såkalte "tilgjengelighetsprinsippet" (the principle of availability) ble introdusert. Tilgjengelighetsprinsippet vil si at *alle data/opplysninger som rettshåndhevende myndigheter i en stat er i besittelse av, skal være tilgjengelige for rettshåndhevende myndigheter i enhver annen stat.* Tilgjengelighetsprinsippet er definert på følgende måte i Haag-programmet:

> *Med virkning fra 1. januar 2008 skal utveksling av ... informasjon bli styrt av betingelsene som er spesifisert nedenfor når det gjelder prinsippet om tilgjengelighet, som betyr at gjennom hele Unionen skal en håndhevende tjenestemann i en medlemsstat som trenger informasjon for å utføre sine plikter, kunne oppnå denne fra en annen medlemsstat, og at et rettshåndhevende organ i den andre medlemsstaten som har denne informasjonen vil gjøre den tilgjengelig for det påpekte formålet, idet en tar i betraktning kravet til pågående undersøkelser i den staten.*
>
> *Utvekslingsmetodene skal ["should", som i sammenhengen betyr "skal" og neppe "bør", vår anmerkning] gjøre full bruk av ny teknologi og må bli tilpasset hver type informasjon, der hvor det passer, gjennom gjensidig tilgang til eller interoperabilitet av nasjonale databaser, eller direkte (on-line) tilgang, innbefattet for Europol, til eksisterende sentrale databaser, som SIS.*[6]

Dette er meget sterke ord. Tony Bunyan i borgerrettighetsorganisasjonen *Statewatch* har kommentert det slik:

> *Bilaterale og multilaterale overenskomster har lenge vært på plass for at rettshåndhevende myndigheter i en EU-medlemsstat skal kunne melde anmodninger til*

[5] Integrasjonsbestrebelsene når det gjelder overvåkingssystemer i EU går mye lenger tilbake i EUs historie, i hvert fall til siste del av 1990-tallet. Se Thomas Mathiesen: *Siste ord er ikke sagt, op.cit.*, s. 82 flg.
[6] På engelsk i Tony Bunyan: "The 'Principle of Availability'", *Statewatch Analysis* 2006. Alle sitater på engelsk i dette høringsbrevet er oversatt til norsk av oss.

de i en annen medlemsstat om spesifiserte saker. …"Problemet" for de rettshåndhevende myndigheter er at denne fremgangsmåten tar tid, innebærer formelle anmodninger og noen ganger rettslig kjennelse."[7]

Haag-programmet forenkler og letter dette på en avgjørende måte.

EU-kommisjonen fulgte opp 25. november 2005 med en såkalt "Kommunikasjon fra Kommisjonen til Rådet og Europaparlamentet om forbedret effektivitet, forsterket interoperabilitet og synergi mellom europeiske databaser på området rettshåndhevelse og innenrikssaker".[8] Kommisjonen la vekt på såkalt "interoperabilitet", "nettverk" (connectivity), "synergi" og "prinsippet om tilgjengelighet" for IT-systemer, og fokuserte særlig på 2. generasjon av Schengen informasjonssystem (SIS II), dessuten på Visa Information System (VIS) som er planlagt med en "felles teknisk plattform" med SIS II (og dessuten med informasjon som dels sammenfaller med informasjonen i EURODAC). Bare noen få måneder før dette (17. mars 2005), uttalte Presidentskapet i et notat til Arbeidsgruppen vedrørende politisamarbeid (med tittelen "Fremgangsmåte for å forsterke effektiv og formålstjenlig informasjonsutveksling mellom EUs rettshåndhevende myndigheter")[9] at i prinsippet

bør JHAs[Justice and Home Affairs Councils] IT-systemer være vidt tilgjengelige [widely accessible] for rettshåndhevende myndigheter for å bekjempe terrorisme og organisert kriminalitet; …[R]ettshåndhevende myndigheter bør ha tilgang til nasjonale håndhevelsesdata i alle medlemsstater, særlig når det gjelder identifikasjon, DNA og fingeravtrykkdata, på treff/ikke treff grunnlag. …[R]ettshåndhevende myndigheter [bør] ha direkte tilgang til nasjonale administrative systemer i alle medlemsstater (for eksempel personregistre, innbefattet juridiske personer, kjøretøy, identitetsdokumenter og førerkort, så vel som fly- og sjøfartsregistre).

I første omgang har det vært vanskelig å gjennomføre Haag-programmet, som også er et bredt kiminalpolitisk program med en omfattende aksjonsplan. Det fremgår av EU-kommisjonens Kommunikasjon til Rådet og EU-Parlamentet, datert 2. juli 2008 - "Rapport om implementing

[7] Samme sted.
[8] COM (2005) 597 final. Vi takker Ben Hayes i *Statewatch* for å ha gjort oss oppmerksom på denne Kommunikasjonen.
[9] 7416/05 ENFOPOL 29.

av Haag-programmet for 2007"[10]. Et såkalt **utilfredsstillende oppnåelsesnivå** fant man for visapolitikken, deling av informasjon mellom rettshåndhevende og rettslige myndigheter, kamp mot organisert kriminalitet, håndtering av kriser innen EU, politi- og toll-samarbeid og rettslig samarbeid i kriminalsaker. Et **tilfredsstillende oppnåelsesnivå** fant man for migrasjon og grensepolitikk, terrorisme, oppbygging av gjensidig tillit og rettslig samarbeid i sivile saker. Dette betyr at i 2007 fungerte tilgjengelighetsprinsippet oftere utilfredsstillende enn tilfredsstillende for de formål man har satt seg. Men ofte fungerte det tilfredsstillende.

Og det fungerer bedre i dag: Med direkte referanse til Haag-programmet ble "Utkast til rådskonklusjoner om en strategi for informasjonshåndtering for EUs indre sikkerhet" sendt fra Sekretariatet til Coreper 25. november 2009.[11] Dokumentet stadfester et utkast til hvordan man "skal sikre at avgjørelser om behovene for å håndtere og utveksle data ["managing and exchanging data"], og avgjørelser om måter å gjøre dette på, blir tatt på en sammenhengende, profesjonell, effektiv og kost-effektiv måte, ansvarlig og forståelig for borgerne og de profesjonelle brukere (s. 1)." På s. 5 heter det at

> *Effektiv og sikker utveksling av informasjon er en forutsetning for å oppnå målene om indre sikkerhet i Den europeiske union.*

Hva betyr så informasjon i dette dokumentet? Det heter i fotnote 10, ved ordet "informasjon" i sitatet over:

> *I denne sammenheng betyr informasjon informasjon og kriminalistisk etterretning som kreves av de kompetente nasjonale myndigheter og er tilgjengelig for dem under det relevante regulerende rammeverk for formålet å forbedre den indre sikkerheten i EU for EUs borgere.*

Datalagringedirektivet er ikke direkte nevnt. Men informasjon som lagres om borgerne med hjemmel i Datalagringsdirektivet er *nettopp av den type informasjon som er definert i nevnte fotnote og behandlet i dokumentet.*

Vi nærmer oss grensekryssende informasjonsutveksling med Datalagringsdirektivet som utgangspunkt.

Prüm-avtalen

[10] COM (2008) 373 final.
[11] *Draft Council Conclusions on an Information Management Strategy for EU internal security,* 16637/09 DG H 3 A (Limite).

I EU arbeides det for tiden særlig med sammenkopling av nasjonale DNA-baser, og et europeisk fingeravtrykkregister som skal kombinere alle data om fingeravtrykk som i dag bare finnes i nasjonale baser. Sammenkoplingen av nasjonale DNA-databaser og nasjonale databaser for fingeravtrykk og for opplysninger om kjøretøy er særskilt interessant.

Den såkalte Prüm-avtalen kommer i denne forbindelse inn. Avtalen har fått sitt navn etter den lille byen Prüm, som ikke ligger langt fra Schengen. Den 27. mai 2005 ble en konvensjon undertegnet i Prüm av syv stater. Fem av de syv statene - Benelux-statene samt Tyskland og Frankrike - var i sin tid delaktige i Schengen-avtalen i 1985 og parter i Schengen-konvensjonen i 1990 (i tillegg kom Spania og Østerrike). På mange måter minner Prüm-avtalens tilblivelse om Schengens opprinnelse. Senere har en rekke andre EU-stater sluttet seg til, blant annet Sverige og Finland. Norge undertegnet Prüm-avtalen 26. november 2009.[12] Medlemslandene kan søke fritt etter DNA-treff i hverandres registre, mens de etter konvensjonen må kontakte politiet for å få vedkommendes identitet, hvilket er et svakt krav.

Det har kommet frem betydelig kritikk fra indre EU-organer som *The European Data Protection Supervisor* (EDPS), som kommenterer initiativet på følgende måte i en pressemelding:

> *15 medlemsstater foreslår å utvide anvendelsen av Prüm-avtalen, en avtale som er inngått mellom syv av dem, til hele EU ut noen endringer. [Derfor, fortsetter EDPS,] tar EDPS' forslag i hovedsak sikte på å forbedre teksten uten å modifisere systemet for informasjonsutveksling i seg selv.* [13]

EDPS ser tydeligvis initiativet som et *fait accompli* som det ikke kan gjøres særlig mye med. Den første tilblivelsen av Schengen-samarbeidet så vel som Prüm-samarbeidet viser mangelen på demokratisk prosess i viktige EU-initiativ.[14]

[12] Pressemelding fra Justisdepartementet 26. november 2009.
[13] EDPS/07/3 11. april 2007.
[14] Det er også andre tegn på en viss oppgitthet overfor begivenhetenes gang (eller ironi over utviklingen?) hos EDSP. I EDSPs "opinion" av 10. juli 2009 om en "Meddelelse fra Kommisjonen til Europaparlamentet og Området vedrørende Frihet, Sikkerhet og Rettferdighet", http://www.statewatch.org/news/2009/jul/stockholm-edps-opin.pdf, har EDSP mange kritiske kommentarer til utviklingen av informasjons- og kommunikasjonsteknologiene, og bruker ord som "overvåkingssamfunn" (s. 3), men anvender underlig nok også

Overhuset i Storbritannia ved dets *European Union Committee* er kritisk i en kommunikasjon 9. mai 2007, [15] der komiteen sier i et forord at

> *Prüm-avtalen handler hovedsakelig om utveksling av data. Uunngåelig reiser dette spørsmål om databeskyttelse. Som så ofte ellers, har disse en tendens til å bli oversett.*

Det er foruroligende om systemet vil tillate uregulert søk på et "treff/ikke treff"-grunnlag, fulgt av automatisk overføring av filen hvis det er et "treff". Tony Bunyan i Statewatch har kommentert dette slik: "'Treff/ikke treff' tilgang vil tillate 'fisketurer' uten noen kontroller i det hele tatt." Det kan bekreftes at "fisketurer" godt kan finne sted: I Prüm-konvensjonen av 27. mai 2005 artikkel 3 (1), under "Automatiserte søk etter DNA-profiler", heter det at de kontraherende parter "skal tillate andre kontraherende parters nasjonale kontaktpunkter … tilgang til referansedata [som bare skal innbefatte DNA-profiler og ikke andre data som direkte kan identifisere personen, se artikkel 2, vårt innskudd] i deres DNA-analysefiler, med anledning til å foreta automatiserte søk ved å sammenlikne DNA-profiler". Slike søk kan bare bli utført i individuelle saker, men til gjengjeld heter det i artikkel 4 (1), under "Automatiserte sammenlikninger av DNA-profiler", at "de kontraherende parter skal, ved gjensidig enighet, via deres nasjonale kontaktpunkter sammenlikne DNA-profiler av de som ikke kan spores med alle DNA-profiler fra andre nasjonale DNA-analysefilers referansedata". Dessuten, i artikkel 4 (2), heter det at ved en match, skal de kontraherende part "uten opphold forsyne den andre kontraherende partens nasjonale kontaktpunkt med de referansedata som en match er blitt funnet ved." Ved en match kan partene etter artikkel 5 for øvrig forsynes med "enhver tilgjengelig videre personlig opplysning og annen informasjon" etter nasjonal lov. Liknende bestemmelser finnes om søk som vedrører fingeravtrykk og kjøretøy.

I EU-dokumentene vi har sett har det stått lite om vanskelighetene med uten videre å bruke DNA-opplysninger i kriminaletterforskning – tolkningen av DNA-spor, muligheten for å plante bevis, muligheten for at DNA-spor tilfeldig legges eller er å finne på et åsted, osv. Kontroll med disse vanskelighetene blir meget store og alvorlige når man tenker seg tilgang på DNA-databaser i alle mulige andre stater, der man ikke vet hvordan kontrollen utføres.

---

begrepet "fri bevegelse av (personlige) data" (s. 4) som sidestilt med "fri bevegelse av personer", en av EUs kjente fire friheter. Undring over formuleringen er også notert av Statewatch.

[15] House of Lords, European Union Committee: *Prüm: An Effective Weapon against Terrorism and Crime?* London: The Stationery Office Limited 2007.

Prüm-avtalen er et praktfullt eksempel på tendensen mot integrasjon av kontrollsystemene i EU. Betydningen av Haag-programmet og Prüm-avtalen kan knapt overvurderes som tegn i tiden. Bestrebelsene på å integrere andre informasjons- og overvåkingssystemer er også av stor betydning. Schengen og Europol er etablert for forskjellige formål. Det er for eksempel også Eurodac og Schengen. Systemenes formål er ofte vage og diffuse. Dertil kommer at et system med ett formål nå tenderer mot å bli integrert med annet et system som har et annet formål. Informasjon samlet med sikte på ett mål vil nå tendere mot bli åpent for innsyn og bruk for andre formål.[16]

Følgende kan sies: Det foreligger så vidt vi vet ingen konkrete planer på det nåværende tidspunkt for å gi stater automatisk tilgang på informasjon fra andre staters lagrede teledata. Men i lys av hva som fremkommer i ovennevnte dokument knyttet til Haag-programmet (16637/09 DG H 3 A, se sitater ovenfor) så vel som hva vi vet fra EUs historie (illustrert ved Prüm-avtalen) kan dette meget vel komme når Datalagringsdirektivet vel er på plass og har vært redskap for politiet en stund. En større terrorhandling, eller et alvorlig kriminalitetsscenario, kan gjerne utløse krav fra organer innen politiet eller fra politiske forsamlinger om at slik tilgang på informasjon blir gjort gjeldende. Med faktisk innføring av Datalagringsdirektivet i Norge er ekspansjonsfaren til stede (se ovenfor). Med institusjonelle arrangementer som Haag-programmet, Prüm-avtalen og tendenser til integrasjon mellom andre informasjons- og overvåkingssystemer er det legitime grunnlag for integrasjon også på teledataområdet til stede. Med den avanserte teknologien som nå finnes på området er integrasjon fullt mulig.

Vi ser denne mulighet som et selvstendig grunnlag for å avvise Datalagringsdirektivet for Norge.

Kanskje vil de ansvarlige myndigheter, og politiet, ikke ønske å avvise direktivet på det de vel vil kalle et hypotetisk grunnlag. I lys av EUs historie ser vi for vår del slik integrasjon som nevnt som langt mindre hypotetisk, og langt mer en høyst reell mulighet, i en fremtid som er rimelig nær. Vi har levende i minne hvordan justismyndigheter og justisminister i sin tid

[16] Synspunktet er hentet fra Simen Wiig: *Flyt og tilgjengelighet. En studie av det europeiske informasjonssamarbeidet innen politi, sikkerhets- og grensekontroll og dets konsekvenser for individers rettssikkerhet og rettigheter.* Masteravhandling i rettssosiologi, Universitet i Oslo 2007.

forsikret om at Schengen-systemet var, og ville forbli, separat fra EU. Kort tid etter kom EU-toppmøtet i Amsterdam (1997), der full integrasjon av Schengensystemet i EU ble en realitet.[17]

Invadering av privatlivet, ekspansjonsfaren og integreringen av Datalagringsdirektivet i det øvrige overvåkingssystemet som nå er under rask utviklingen, setter personvernsproblemene og trusselen mot rettsstaten på sin spiss, og i et enda klarere lys enn om man ser Datalagringsdirektivet isolert.

Hva med effektiviteten?

Politiet kommer nok til å fremheve at vi gjennom de punktene vi har tatt opp, og måten vi har tatt dem opp på, undergraver politiets muligheter for å forfølge og slå ned på alvorlig kriminalitet. Presumptivt er vi interessert i å "stikke kjepper i hjulene" på politiet, for eksempel ved å forsinke rask utvikling av enda sterkere virkemidler (ekspansjonsfaren). Vi ser det definitivt ikke slik. De aller fleste ønsker å forebygge terrorhendelser, som har vært fraværende hos oss i en lang rekke år. De aller fleste ønsker å oppklare og forebygge annen alvorlig kriminalitet. Men politiet har allerede omfattende virkemidler for dette, og kan dessuten allerede i dag med rettens tillatelse bruke trafikkdata i etterforskning. Datalagringsdirektivet vil ikke i vesentlig grad høyne effektiviteten. I balanseringen mellom liten høyning av effektivitet og stor faktisk og potensiell trussel mot personvernet, er det klart at trusselen mot personvernet veier tyngst.

Uansett effektivitet: Det er på helt *prinsipielt grunnlag* vi går imot innføring av Datalagringsdirektivett. Gjennom de siste årene har norsk personvern blitt svekket ved innføringen av en rekke overvåkingssystemer, og ved at personer i Norge i dag etterlater seg en meget lang rekke elektroniske spor som kan få følger for personvernet. **Innføring av**

[17] Se Thomas Mathiesen: *Schengen – Politisamarbeid, overvåking og rettssikkerhet i Europa, op. cit.,* samt Gyrd Brændeland i *Klasssekampen* 21. juni 1997. Den 9. november 1995 uttalte for eksempel daværende justisminister Grete Faremo under debatten som den gang fant sted om Schengen: "I debatten har enkelte antydet at det er mulig at hele Schengen-samarbeidet vil inngå som en regulær del av EU-samarbeidet. Teoretisk er det selvfølgelig mulig, men det er mildt sagt usannsynlig at dette vil skje i overskuelig framtid." Så sent som 28. februar 1996 uttalte samme justisminister i Stortingets spørretime at "Jeg har tidligere redegjort for de mange hypoteser og til dels urealistiske hypoteser som må slå til for at et Schengen-samarbeid skal inngå som en del av det ordinære EU-samarbeidet om justis- og politispørsmål". Den 18. juni 1997 måtte daværende stortingsrepresentant Halvard Bakke (A) i lys av Amsterdam-toppmøtet si til *Aftenposten* at "Vi har forutsatt at dette ville skje". Se Mathiesen *op.cit*. s. 124-25.

Datalagringsdirektivet representerer som sagt et paradigmeskifte i Norge ved at *alle* kan overvåkes. Nå er nok nok. Et slikt paradigmeskifte må avvises.

Avslutning

Av ovennevnte grunner, nemlig

- ***invaderingen av privatlivet* som følger med direktivet,**
- ***ekspansjonsfaren* eller svekkelsen av "snille" bestemmelser knyttet til direktivet når det først er vedtatt, og**
- **faren for at den pågående *integrasjonen av overvåkingssystemene i Europa* også vil omslutte direktivet,**

avviser vi direktivet for Norge.

Oslo, den 12. april 2010

For styret i KROM

Knut-Olav Haraldseid **Astrid Renland**