

MER OVERVÅKNING = MINDRE TRYGGHET



EUs DATALAGRINGS-DIREKTIV[1] er nå på vei inn i norsk lov, og innebærer lagring av data om alle landets innbyggeres kommunikasjon og nettsøk. Hva om en betjent sto oppstilt ved hver eneste postinnlevering og ba om å få notere seg hvem man var og hvem man sendte brev til? Eller om man hver gang man skulle ringe til noen først ble møtt av en person som skulle notere hvem man var, hvem man skulle ringe til, dato, tidspunkt og hvor lenge samtalen varte? Dette er nå i ferd med å bli virkeligheten for all elektronisk kommunikasjon.

Trafikkdata lagring er et tiltak som i praksis kriminaliserer hele befolkningen. Det er rettet mot befolkningen som helhet, og kan derfor ikke sies å være et spesifikt kriminalitetsforebyggende tiltak. Det er et kontrolltiltak overfor alle innbyggere.

Vi vet at med økede kontrollmuligheter vil også trangen til mer kontroll av flere handlinger, og bruk av de lagrede dataene i flere sammenhenger, bli uimotståelig. Var det ikke slik, ville det ikke være noen hensikt med kontroll av mennesker som ikke er under (formell) etterforskning. Hvis funksjonen var å spesifikt ramme kriminelle, ville man konsentrert seg om punktovervåkning av de som var under etterforskning.

Stipendiat og tidligere førstestatsadvokat Inger Marie Sunde etterlyser en bedre løsning for oppklaring av kriminalitet enn å overvåke alle landets innbyggeres kommunikasjon og nettsøk[2]. Svaret er tradisjonelt politiarbeid med infiltrasjon i og overvåkning av kriminelle miljøer og personer, kombinert med bedre utdanning av politi og dommere i teknisk bevisførsel. Politiet

må gis nok midler til dette. Viktig er det også å styrke oppfølgingen, særlig av barn og unge med problemer.

EN FARLIG FEILFORESTILLING

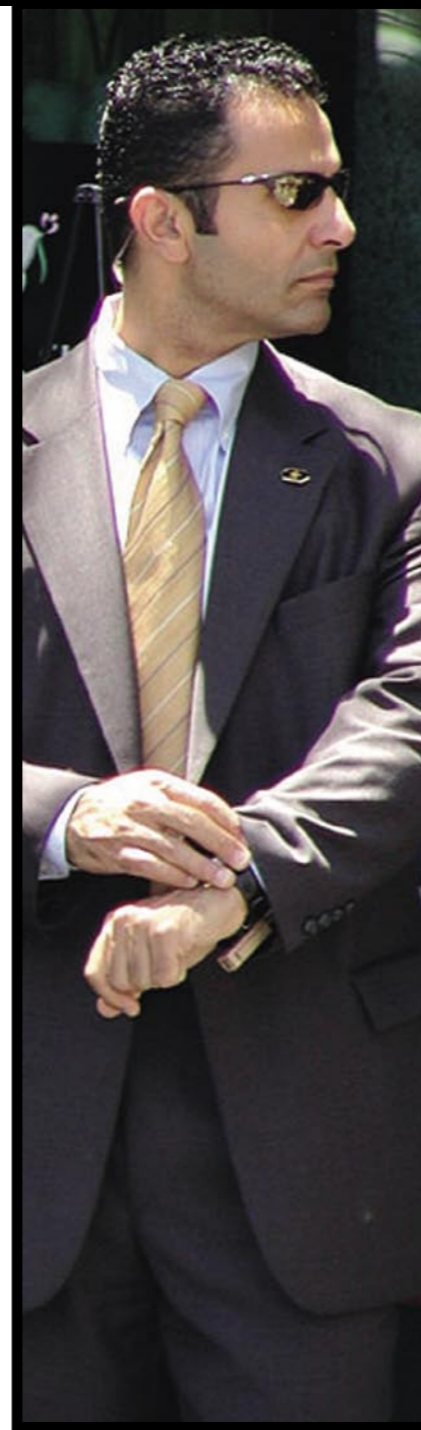
Inger Marie Sundes argumentasjon i ulike media[3] bygger på en feilforestilling om at detaljkontroll over individenes bevegelser og handlinger ikke er farlig så lenge kontrollen skjer i en rettsstat og et demokrati. Men en rettsstat og et demokrati utsetter ikke alle borgere for overvåkningstiltak, og å gjøre

alle borgere sporbare er et etterforskningspreget overvåkningstiltak. Da nytter det ikke å komme og si at "vi skal sørge for at opplysningene bare utleveres i spesielle tilfeller". Slike opplysninger vil bli brukt hvis de først er samlet og lagret.

At en slik mengde av data også vil representere en uimotståelig fristelse for mange andre enn politiet, og at data alltid vil komme på avveie, er uunngåelig. Men det må understrekes at dette absolutt ikke er noe hovedargument. Det er mer enn alvorlig nok, selv om ingen andre enn politiet noensinne skulle klare å få ut en eneste bit med trafikk- og lokasjonsdata. Og da er vi over på diskusjonen om rettsstaten. Er det akseptabelt i en rettsstat at politiet skal ha mulighet til å komme til kunnskap om lagrede informasjon om borgers bevegelser uten at de på forhånd er under etterforskning for noe kriminelt?

Hvis man registrerer telefonnumrene som har vært i kontakt med hverandre, har man et ganske så treffsikkert bilde av hvem som snakker med hvem og når de gjør det. Dette gjelder i særlig grad når det er snakk om mobiltelefoner. For epost er koblingen person-epostadresse enda tettere enn ved telefonnummer.

En kartlegging av hvilke websteder eller nettsider man besøker gir et meget nøyaktig bilde av en persons interesser og aktiviteter, politiske holdninger, livssyn, seksualitet, eventuelle sykdommer m.m. Å lagre disse opplysningene om alle borgere innebærer å introdusere et etterforskningspreget tiltak mot dem. Dette er fundamentalt nytt, tidligere har lagring



av informasjon om individers bevegelser bare skjedd når noen har vært under etterforskning, som Guro Slettemark har påpekt.

Riktignok sier det norske lovforslaget at nettadressene (URL'ene) man er inne på ikke skal lagres – i denne omgang, til forskjell fra f.eks. i Storbritannia. Direktivet påbyr ikke lagring av URL'ene, men åpner for det, og flere land går derfor inn for slik lagring fra starten av. Så det ligger ikke noen trygghet i at Norge i denne omgang ikke skal lagre URL'er. Neste år kommer det sikkert et forslag om at URL'er likevel må lagres, fordi det viser seg at "vi (politiet) trenger dem likevel".

Selv om det "bare" logges hvilke IP-adresser man besøker, er likevel avstanden ikke så stor til å logge hvilke nettsteder man besøker – f.eks. dersom det er en bestemt organisasjon som eier IP-adressen, har man logget en kobling mellom personen og denne.

Det finnes en del tilfeller der forskjellen mellom å lagre trafikkdata og innhold blir visket ut. Her er et eksempel:

Sitat

12:00:00 <min-ip> <http://www.google.com> 12:00:10 <min-ip> <http://www.google.com/?q=eksplosiver> 12:01:03 <min-ip> <http://www.google.com/?q=eksplosiver&start=20&num=20> 12:02:40 <min-ip> <http://da.wikipedia.org/wiki/Kategori:Eksplosiver>

Samtalens "innhold" altså html-koden som blei overført fra Google til meg er rett nok ikkje inkludert i loggen. Men eg vil like fullt hevde at trafikk-loggen gir eit temmelig komplett bilete av interaksjonen som foregikk mellom meg og Google.

Eg gikk til heimeside til Google. Eg søkte på "eksplosiver", eg fant ingenting av interesse på første side, så eg trykte på "Next". På neste side fant eg ein link til danske wikipedia som eg trykka på. Alt dette er trivielt lesbart fra loggen.

(sitat slutt)[4]

RETTSSTATENS GRUNNLAG

I en rettsstat er politiets kontrollmakt begrenset til de som er under konkret mistanke for noe kriminelt. Å gi politiet mulighet til å kartlegge alles kommunikasjon og nettsøk er et brudd på rettsstatens prinsipper. Da må det, uten å bli beskyldt for å være paranoid, være lov å påpeke at rettsstatens levedyktighet er avhengig av at dens prinsipper opprettholdes.

Det kan se ut til at den største faren i dette bildet ikke er politiets eller andres ønske om kontroll, men derimot den naive og uhistoriske troen på at rettsstat og demokrati er en slags trylleformular gitt en gang for alle, en evigvarende

vaksine mot forvitring av verdiene vi forbinder med dem. Det er de ikke; rettsstaten må kontinuerlig bevisst opprettholdes.

I en rettsstat er det slik at ingen etterforskning iverksettes mot noen med mindre man er mistenkt for noe påvist kriminelt. Datalagringsdirektivet representerer et paradigmeskifte – det skal samles og lagres opplysninger om alle borgers elektroniske bevegelser i en tid da elektronisk kommunikasjon blir mer sentral enn noensinne i vårt dagligliv.

Dersom vi ønsker å opprettholde de verdiene som vi har lært å forbinde med rettsstaten og demokratiet, er vi nødt til å holde fast på prinsippet om at den makten som myndigheter og politi har over innbyggerne må begrenses. Bare i kriminelle tilfeller bør inngrep som registrering og kartlegging av bevegelser kunne aksepteres.

KILDER/REFERANSER

[1] se f.eks.: <http://efn.no/datalagringsrapport-o8092006.pdf>

[2] <http://www.aftenposten.no/meninger/debatt/article1564737.ece>

[3] se f.eks.: <http://www.aftenposten.no/meninger/kronikker/article1549610.ece>

[4] Sitert fra innlegg på efn-listen av Eivind Krystad, 1. desember 2006 (<http://efn.no/efn-listen.html>)

– Per Inge Østmoen er styremedlem i EFN og leder for EFNs personvernvalg.
– Thomas Gramstad er leder for EFN.
– EFN er en elektronisk borgerrettsorganisasjon – en rettighetsorganisasjon for ALLES rettigheter – som jobber med medborgerskap og juridiske rettigheter i IT-samfunnet. www.efn.no

