

15 APR 2010

Sekretariat: Berit Holm
Møllergaten 4, 0179 Oslo
Tlf: 24 14 53 53/ 952 30 632
Telefaks: 24 14 53 51
Bank: 9041 22 50655

Org.nr.: 988 934 488

Det kongelige samferdselsdepartement
Postboks 8010 Dep
0030 Oslo

Oslo, den 14. april 2010

**DATALAGRINGSDIREKTIVET – HØRINGSSVAR FRA
FORSVARERGRUPPEN AV 1977**

Det vises til høringsbrev av 8. januar 2010. Det beklages at fristen for vår høringsuttalelse er blitt noe oversittet.

Innledningsvis skal det fremheves at Forsvarergruppen av 1977 anser forslaget om implementering av Datalagringsdirektivet som et svært alvorlig anslag mot norske borgeres personvern og rettsikkerhet. I høringsnotatet er de negative konsekvensene for lite påaktet, samtidig som det ikke i tilstrekkelig grad er fokusert på om Direktivet reelt sett vil kunne ivareta de formål som angis.

Det er i denne forbindelse helt sentralt for det første å vise til at det fortsatt er svært usikkert hvilken utstrekning Direktivet vil få gjennomslag i andre land. EMD har således ikke behandlet forholdet til EMK art 8, og det hersker usikkerhet i flere enkeltstater, som f. eks. Tyskland, Romania og Sverige. Det blir dermed overraskende useriøst når PST og KRIPOS uttaler seg om at Norge vil bli en "fristat for terrorister og kriminelle" dersom Direktivet ikke blir gjeldende også i Norge.

For det andre er det sentralt for den videre debatten at Direktivets pålegg om lagring av data i stor skala, uavhengig av mistanke om alvorlig kriminalitet, må gi myndighetene en betydelig bevisbyrde for at dette også vil få stor effekt for kriminalitetsbekjempelsen. Det er Forsvarergruppens syn at den organiserte kriminalitet må bekjempes med andre midler enn dem som rammer hele befolkningen, og at erfaring tilsier at denne virksomhet vil kunne tilpasse sin organisering også til slike reguleringer.

Forsvarergruppen av 1977 vil på denne bakgrunn vise til og tiltre de høringsuttalelser som foreligger fra Den Norske Advokatforening og Den internasjonale juristkommisjon, norsk avdeling ICJ). I begge disse uttalelsene fokuseres helt sentrale innvendinger mot forslaget i høringsnotatet, og disse må tillegges avgjørende vekt i den videre debatt.

1. Overordnede betraktninger

Som følge av den svært raske teknologiske utvikling de senere år, har det oppstått muligheter for detaljert kartlegging av enkeltpersoners gjøren og laden med basis i data som lagres – knyttet til betalingstransaksjoner, telefonbruk, bompaseringer,

t-banereiser og mange andre livsområder. Det er mao ikke tale om data som registreres i overvåkningshensikt, men for andre formål.

2)

Slike opplysninger har politiet etter hvert begynt å innhente i omfattende grad for bruk i etterforskning og som bevis. Dette har skjedd med grunnlag i straffeprosesslovens alminnelige regler om beslag og utleveringspålegg, og uten at reglene er utformet under hensyn til overvåkingsaspektet og de særlige personvern hensyn som gjør seg gjeldende ved denne type bevisinnhenting. Uavhengig av spørsmålet om pålagt datalagring, er det etter Forsvarergruppens oppfatning riktig og viktig at innhenting av personvernsensitive data underlegges særlig regulering i straffeprosessloven, med klart definerte skranker.

Strafferettspleiens grunnleggende formål er å beskytte vår samfunnsorden og dennes grunnverdier, kollektive verdier så vel som individuelle.

Av de grunnleggende rettsstatsidealer vår samfunnsorden bygger på, og som rettsordenen skal beskytte, er individets frihet, samt balansering av makt slik at maktmisbruk hindres.

På et makronivå er derfor hensynet til å begrense det totale overvåkningsnivå, samt mulighetene for kartlegging av individene, essensielt for å sikre grunnverdiene i vår samfunnsorden. Herunder er muligheten til fri kommunikasjon og meningsdannelse uten frykt for innsyn en grunnforutsetning for et fungerende demokrati.

Samtidig er rettshåndhevelse en nødvendig forutsetning for opprettholdelse av rettsstaten. På mikronivå (i den enkelte sak), vil det normalt være vanskelig å tillegge de mer abstrakte motforestillinger knyttet til *det totale overvåkningsnivå i samfunnet* avgjørende vekt i vurderingen av hvorvidt opplysninger som kan være av nytte for en etterforskning, skal tillates innhentet. Man står overfor inkommensurable størrelser som ikke enkelt lar seg avveie dersom avveiningen skjer på mikronivået / i den enkelte sak.

Dersom man i hensikt å beskytte rettsstaten og dens idealer, etablerer overvåkings- / kartleggingsmuligheter overfor borgerne som de facto underminerer grunnleggende rettsstatsidealer, vil dette være en direkte forfeilet strategi. Man bruker tiltak for å beskytte et gode, som ødelegger det gode tiltakene skal beskytte. Man må ikke la det gode bli det godes fiende.

Dette synspunkt blir enda mer fremtredende når man argumenterer for nødvendigheten av datalagring med saker innen PSTs ansvarsområde – å verne samfunnet mot terrorisme og andre anslag mot vår samfunnsorden. Dersom man for å verne vår vestlige rettsstat mot terror, tar i bruk virkemidler som underminerer grunnverdiene i den samfunnsorden man søker å forsvare, løper man i praksis terroristenes ærend. Deres mål er jo nettopp å bekjempe den vestlige, liberale samfunnsorden. Så lenge personvern hensynene primært fremkommer i en makro-vurdering, og fremstår langt mindre tydelige i en avveining på mikro- / enkeltsaksnivå, er det nødvendig å foreta de grunnleggende avveininger på makronivået, mao ved utforming av klare begrensninger i hjemlene. Man bør derfor i mindre grad enn ellers overlate skjønnsmessige vurderinger til rettsanvenderen i den enkelte sak

2. Bør det pålegges lagring ut over den tid tilbyder har behov for data?

Forsvarergruppens hovedsynspunkt er at datalagring bør på prinsipielt grunnlag ikke tillates eller pålegges ut over hva som følger av tjenestetilbyders egne behov

Etter Forsvarergruppens syn er det en fundamental og prinsipiell forskjell på å innhente data som er lagret for andre formål, og det å pålegge lagring av data for myndighetenes formål.

I lys av de sterke personvern hensyn som gjør seg gjeldende, og som i lys av sin direkte knytning til grunnleggende rettsstatsidealer fremstår avgjørende å beskytte for å hindre at vi undergraver rettsstaten ved å de facto ta ytterligere skritt i retning av et overvåkningssamfunn, bør lagring av personverns sensitiv informasjon *for myndighetenes formål* kun skje i konkrete saker der det er mistanke om straffbart forhold.

Når det gjelder telefondata – som er mest praktisk – medfører teleselskapenes lagringspraksis at forskjellen i forhold til en pålagt lagringstid på 6 mnd ikke er vesentlig. Hva gjelder internett-trafikkdata der tilbydernes behov er begrenset, vil imidlertid innføring av en pålagt 6 måneders lagringstid være en omfattende utvidelse. Nettopp disse datatyper kan også på andre måter være mer sensitive å innføre pliktig lagring for, i den grad det lagres data som kan settes sammen til å gi informasjon om hvilke nettstedet man har besøkt, hvilket derved også forteller hvilket innhold en person har lest. Man er da vesentlig nærmere kommunikasjonsavlytting enn hva som gjelder for teledata.

3. Bruk / uthenting av data

3.1 Beslutningskompetanse

Forsvarergruppen er enig i at uthenting av data må besluttes av retten. Den personvernmessige sensitivitet av dataene tilsier uten videre at dette bør undergis strengere regler enn beslag og utleveringspålegg ellers. Dette gjelder særlig idet opplysninger som først er innhentet i en straffesak senest på tidspunktet for uttak av tiltale blir tilgjengelig for samtlige aktører, herunder siktede og fornærmede. Opplysningene er således i praksis ikke beskyttet av taushetsplikt etter at innhenting er besluttet.

3.2 I hvilke saker utlevering kan skje

I tråd med direktivets krav om at utlevering skal begrenses til ”særlige saker”, er det foreslått innført et krav om at det forhold mistanken gjelder, må ha en strafferamme på 3 års fengsel eller mer.

Forsvarergruppen vil påpeke at reguleringen her bør koordineres med reguleringen i strpl. § 216b, som bl.a. regulerer politiets adgang til å pålegge tilbyder av nett eller tjeneste ”å gi politiet opplysninger om hvilke kommunikasjonsanlegg som i et bestemt tidsrom ... har vært satt i forbindelse med anlegg ...” – mao nettopp slike data som datalagringsdirektivet omfatter. I de tilfeller som reguleres i strpl. § 216b foreligger det imidlertid en konkret mistanke *som grunnlag for datalagringen i første omgang*. Dataene lagres mao etter en målrettet begjæring, ikke som masselagring ut fra et ”kjekt å ha”-prinsipp.

Det fremstår som grunnleggende ulogisk å ha lempeligere strafferammekrav for å innhente data som er lagret uten konkret mistanke, enn hva som gjelder for innhenting 4)

av tilsvarende data etter strpl. § 216b. På dette grunnlag mener Forsvarergruppen at strafferammen for utlevering av slike data etter strpl. § 210 bør settes til 5 år, slik at det blir sammenheng i regelverket. Tilsvarende bør det ikke gjøres unntak for strafferammekravet for andre bestemmelser enn de som fremgår av strpl. § 216b første ledd litra b.

På grunn av den lovgivningsteknikk som benyttes i Norge med strafferammer som ofte går svært langt ut over hva som kan forventes ilagt av straff for det konkrete forhold, bør det for å fange opp direktivets begrep "særlige saker" etter Forsvarergruppens syn *gis retningslinjer i forarbeidene om at det også må være grunn til å anta at den konkrete handling siktelsen gjelder, kan resultere i en utmålt straff på et visst nivå, f.eks. minst 6 mnd ubetinget fengsel eller samfunnsstraff av tilsvarende omfang. En slik vurdering må da ta utgangspunkt i utmålingsnivå for handlingen slik den er beskrevet, men uavhengig av personlige omstendigheter hos siktede.*

Hva gjelder forslaget til utforming av strpl. § 210 bør vilkåret om skjellig grunn til mistanke om straffbart forhold – som ikke uttrykkelig fremgår av eksisterende lovtekst, men som etter sikker rett er innfortolket – redigeres inn i bestemmelsen som sådan når man først skal foreta endringer i paragrafen. Presiseringen i forhold til utlevering av kommunikasjonsdata vil da være begrenset til at mistanken der må være rettet mot *noen*.

I lys av at beslag og utleveringspålegg i prinsippet er to sider av samme sak, bør den tilsvarende endring som foretas i § 210, også foretas i § 203 (data kan i prinsippet beslaglegges, ikke bare utleveres). Også denne bestemmelse er uhensiktsmessig utformet ved at den ikke uttrykkelig reflekterer skjellig grunn-vilkåret.

Som det er påpekt enkelte steder i høringsnotatet, er det ikke bare i politiets / påtalemyndighetens interesse at data kan hentes ut. Relativt ofte er det behov for siktede / forsvarer å begjære innhentet slikt materiale for å imøtegå påtalemyndighetens bevisstilbud. Dette kan gjelde andre telefoner eller andre perioder enn hva politiet har fokusert på, men det kan også være tale om f.eks. å få innhentet data knyttet til fornærmede med sikte på å avsløre uriktigheter i den forklaring som danner grunnlag for tiltalen.

Etter Forsvarergruppens syn bør strafferammebegrensningen i den foreslåtte lovtekst, ikke gjelde der innhenting skjer for å forebygge at noen uskyldig blir straffet, jf. parallellen i taushetspliktbestemmelsen om sterk taushetsplikt i strpl. § 119 tredje ledd.

3.3 Forholdet til "equality of arms"

Som man er inne på i høringsnotatet, kan den begrensede lagringstid medføre at forsvarer og siktede kommer inn i bildet for sent til å begjære sikring av data som kan tale til siktetes gunst. Dette hensyn til "equality of arms" må etter forsvarergruppens syn søkes avhjulpet med regler om at politiet ved innhenting av data, omgående må forelegge spørsmålet om hvorvidt ytterligere data bør sikres, for forsvarer.

4. Lagringssted

Forsvarergruppen slutter seg til at lagring – uansett omfang – forblir tilbyders ansvar.

5)

5. Lagringstid

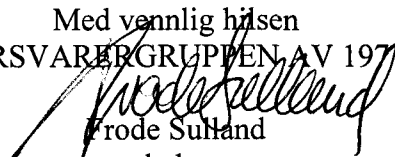
For det tilfelle at det innføres pliktig lagring ut over den periode tilbyder selv har behov for dataene, bør lagringstiden etter Forsvarergruppens syn gjøres så kort som mulig.

6. Økonomiske konsekvenser

Det er viktig å være oppmerksom på den betydelige omfangsøkning bruk, analyse og bevisføring knyttet til kommunikasjonsdata medfører for rettsprosessene. Dataene innebærer at forsvarerarbeidet blir svært mye mer omfattende, og nødvendiggjør til dels bruk av ekstern analyseekspertise på forsvarersiden. Fra et egeninteresseståsted skal vel ikke forsvarerne klage på dette, men det oppstår spørsmål om hvorvidt eskaleringen av kompleksiteten i sakene står i samsvar med de samfunnsmessige gevinster.

Hertil kommer det forhold at bevisførsel om kommunikasjonsdata ofte er svært utfordrende, og lett kan bli så vanskelig tilgjengelig for retten at den i praksis aksepterer etterforskers redegjørelse for resultatene uten å etterprøve slutningene. Dette er rettssikkerhetsmessig svært uheldig.

Den ekstra kompleksitet i etterforskningen og bevisføringen medfører også at etterforskningen tar lengre tid, at forsvarernes behov for tilstrekkelig tid til forberedelse av forsvaret oftere vil medføre at fristene for avholdelse av hovedforhandling blir for knappe til at forsvaret kan forberedes forsvarlig. Mer arbeid knyttet til den enkelte sak vil også kunne medføre større utfordringer mht berammelser generelt.

Med vennlig hilsen
FORSVARERGRUPPEN AV 1977

Frode Sulland
leder