Personvernkommisjonen:

Uttalelse om datalagringsdirektivet

Juni 2008

Personvernkommisjonen har drøftet EU-direktiv 2006/24 (datalagringsdirektivet) og samlet seg om en felles uttalelse. Da forslag til innføring av direktivet i norsk rett ennå ikke er lagt frem, er våre kommentarer basert på direktivteksten.

Personvernkommisjonen har som mandat å vurdere hvordan personvernet bør ivaretas i møte med motstående hensyn og verdier. Personvernkommisjonen mener det må foretas en grundig utredning av konsekvensene for personvernet dersom direktivet blir iverksatt. Vi må også få en vurdering av konsekvensene dersom direktivet *ikke* innføres i Norge.

Vi kan ikke støtte innføring av direktivet uten at *behovet* for utvidet lagring er bedre dokumentert. Både politiets og andre nasjonale myndigheters behov for utvidet lagring og tilgang til trafikkdata i det omfang som er foreslått må derfor begrunnes bedre.

Direktivets overordnede formål er å bekjempe alvorlig kriminalitet. Den teknologiske utvikling har forandret metodene som brukes både ved terror og andre former for kriminalitet. Dette har skapt et behov for nye metoder ved etterforskning og bekjempelse av kriminalitet. I fotsporene til den teknologiske utviklingen følger kriminelle som søker å utnytte denne til terrorisme og andre forbrytelser. Derfor er det viktig for politi og påtalemyndigheter å ha tilgang til de verktøyene man til en hver tid trenger til bekjempelse av kriminalitet. Det er også viktig at dette skjer innenfor demokratiske og klare rammer. Vi utelukker ikke at trafikkdata kan være viktige for politiet ved etterforskning og oppklaring av kriminelle handlinger, men vi stiller oss likevel kritisk til beslutningsgrunnlaget for den omfattende lagringsplikten som følger av direktivet. Derfor etterlyser kommisjonen dokumentasjon av politiets og andre myndigheters behov for trafikkdata i det omfang som følger av direktivet.

Personvernkommisjonen ser behovet for et regelverk både for lagring og utlevering av trafikkdata. I dag får politiet tilgang til trafikkdata fordi teletilbydere lagrer opplysningene for kommunikasjons- og faktureringsformål. Politiets tilgang til opplysninger er regulert i ulike regler og gjennom praksis fra Post- og teletilsynet. Regelverket er uoversiktlig og vanskelig tilgjengelig for borgerne. Dette er i seg selv en svakhet. Videre ser man nå en utvikling i teleoperatørenes faktureringsrutiner som kan føre til at politiet mister denne tilgangen til trafikkdata som de til nå har hatt. Som en følge av den teknologiske utviklingen går teletilbyderne fra å fakturere for *bruk* (som fordrer lagring av trafikkdata) til å fakturere for *tilgang*. Dermed har de ikke behov for å lagre trafikkdata. En slik utvikling gjør at politiet vil miste verdifull informasjon. Etter Personvernkommisjonens oppfatning er det derfor ønskelig med en *grundig utredning av behovet for et regelverk som sikrer politiets arbeidsmetoder og ivaretar personvernet*.

I enkelte saker er det vanskelig for politiet å få tak i vitner. Tendensen er særlig tydelig innen organisert kriminalitet. I slike saker ser man at trafikkdata og elektroniske spor er svært sentrale bevis. Informasjonen er på mange måter et taust vitne og representerer i mange saker en tråd som lar seg følge. Men dersom det legges opp til pliktig lagring av trafikkdata, så vil det sannsynligvis forekomme ønsker/press fra ulike hold for å få tilgang til disse data.

Kredittilsynet og tollvesenet kan finne gode begrunnelser for at tilgang til trafikkdata vil bistå disse etatene i sitt arbeid. Helsevesenet kan argumentere for at kartlegging av sosiale kontaktnett gjennom trafikkdata kan redde liv og helse når man trenger å spore bærere av alvorlige smittsomme sykdommer. Nød- og redningsetater vil kunne argumentere for at trafikkdata vil kunne hjelpe dem med sporing av savnede personer. Personvernkommisjonen mener det er en reell fare for at pliktmessig lagring av trafikkdata med bekjempelse av alvorlig kriminalitet som formål etter hvert vil resultere i at disse data brukes til andre formål[1], som hver i sær kan være gode, men hvor den samlede bruken kan utgjøre en alvorlig trussel mot personvernet.

Personvernkommisjonens fokus er naturlig nok direktivets innvirkning på personvernet. Vi mener at datalagringsdirektivet setter både personvernet og ytringsfriheten på prøve. Dette vil gjelde selv om lagring av trafikkdata i henhold til direktivet ikke anses som kontinuerlig eller regelmessig overvåkning av borgerne. Verdien av lagring må nemlig også veies opp mot effekter på frimodighet. Dette gjelder selv om formelle friheter ikke berøres, og selv om de registrerte data kun skal være tilgjengelige for politiet under regulerte forhold. Allerede vissheten av at noen *kan* lete seg fram til dine kontakter og dine bevegelser, både i det virkelige rommet og på Internett, kan være nok til å hemme borgere i utøvelsen av sine friheter til å samles, til å ytre seg og til å søke opplysninger. Dette er grunnleggende rettigheter i et demokrati, som kommer til uttrykk både i norsk lovgivning og i Den europeiske menneskerettskonvensjon (EMK). Etter kommisjonens oppfatning vil innføring av direktivet kunne svekke opplevelsen av privatliv og privat kommunikasjon.

EMK artikkel 8 annet ledd åpner for at det kan gjøres inngrep i personvernet. For at et slikt inngrep skal være forsvarlig må det blant annet være *nødvendig i et demokratisk samfunn*. I dette ligger det etter Den Europeiske Menneskerettighetsdomstolens (EMD) praksis at det må være en «pressing social need» for å gripe inn i personvernet. Det holder ikke at det er hensiktsmessig, rimelig eller ønskelig. Inngrepet som gjøres må dessuten være proporsjonalt i forhold til formålet som ønskes oppnådd. Den omfattende lagringsplikten som følger av direktivet kan etter Personvernkommisjonens oppfatning være problematisk i forhold til nødvendighetsprinsippet og proporsjonalitetsprinsippet. Forskning fra blant annet Tyskland[2] sår tvil om betydningen av trafikkdata for oppklaring av kriminalitet. Rapportene fra Tyskland omhandler selvsagt forhold knyttet til det tyske kriminalitetsbildet, og kan dermed ikke påberopes direkte i forhold til norske forhold. Kripos mener å ha erfaring for at trafikkdata har stor betydning for oppklaring av kriminalitet. Personvernkommisjonen etterlyser imidlertid en studie, tilsvarende den man har gjort i Tyskland, for norske forhold. Kriteriene som følger av

---

[1] Våren 2008 ble det rapportert at Deutsche Telekom ulovlig hadde analysert trafikkdata i et forsøk på å identifisere en pressekilde, jf. *Prosecutors investigate Deutsche Telekom over data misuse*; 29. mai 2008, tilgjengelig på adresse: http://www.out-law.com//default.aspx?page=9153.; *Overvåkingsskandalen vokser*; 3. juni 2008, tilgjengelig på adresse: http://e24.no/utenriks/article2462382.ece

[2] Se: Max-Planck-Institut für ausländisches und internationales Strafrecht: *Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO: Forschungsbericht im Auftrag des Bundesministeriums der Justiz* (Freiburg, februar 2008); tilgjengelig på adresse: http://www.vorratsdatenspeicherung.de/images/mpi-gutachten.pdf, som hevder at trafikkdata kun vil bidra til oppklaring i et lite antall, anslagsvis 0,002 % av det totale antall kriminalsaker, og anslag fra det tyske Bundeskriminalamt, som ifølge en separat studie utført sommeren 2007 regner med at datalagring vil føre til en økning i oppklaringsraten «fra dagens 55 prosent, i beste fall til 55,006 prosent», jf. http://www.heise.de/newsticker/Vorratsdatenspeicherung-fuer-eine-0-006-Prozentpunkte-hoehere-Aufklaerungsquote--/meldung/92746

EMK artikkel 8 krever etter kommisjonens oppfatning en grundig klargjøring i form av *dokumentasjon av behovet for lagring* (både lagringstid og omfanget av opplysninger) og en grundig konsekvensutredning: Både personvernmessige konsekvenser av en eventuell innføring og konsekvenser for politiet og kriminalitetsbildet dersom Norge ikke innfører direktivet. Personvernkommisjonen er usikker på om slik dokumentasjon eller utredninger ligger til grunn for direktivet eller for arbeidet som er gjort i forbindelse med en eventuell innføring av direktivet i norsk rett.

Det synes klart for Personvernkommisjonen at direktivet representerer noe nytt i forhold til dagens regime for lagring av trafikkdata. Direktivet innebærer for det første *lagring av nye typer data*, som for eksempel geolokaliseringsdata og epost-logger. For det andre vil direktivet medføre *lengre lagringstid* enn det som følger av dagens praksis. For det tredje berøres langt *flere organisasjoner* enn det som er dagens situasjon, blant annet omfatter direktivet mange ISPer. For det fjerde gir direktivet et *nytt normativt grunnlag* for lagring av trafikkdata – en plikt til å lagre for andre formål enn faktureringsformål. Det er også et moment at man går fra en *rett til å lagre opplysninger* for visse formål, til en *plikt til å lagre opplysninger*. Disse forholdene må hensyntas i vurderingen av om og eventuelt hvordan direktivet skal innføres i norsk rett.

Dersom direktivet skulle bli innført, mener kommisjonen at det er viktig at lagringstiden gjøres så kort som mulig. Personvernkommisjonen vil også peke på spørsmålet om hvilken sikkerhet man har for de opplysningene som lagres. Mye tyder på at mange organisasjoner ikke har fullgode mekanismer for sikring av trafikkdata mot uautorisert spredning[3]. Det har vært fremhevet som en trussel mot sikkerheten at tilbydere pålegges å lagre store mengder data på vegne av myndighetene, og at manglende egeninteresse i lagring av opplysningene til dette formålet vil kunne gå ut over sikkerheten. Dersom lagring i en så omfattende skala som direktivet legger opp til blir gjennomført, må det fra myndighetens side settes krav til sikring i form av kryptering og deponeringsmekanismer som hindrer at så vel teletilbyderen selv, som myndighetene, kan få tilgang til lagrede data før korrekt rettslig grunnlag for tilgang kan fremlegges. Det må også sikres at enhver tilgang som gis, avgrenses til de data det skal være lovlig tilgang til. Det er etter kommisjonens oppfatning avgjørende at en eventuell innføring av direktivet ledsages av sikringer – tekniske og organisatoriske så vel som juridiske – mot at det lagrede materialet kan brukes til strategisk informasjonsanalyse eller andre former for generell informasjonssøking. I forhold til den tekniske siden vil dette innebære at det må utvikles nye, finmaskede systemer for tilgangskontroll og datasikring som, så vidt Personvernkommisjonen har kjennskap til, ikke er tilgjengelig på markedet i dag.

Oslo 12. juni 2008

***

For spørsmål vedrørende denne uttalelse, vennligst ta kontakt med kommisjonens leder Kjellbjørg Lunde (mobil: 95770083, arbeid: 55572000, epost: kjellbjorg.lunde@fmho.no) eller sekretariatets leder Lee Bygrave (epost: l.a.bygrave@jus.uio.no).

---

[3] Personvernkommisjonen viser til den såkalte Tele2-saken, hvor Tele2 våren og sommeren 2007 lot kredittopplysninger om et sekssifret antall personer tilflyte uvedkommende. En enda større skandale fant sted i Storbritannia høsten 2007, hvor to ukrypterte disker med personopplysninger vedrørende alle familier i Storbritannia med barn under 16 år kom på avveie. Se: *Brown apologises for records loss*, BBC News, 21. november 2007, http://news.bbc.co.uk/2/hi/uk_news/politics/7104945.stm.