



Fra Økokrim: Lagringsplikt for trafikkdata¹

Økokrim-sjef Einar Høgetveit

Einar Høgetveit,
cand. jur. 1978,
Universitetet i Oslo,
lic. jur. 1985 samme
sted. Har vært i
Økokrim siden 1991,
Økokrim-sjef fra 2000.
Har tidligere jobbet
bl.a. i Lovavdelingen
i Justisdepartementet.
Leder av Straffelov-
kommisjonen 1994–
2002. einar.hogetveit@
politiet.no

Datalagringsdirektivet

For tiden diskuteres om Norge bør implementere EUs datalagringsdirektiv av 15. mars 2006 (2006/24). Direktivet pålegger teletilbydere å lagre opplysninger om tid, sted, varighet, avsender og mottaker for all telekommunikasjon (telefoni og internett), såkalte trafikkdata, i en periode fra seks måneder til to år. Formålet er å sikre at slike data er tilgjengelige i forbindelse med etterforskning og irettføring av alvorlig kriminalitet, slik det enkelte land definerer dette.

Lagring av trafikkdata var vedtatt i flere EU-land allerede før EU-direktivet om dette ble vedtatt. For eksempel vedtok Danmark i 2002 en lagringsplikt på ett år. Direktivet skal sikre at landenes regler på dette området ikke blir for sprikende.

Hva lagringsdirektivet ikke gjelder

På bakgrunn av ulike innlegg i den norske debatten kan det være behov for å slå fast hva datalagringsdirektivet *ikke* dreier seg om. Det er blant annet ikke tale om å lagre *innholdet* i kommunikasjonen, bare trafikkdata. Det er heller ikke tale om å registrere hvilke *nettsider* man besøker. Lagringen skal ikke skje hos *politiet* eller et annet myndighetsorgan, men hos teletilbyderne eller ved en sentralisert løsning for disse, og da bare som ikke-lesbare rådata. Det er videre ikke grunnlag for å hevde at lagring av trafikkdata innebærer at de som bruker teletjenester, blir gjenstand for *overvåking*, i noen som helst rimelig betydning av dette ordet; det er ikke noen som vil følge løpende med på hva som registreres, og det vil ikke være anledning til å gå på «fisketur» i datamengdene.

I debatten har man også møtt argumentet om at lagring av trafikkdata innebærer at *alle behandles som kriminelle*. Men i så fall betraktes vi alle som kriminelle i svært mange sammenhenger. I et moderne samfunn som vårt samles det elektroniske spor om oss på en rekke ulike steder. Dette gjelder for eksempel finansin-

1. En kortere utgave av denne artikkelen er trykt som innlegg i Aftenposten 8. september 2008.



stisjoner som forvalter våre bankkonti, næringsdrivende som lagrer kunderegistre og regnskapsbilag, bomselskaper som registrerer våre passeringer, eller fastleger som fører pasientjournaler. Håndtering av personopplysninger er en del av hverdagen i enhver moderne bedrift, også hos teletilbydere.

Direktør i Datatilsynet, Georg Apenes, er en iherdig motstander av å implementere direktivet i Norge. Han mener direktivet er uttrykk for det han kaller «totalitært svermeri». Dette er kanskje elegant retorikk og viser klart hans ståsted, men er vel ellers lite opplysende.

Det er videre liten grunn til å hevde, slik Personvernkommisjonen gjør i en uttalelse fra juni 2008, at en implementering av direktivet vil kunne *hemme borgerne* i deres frihet til å samles, ytre seg og søke opplysninger. Norge har solide demokratiske tradisjoner, og de borgerlige frihetene står sterkt. Det er liten grunn til å tro at en plikt til å lagre trafikkdata – en lagring som skjer i stor utstrekning i dag (om enn ikke alltid i samme grad som EU-direktivet krever) – vil ha snyderlig innvirkning på borgernes frimodighet.

Lagring i dag

Lagring av trafikkdata skjer i stor utstrekning i dag. Blant annet har telefontilbydere behov for dette for å fakturere kundene for bruk av tjenester. Dermed har også politiet kunnet få tilgang til slike data etter foreskrevne prosedyrer til bruk i etterforskningen av straffbare handlinger. Ifølge lov om elektronisk kommunikasjon (ekomloven) § 2-7 andre ledd skal slike data slettes så snart de ikke lenger er nødvendige for kommunikasjons- eller faktureringsformål. En sletteplikt følger også av personopplysningsloven § 28. Etter Datatilsynets konsesjonspraksis skal dataene slettes etter tre til fem måneder.

Men i praksis skjer lagring også i lengre tid enn dette, slik at politiet når vilkårene er til stede, har kunnet innhente trafikkdata også eldre enn fem måneder. I framtiden kan det imidlertid tenkes at det blir gratis å ringe eller at teletilbyderne vil fakturere for tilgang til en tjeneste, ikke bruk, slik at de selv ikke vil ha behov for lagring. Dersom det ikke innføres en lagringsplikt for trafikkdata, vil sjansen øke for at dataene er slettet når politiet trenger dem i etterforskningen.

Behovet for lagring

Personvernkommisjonen etterlyser i sin uttalelse dokumentasjon av behovet for lagring av trafikkdata i det omfang som følger av direktivet. Nå har spørsmålet om implementering av direktivet ennå ikke vært på høring – noe det snarest bør – og behovet vil ventelig bli bedre belyst da. Men det er enkelt å peke på kriminalitetstyper som vanskelig – og noen ganger overhodet ikke – lar seg oppklare uten at politiet har tilgang til trafikkdata.

Ett eksempel er internettrelaterte overgrepssaker. I den såkalte «Operasjon Kola», som er et samarbeidsprosjekt mellom Interpol og Europol, ble det på bakgrunn av arrestasjon av en belgisk far, som misbrakte sine døtre, avdekket et internasjonalt nettverk som inkluderte mer enn 2.500 mistenkte i 19 forskjellige land, deriblant Norge. Politienheter i 28 land samarbeider om saken, og det er tatt beslag i over en million bilde- og filmfiler, samt over 50.000 e-poster. Etterforskningen pågår fortsatt, og så langt er det identifisert og lokalisert mer enn 30 barn, som således er reddet fra misbruk. En slik sak er ikke mulig å etterforske uten trafikkdata.

Et annet eksempel er den såkalte «Operasjon Sledgehammer» fra høsten 2007. På en kroatisk internettside med bilder av seksuelle overgrep ble det i løpet av en 76-timersperiode notert 12 millioner treff fra nesten 150.000 forskjellige IP-adresser fra 170 ulike land. Flere hundre av IP-adressene var norske, men da de aktuelle IP-adressene ble overlevert norsk politi, var de nødvendige data for identifikasjon ikke lenger lagret.

Et annet eksempel på en sakstype som ikke er mulig å etterforske uten tilgang til trafikkdata, er den stadig økende forekomsten av nettbedragerier.

Det er dårlig sammenheng mellom å mene at politiet skal bekjempe slike former for kriminalitet, samtidig som man er motstander av lagring av trafikkdata.

Trafikkdata kan være avgjørende for oppklaring i nær sagt alle typer saker. Det er få saker av alvorlig art hvor ikke etterforskningen også inneholder elektroniske spor og lagrede trafikkdata. Et typisk eksempel er narkotikasaker, som ofte starter med pågrepelse av en kurér, mens analyse av trafikkdata gir grunnlag for videre etterforskning mot mottagere og bakmenn. I flere innsidesaker har tilgang til trafikkdata vært helt nødvendig for å avsløre kontakt mellom aktørene.

Trafikkdata kan også være nyttige for å fastslå at en sak kan være mindre alvorlig enn den først gir inntrykk av. Politiet har i noen tilfeller etterforsket trusler mot norske skoler på Internett. På grunnlag av trafikkdata har det lyktes å identifisere avsendere og få konstatert at det ikke foreligger noen reell fare for realisering av trusselen. I et annet tilfelle ble Internett brukt til å framsette alvorlige trusler og sjikane mot en mindreårig jente. Meldingene ga inntrykk av å komme fra en voksen person, men trafikkdata avslørte at de kom fra en jevnaldrende jente.

Trafikkdatas bevisverdi

Det hevdes som et argument mot lagringsplikt for trafikkdata at de ikke er egnet som bevis. Det vises til at de er produsert for helt andre formål og kan være lette å manipulere. Dette gir uttrykk for en manglende forståelse for hva et bevis er. De typiske bevis er jo

nettopp ikke laget for å være bevis, men innsamles i ettertid av politiet fordi de kan kaste lys over saken. Å vurdere tyngden av et bevis opp mot mulige feilkilder er politiets oppgave, noe som på dette området i prinsippet ikke skiller seg fra annen bevishåndtering.

Datakyndige kriminelle

Det er hevdet at direktivet ikke «treffer» i forhold til formålet, fordi datakyndige kriminelle vil finne andre måter å kommunisere på, for eksempel ved å bruke satellitt-telefon fra teletilbydere utenfor EØS-området. Nå kan vel trafikkdata bli lagret også i land utenfor EØS-området. Og selv om det finnes lovbrytere med stor datakunnskap, gjelder dette likevel de færreste. I praksis er de fleste avhengig av å kommunisere gjennom vanlige kanaler.

Det er ellers et litt underlig argument at fordi politiet eventuelt ikke klarer å ta noen datakyndige kriminelle, bør man heller ikke ha mulighet til å avsløre gjerningspersoner som er mindre avanserte.

Behov for å forebygge misbruk

Trafikkdata og andre personopplysninger lagres som nevnt i stort omfang i vårt samfunn uavhengig av datalagringsdirektivet. Enhver lagring av persondata muliggjør misbruk. Direktivet søker på sitt område å motvirke dette på ulike måter. Dels skal det være straffbart å skaffe seg urettmessig adgang til et informasjonssystem og til de dataene det inneholder. Den som lider skade som følge av en ulovlig behandling av de lagrede dataene, har krav på erstatning. Utlevering av dataene skal bare skje til kompetente myndigheter og etter foreskrevne prosedyrer i overensstemmelse med krav om nødvendighet og proporsjonalitet. Direktivet inneholder også krav til måten dataene skal lagres og sikres på.

Dette er likevel generelle og lite presise regler, og i det videre lovgivningsarbeidet i Norge bør det legges betydelig energi i å utvikle rettssikkerhetsgarantiene. Etter mitt syn er det dette debatten bør dreie seg om, snarere enn om direktivet bør kastes helt på skraphaugen.

EØS-relevant?

Det er reist spørsmål om lagringsdirektivet er såkalt EØS-relevant. Det pågår en tvist mellom EU og Irland om dette. Dersom direktivet ikke er EØS-relevant, vil Norge ikke være forpliktet til å implementere det. Men spørsmålet om det bør innføres en lagringsplikt for trafikkdata i Norge kan og bør avgjøres uavhengig av spørsmålet om EØS-forpliktelse.

Det er for øvrig grunn til å merke seg at bakgrunnen for Irlands søksmål mot EU er landets ønske om å beholde en lengre lagringstid, nemlig tre år, enn den toårsfristen som EU-direktivet tillater.

Datalagring trengs

Det finnes relevante argumenter mot datalagring. Motstanderne av EUs datalagringsdirektiv har vært flinke til å framføre disse i debatten. Dette har derfor ikke vært mitt anliggende her. Mitt hovedbudskap er å framholde at det vil bety en vesentlig svekkelse av kriminalitetsbekjempelsen i Norge dersom teletilbyderne ikke pålegges en lagringsplikt for trafikkdata. Norge vil dessuten bli stående igjen som nærmest det eneste land i Europa hvor politiet ikke har tilgang til slike bevis.

Dette bør politikerne være klar over når de skal ta stilling til spørsmålet om lagringsplikt.