



Sammendrag

Elektronisk kommunikasjon setter innholdsrike spor

All elektronisk kommunikasjon setter elektroniske spor som kan logges og lagres. Nye tjenester knyttet til PC, internett og mobiltelefoni setter spor som kan si mye om en persons kommunikasjon, bevegelser, handlinger og interesser. Den nye ekomloven er derfor også en viktig personvernlov.

Tillit er avgjørende for bruken av elektroniske medier

Vårt moderne samfunn er blitt avhengig av at folk utnytter elektroniske tjenester. Både elektronisk handel og offentlige tjenester på nett er avhengig av folks tillit til at det er trygt å bruke de nye elektroniske mediene. Da må personvernet ivaretas og brukerne bør gis mulighet til å forsikre seg om at lagrede kommunikasjonsdata ikke misbrukes.

Internasjonal utvikling legger press på personvernet

Følgene av 11. september og "krigen mot terror" har internasjonalt satt personvernet under press gjennom økt tilbøyelighet til å tillate lagring av elektroniske spor for bruk i kriminalitetsbekjempelse. Det danske Folketinget har vedtatt lovgivning som pålegger teleoperatører og internettleverandører å registrere trafikkdata og lagre dem i ett år for bruk i en eventuell etterforskning.

Lagringstid og anonyme tjenester er stridstema

Skal trafikk- og lokasjonsdata fra elektronisk kommunikasjon lagres i ett år og skal vi innskrenke muligheten til å kommunisere anonymt gjennom elektroniske nettverk? Denne type tiltak kan gi politiet bedre vilkår og slik bidra til et tryggere samfunn. Samtidig vil de gripe inn i personvernet. Interessene må avveies politisk.

Personvern og samfunnsvern

En norsk mobiltelefonoperatør lanserer i disse dager en tjeneste som lar velmenende foreldre overvåke sine barns bevegelser. Barnet utstyres med en brikke for satellittbasert geografisk posisjonering som for eksempel kan festes på armen, sys inn i klærne eller innlemmes i barnets mobiltelefon. Så kan foreldrene over internett observere barnets posisjon med tre meters nøyaktighet på et kart og bli varslet på mobiltelefon hvis det beveger seg utenfor det man har angitt som "tillatt" område. Dette er en tjeneste basert på elektronisk kommunikasjon, som møter et legitimt behov og som kan

bidra til økt trygghet for mange. Samtidig gir den store muligheter for misbruk og utgjør således en utfordring for personvernet. Slik representerer den også en type problemstillinger som vil florere i årene som kommer.

Ekomloven er også en personvernlov

Elektronisk kommunikasjon omfatter i dag nesten all kommunikasjon som ikke skjer ansikt-til-ansikt eller gjennom papirpost. Viktige elektroniske kanaler er fasttelefoni, mobiltelefoni, e-post, internett og videokonferanser. Reguleringen av dette området må derfor ikke bare sikre allmenn tilgjengelighet til gode og kostnadseffektive kommunikasjonstjenester,

men må samtidig ivareta andre sentrale hensyn som folks tillit til elektroniske tjenester, effektiv kriminalitetsbekjempelse og vern av privatsfæren. Når Stortinget nå diskuterer proposisjonen til ny lov om elektronisk kommunikasjon (Ekomloven) må representantene forholde seg til alle disse legitime hensynene.

Økende bruk av nye medier

Både på jobben og privat har spesielt PC og mobiltelefon fått helt sentrale roller i kommunikasjon mellom mennesker. Stadig flere jobber, handler, koordinerer gjøremål, møter nye mennesker, flørter med kjæresten samt prater med venner og familie ved hjelp av de nye mediene. En global undersøkelse viste nylig at 80% av arbeidstakere foretrekker e-post i jobbrelatert kommunikasjon, mens 20% foretrekker telefon. Nyere og kanskje noe overraskende anvendelser inkluderer helsetjenester online, som for eksempel leger som kan kontaktes pr e-post og psykologer som kan gi terapi over nettet. For mange representerer internett en unik arena hvor de har lettere for å uttrykke seg direkte og åpenhertig enn ved et fysisk møte. Det har åpenbart stor nytteverdi for mange mennesker å kunne kommunisere fritt, også elektronisk, uten å frykte at uvedkommende kikker en i kortene, det være seg myndigheter eller private aktører.

Brukernes tillit krever transparens

Regjeringens mål i eNorge-planen baserer seg på at folk må ha tillit til at det er trygt å benytte de nye elektroniske mediene. Denne tilliten er ingen selvfølge og forutsetter blant annet at tjenestene virker slik de skal, at kommunikasjonen er skjermet mot innsyn fra uvedkommende og at kommunikasjonsdata er sikret mot misbruk. Et viktig element for å sikre tilliten til de nye mediene er transparens i forhold til hvordan innsamlede kommunikasjonsdata anvendes. Brukerne bør gis mulighet til å føre en viss kontroll med leverandører av elektro-

niske kommunikasjonstjenester for å sikre at lagrede kommunikasjonsdata ikke spres eller misbrukes på annen måte.

Elektroniske spor

All elektronisk kommunikasjon setter spor som kan loggføres og lagres slik at det i ettertid er mulig å si noe om hvilken kommunikasjon som har funnet sted. Spesielt innholdsrike spor etterlates ved bruk av moderne elektroniske hjelpemidler som PC og mobiltelefon. Slike spor kan gjøre det mulig å si mye om en persons kommunikasjon, bevegelser, handlinger, interesser og oppfatninger. Nettopp derfor er det viktig at slike spor ikke lagres unødige og at det som faktisk lagres ikke tilflytter uvedkommende. Vi skiller mellom tre ulike typer kommunikasjonsdata:

- *Trafikkdata:* Hvilke kommunikasjonsanlegg (f eks PC eller mobiltelefon) har vært i forbindelse med hverandre, når og hvor lenge?
- *Lokasjonsdata:* Hvor befant kommunikasjonsutstyret seg geografisk da det ble kommunisert?
- *Innholdsdata:* Hva var innholdet i kommunikasjonen - hva ble sagt eller skrevet?

Disse dataene kan kobles til abonnements- eller identitetsdata. Dette er opplysninger om identiteten til abonnenten eller brukeren og finnes i et abonnementsregister (f eks hos Telenor) eller i en registreringsbok (f eks på en internettkafe). For telefoni er tjenestetilbyder pliktig til å ha slike registre, mens det så langt ikke er etablert en tilsvarende plikt for tilbydere av databaserte kommunikasjonstjenester. Uregistrerte kontantkort for mobiltelefoni kan sies å befinne seg i en gråsoner i forhold til registerplikten, men er etter gjeldende praksis tillatt. På datasiden finnes det mange anonyme kommunikasjonstjenester – dette gjelder tjenestetilbydere som kan tilby brukeren garanti for full anonymitet samt tilbydere som ikke har noe eget behov for kunderegister (f eks når tjenesten er rent reklamefinansiert).

Internasjonal utvikling

I etterforskning av så godt som alle typer kriminalitet er utnyttelse av elektroniske spor helt nødvendig. Terrorangrepene på USA den 11. september 2001 og den påfølgende "krigen mot terror" har internasjonalt medført en økt innsats for å samle inn og utnytte elektroniske spor til å avverge og etterforske terror og annen alvorlig kriminalitet. Personvernet er kommet under press ettersom flere land har tilpasset sitt lovverk for å tillate økt registrering og lagring av data knyttet til elektronisk kommunikasjon. For eksempel vedtok det danske Folketinget i mai 2002 ny "antiterror"-lovgivning som blant annet påbyr alle teleoperatører og internettleverandører å registrere og lagre trafikkdata i ett år. Så langt har denne tendensen ikke vært spesielt fremtredende i Norge.

Nytt europeisk regelverk

Europarådets konvensjon om cyberkriminalitet fra 2001 samt EU-direktiv 2002/58 om personvern i elektronisk kommunikasjon skal begge implementeres i norsk lovgivning. Konvensjonen åpner for adgang til lagring av trafikkdata samt avlytting av kommunikasjon ved behov i etterforskning. EU-direktivet sikter blant annet mot å beskytte personvernet ved kommunikasjon og begrenser mulighetene til å få tilgang til trafikk- og lokasjonsdata. Direktivets regler kan likevel fravikes i forbindelse med kriminalitetsbekjempelse og av hensyn til statens sikkerhet. Den norske straffeprosessloven gir hjemmel for bruk av alle typer kommunikasjonsdata og synes å være i samsvar med såvel konvensjonen som direktivet.

EU vurderer å pålegge lagring av trafikk- og lokasjonsdata fra bruk av mobil- og fasttelefon, e-post, chat-rom, tekstmeldingstjenester, internett og annet elektronisk kommunikasjonsutstyr for en periode på ett til to år. Flere EU-land, herunder Frankrike, Belgia, Spania, Storbritannia og altså Danmark, har allerede innført slik lagringsplikt og et eventuelt pålegg vil omfatte Norge gjennom EØS-avtalen.

Ekomloven

Lov om elektronisk kommunikasjon (Ekomloven) skal erstatte Teleloven fra 1995 og vil bli den nye "grunnloven" for det omfattende saksområdet elektronisk kommunikasjon. Den vil bli en svært viktig lov også i forhold til personvernet. Proposisjonen til ekomlov medfører ikke i utgangspunktet noen vesentlig innskrenkning av personvernet knyttet til elektronisk kommunikasjon. Imidlertid overlates viktige avveininger til forskriftene - primært spørsmålet om utvidet lagringstid for trafikkdata. Samferdselsdepartementet vil da, uten å måtte konsultere Stortinget, kunne treffe politiske valg om en mulig innsnevring av den uovervåkede sfære. Det finnes gode juridiske grunner for en løsning hvor detaljer overlates til forskriftene. Viktige avveininger omkring samfunnets overvåkningsnivå og kårene for menneskers integritetsvern bør likevel gjøres gjenstand for politisk og offentlig debatt. Da Danmark i fjor innførte loggingsplikt og 12 mnd lagring for trafikkdata ble dette ikke lagt til en forskrift, men tatt inn i lovteksten etter debatt i Folketinget.

Lagring av trafikk- og lokasjonsdata

Av hensyn til effektiv etterforskning og samfunnets interesse i oppklaring av kriminalitet er det ønskelig at loggførte elektroniske spor lagres i en begrenset periode for mulig bruk i en eventuell etterforskning. Proposisjonen medfører i utgangspunktet ingen endring i prinsippet om at trafikk- og lokasjonsdata skal slettes eller anonymiseres så fort man ikke lenger trenger dem til faktureringsformål, dvs. senest etter 3 eller 5 mnd avhengig av om det faktureres månedlig eller kvartalsvis.

Spørsmålet er: bør det innføres loggingsplikt for trafikk- og lokasjonsdata med lagringstid på opptil ett år? Fordelen med å gjøre dette er at det da blir mulig for politi og rettsvesen å gå noe lengre tilbake i tid for å studere elektroniske spor som kan bidra til oppklaring og domfellelse i en sak. Medaljens bakside er at personvernet vil svekkes noe.

Trafikk- og lokasjonsdata er undergitt grunnleggende personvernrelaterte prinsipper som minimalitets- og formålsbestemthetsprinsippet. Dette krever tilbakeholdenhet i for-

hold til lagring og sekundær utnyttelse av kommunikasjonsdata. Slike data må derfor lagres kun hvis dette er strengt nødvendig og de bør ikke benyttes til sekundære formål som er uforenlige med de formål som dataene i hovedsak ble samlet inn for.

Adgangen til anonym kommunikasjon

Proposisjonen endrer ikke adgangen til å tilby og bruke anonyme kommunikasjonstjenester. Teknologirådet mener likevel at dette temaet bør være på dagsorden i debatten omkring ekomloven. Muligheten til å kunne opptre anonymt i ulike sammenhenger er et sentralt element i et demokrati. Anonymitet kan spille en positiv rolle i forhold til ytringsfrihet, politisk deltakelse, personvern og den enkeltes livsutfoldelse. Samtidig er anonymiteten problematisk i en situasjon hvor man er avhengig av elektroniske spor for å kunne ta kriminelle og terrorister.

Spørsmålet er: bør anonyme kommunikasjons-tjenester forbys ved at tilbydere av enhver elektronisk kommunikasjons-tjeneste pålegges å ha identitetsregistre eller passordløsninger med referanse til brukerens identitet? Dette er en forutsetning for å kunne nyttiggjøre seg eventuelle trafikkdata og kan gjøre det vanskeligere for kriminelle å unnsnippe lovens lange arm.

Muligheten for sterk anonymitet ved elektronisk kommunikasjon er allerede ganske begrenset som følge av mulighetene til å sammenholde loggførte data fra mange ulike kilder. Det kan derfor være grunn til å forsvare det som er igjen av elektronisk anonymitet. På den annen side kan man i de fleste tilfeller oppnå tilstrekkelig anonymitet overfor dem man kommuniserer med gjennom bruk av pseudonym eller brukernavn. Man kan altså kommunisere med en viss anonymitet selv om adgangen til sterk teknisk anonymitet (usporbarhet) skulle tas bort. Det vil da bli mulig for politiet ved en eventuell etterforskning eller et søk etter en savnet person å finne ut hvem som har kommunisert med hvem og når.

Redaksjon

Erlend Jakobsen, Tore Tennøe

Abonnement

post@teknologiradet.no

Alle utgaver av *Fra rådet til tinget* kan leses på

www.teknologiradet.no

Overvåkningsnivå og autonomi

Det gode liv tar for de aller fleste utgangspunkt i en viss autonomi. Folk må ha et frihetsrom hvor de kan ta beslutninger om egen livsførsel uten å bekymre seg over innsyn fra omverdenen. Dessuten må det samlede overvåkningsnivå i samfunnet ikke bli så høyt at man tar bort behovet for et tillitsforhold mellom borgerne og samfunnet. Samtidig må samfunnet kunne beskytte seg mot terror og annen alvorlig kriminalitet.

Anbefalinger

Lovgiver bør drøfte følgende spørsmål knyttet til personvernens side av ekomloven:

- Skal det innføres obligatorisk logging av trafikkdata med lagringstid på ett år?
- Skal kommunikasjons-tjenester med sterk teknisk anonymitet forbys?
- Bør brukerne få bedre innsyn i hvordan lagrede kommunikasjonsdata anvendes?

Deltakere i Teknologirådets ekspertgruppe på området IKT og personvern er: Ann-Kristin Olsen, Fylkesmann i Vest-Agder; Lee A. Bygrave, Universitetet i Oslo; Andreas Wiese, Dagbladet; Einar Johan Aas, NTNU; Tian Sørhaug, Senter for Teknologi, Innovasjon og Kultur; Einar Snekkenes, Høgskolen i Gjøvik; Ben Johnsen, Universitetet i Tromsø; Inger Marie Sunde, Økokrim og Erlend Jakobsen, Teknologirådet

Teknologirådet er et uavhengig, rådgivende organ for teknologivurdering. Det ble opprettet ved kgl. res. 30. april 1999, etter initiativ fra Stortinget. "Fra rådet til tinget" utgis av Teknologirådets sekretariat

Pb. 522 Sentrum
0105 Oslo

Prinsensgate 18
Norway

T: +47 23 31 83 00
F: +47 23 31 83 01

www.teknologiradet.no
post@teknologiradet.no