Nordisk Tidsskrift for Kriminalvidenskab 2000

IKT-KRIMINALITET: ETTERFORSKINGSMETODER OG PERSONVERN

AV FØRSTESTATSADVOKAT INGER MARIE SUNDE

Modern computer crime ("high tech crime") is usually related to the use of electronic communications, such as Internet and cell phone networks. Exponential growth in the use of these networks has increased society's vulnerability for serious crime. Information concerning subscriber identity and traffic data is essential to law enforcement in such electronic environments. Experience has shown that these data should be registered and kept with the providers of telecommunication networks and services, for at least one year after the use of the service. The information should be released to the police upon request in connection with the investigation of crime. Effective international police cooperation is an essential requirement for the ability to solve these cases. National and international legal measures should provide for solutions that enable the police to collect such data and exchange them with appropriate law enforcement agencies internationally.

*This essay highlights the variety of new issues confronting the police in connection with computer crime investigation, and discusses issues surrounding access to information in relation to the EU Telecommunications Directive, Article 8 of the Human Rights Convention, and the recently-drafted Cyber-crime Convention of the Council of Europe, as well as Norwegian law.**

I. Problemstilling og faktisk bakgrunn

1. IKT inngår i all type kriminalitet

Med "IKT-kriminalitet" menes kriminalitetsformer som er relatert til bruk av informasjons- og kommunikasjonsteknologi. Begrepet dekker nye kriminalitetsformer som datainnbrudd og skadeverk via kommunikasjonsnett. Det dekker også all type kriminalitet hvor man tar beslag i elektroniske bevis. Eksempelvis faller narkotikasaker hvor det tas beslag i siktedes e-post og saker om spredning av barnepornografi via internett, i den siste kategorien.

2. Problemstillingen

Bruk av IKT har stor betydning for kriminalitetsutviklingen og er noe politiet må forholde seg til i alle typer straffesaker. Dette innebærer store utfordringer,

[1]* Title in English: *Computer Crime: Methods of Investigation and Personal Privacy.*

ved at nyttiggjøring av elektroniske bevis krever kompetanse og teknisk utstyr som politiet ofte ikke har. Speilbildet av denne situasjonen er imidlertid at elektroniske tjenester kan legge igjen mange spor. Politiets ambisjon er å klare å utnytte disse sporene for å oppklare sakene. Tilgangen på elektroniske bevis avhenger ikke bare av kompetanse og utstyrsmessige forhold, men i høy grad av regelverket knyttet til elektroniske tjenester, da særlig tele- og personvernlovgivningen. Retten til privat og fortrolig kommunikasjon inngår som en sentral interesse i personvernet. På den annen side står politiets ønske om å kunne spore en kommunikasjon (informasjonsoverføring) tilbake til en bestemt person, i forbindelse med etterforsking[1]. Den teknologiske utvikling har gitt et vell av kommunikasjonstjenester som man ikke tenkte seg for bare få år siden. Det har medført at deler av regelverket har kommet på etterskudd.

Brytningen mellom politiets behov og personvernregler i forbindelse med bekjempelse av IKT-kriminalitet er tatt opp på høyeste nivå på den internasjonale politiske arena, i G8, EU, FN og OECD. I tillegg er Europarådet i ferd med å sluttføre teksten til en *Cyber-crime Convention,* hvor man foruten medlemsstatene også tilbyr og forventer tilslutning fra IKT-dominerende stater som USA og Japan. På samme tid har EU vedtatt to direktiver, Personverndirektivet[2] og Telekommunikasjonsdirektivet[3]. Direktivene regulerer behandlingen av personopplysninger, Telekommunikasjonsdirektivet spesifikt i forbindelse med bruk av elektroniske kommunikasjonstjenester (direktivet blir også kalt ISDN-direktivet).

Erfaring viser at dersom politiet skal ha mulighet til oppspore gjerningspersoner som har benyttet elektroniske kommunikasjonsnett i forbindelse med handlingen, må det foreligge logger over bruken av tjenestene og abonnementsdata som identifiserer kundene. Følgende krav må være oppfylt:

- Det må ikke være adgang til å tilby anonyme kommunikasjonstjenester slik at brukeren er uidentifiserbar for politiet.
- Det må foreligge logger som sporer bruken tilbake til abonnent.
- Loggene og abonnementsdataene må oppbevares i minst ett år etter at bruken skjedde.
- Oppbevaringen må forlenges i enkelttilfelle på politiets anmodning i forbindelse med etterforsking.
- Opplysningene må utleveres direkte til politiet i forbindelse med etterforsking.

Dessuten må man sørge for at regelverket stiller like krav til alle tilbydere av elektronisk kommunikasjon via offentlig nett, uavhengig av hvilken type teknologi som er brukt.

3. Generelle utviklingstrekk
De teknologiske utviklingstrekk som i særlig grad preger kriminalitetsutviklingen kan beskrives som følger:

- Feltet *elektronisk kommunikasjon* er i rivende utvikling. All kommunikasjon via nett digitaliseres. De forskjellige kommunikasjonsnettene kan i økende grad utnyttes i kombinasjon (konvergens). Telefoni i kombinasjon med internett er et eksempel på dette. Nettene blir multimediabærende, dvs at de kan formidle tekst, lyd og bilde.
- *Mobilitet*. De elektroniske kommunikasjonsnettene vil være tilgjengelige fra ethvert sted til enhver tid. Eksempelvis kan de samme elektroniske banktjenestene utnyttes fra Norge og Jamaica, bare man har tilgang til en Internett-terminal, f eks på en Internett-café. Mobiliteten forsterkes ved utviklingen av håndholdte terminaler. Disse vil bli mer intelligente, dvs få flere funksjoner og større kapasitet enn i dag. De vil med andre ord langt på vei erstatte den stasjonære kontorPCen. Såkalte "lap toper" er kjente eksempler på slike terminaler som kan gi Internett-tilgang sammen med en mobiltelefon, mens "WAPer"[4] og "PDAer[5]" bare er i sin spede barndom teknologisk sett. Dette er en type avanserte mobiltelefoner, som kan ha personlige støttefunksjoner, tradisjonelle PC-egenskaper og Internett-tilgang.
- *Overføringskapasiteten* vil øke enormt. Det blir enklere å overføre store mengder informasjon på kort tid. Det gir et stort potensiale for spredning av filmer og musikk via Internett. Det betyr også at man lettere kan skaffe seg store mengder stjålen informasjon i forbindelse med et datainnbrudd.
- Det vil bli en selvfølge *å kryptere* informasjon som kommuniseres og lagres. Det forringer politiets mulighet til å nyttiggjøre seg beslag i elektronisk informasjon, dvs få forståelige bevis fra et kryptert innhold. Avlytting som etterforskingsmetode vil ofte ikke være hensiktsmessig, fordi den digitalt avleste krypterte informasjon er uforståelig og i praksis ukrypterbar.

Utviklingstrekkene har medført at trusselbildet for IKT-kriminalitet har blitt bredere. Tidligere fokuserte man mest på den interne trussel, dvs den utro medarbeider som misbrukte dataanlegget. Nå må den eksterne trussel legges til. Grunnen er koblingen i nettverk. Elektronisk kommunikasjon kan skje på et hvilket som helst tidspunkt overfor hvem som helst som er tilknyttet kommunikasjonsnettet. Etterhvert som antallet brukere øker og nettene konvergerer, blir man sårbar for stadig flere. Men få unntak er samtlige anmeldte tilfeller av datainnbrudd i Norge siden 1997 begått av eksterne gjerningspersoner, dvs at utenforstående har begått angrepet via Internett. Dette er en situasjon som nær sagt ikke ble vurdert i forbindelse med revisjonen av datainnbruddsbestemmelsen i

straffeloven § 145 annet ledd, i 1987. Da fokuserte man på angrep mot "stand alone" datamaskiner og lagringsmedier. Grunnen er selvsagt at den almenne bruk av Internett først begynte å utvikle seg i 1993, da web-grensesnittet ble introdusert. Siden den gang har utviklingen økt i eksponensiell takt. Bruken av Internett og mobiliteten kan antakelig sies å ha revolusjonert hele den elektroniske kommunikasjonsverden.

4. Sporing av gjerningspersoner på Internett

De fleste nye IKT-straffesaker gjelder bruk av Internett. Politiet har derfor på kort tid opparbeidet erfaring med sporing av gjerningspersoner som har benyttet dette mediet. Slik sporing er avhengig av tilgang på abonnent- og trafikkdata fra tele- og tjenestetilbyderne ("tilbyderne"). Selv om den følgende beskrivelsen tar utgangspunkt i Internett, er den gyldig for all sporing som gjelder bruk av elektroniske tjenester og telenett. Ved sporing på Internett er IP-adressen et sentralt identifikasjonsparameter. I andre nett kan man være avhengig av andre parametre. Det har sammenheng med hvilket teknisk "språk" (protokoll) som brukes over det aktuelle nettet. Beskrivelsen av sporing på Internett er derfor en *illustrasjon* av etterforskingssituasjonen knyttet til et kommunikasjonsnett.

4.1. Elektroniske spor - IP-adresser – Tilbydernes rolle

Man antar at flere hundre millioner datamaskiner verden over er tilknyttet Internett. For å styre kommunikasjonen har hver datamaskin (server) som er pålogget en unik IP-adresse. Alle elektroniske impulser (datapakker) som overføres i forbindelse med kommunikasjonen adresseres med IP-adresse, slik at de styres til korrekt server. IP-adressen sørger f eks for at e-post kommer frem til riktig adressat, eller at man finner ønsket web-side i forbindelse med informasjonssøk på nettet[6].

IP-adressene skrives som nummerserier i fire sekvenser med inntil tre sifre i hver sekvens, f eks 194.19.127.64. IP-adressene generes av en algoritme. Antallet er begrenset til 2^{32}, dvs noe mer enn 4 milliarder IP-adresser[7]. Tilbydere av Internett-tilgang[8] må skaffe seg en viss nummermengde som de kan leie ut til sine abonnenter eller brukere. Tilbyderne har ofte flere kunder enn IP-adresser[9]. Derfor deler de nummermengden på såkalte faste og dynamiske adresser. Brukere som har stort eller døgnkontinuerlig behov for Internett-tilknytning, f eks bedrifter, vil gjerne ha fast linje. Det vil si at de disponerer den samme IP-adressen gjennom abonnementsforholdet[10]. Fast linje prises meget høyere enn oppringt linje til Internett. Brukere med et begrenset Internett-behov vil derfor abonnere på oppringt linje. Ved hver pålogging til Internett vil brukeren bli tildelt en ledig IP-adresse. Brukeren disponerer IP-adressen inntil han logger seg av. Da blir IP-adressen ledig for en annen bruker hos samme tilbyder. Internettkontakten skjer via brukerens telefonlinje[11].

Dersom tilbyderne logger bruken av sine tjenester, herunder hvilke brukere

som til enhver tid disponerer IP-adressene, vil de på basis av en gitt dato/tidspunkt kunne finne ut hvilken brukerkonto[12] som disponerte IP-adressen, og hvilket telefonnummer oppkoblingen ble gjort fra.

På Internett finnes databaser som gir oversikt over hvem som disponerer de enkelte IP-adressene (whois)[13]. Databasene kan sammenlignes med telefonkataloger. Fastlinje-abonnentene er oppgitt i databasene. Brukere med oppringt linje er imidlertid ikke registrert, siden de ikke disponerer en bestemt adresse. I disse tilfellene vil databasene bare inneholde henvisning til den tilbyder av Internett-tilgang som er tildelt den nummerblokken som IP-adressen tilhører. Ønsker man å finne ut hvilken bruker som disponerte IP-adressen på et gitt tidspunkt, må man henvende seg til den aktuelle tilbyder som kan ha opplysningen i sine logger sammenholdt med kunderegisteret.

4.2. Etterforskingssituasjonen

Saker om Internett-kriminalitet åpnes normalt på bakgrunn av en anmeldelse, f eks om et datainnbrudd, et databedrageri eller tips/anmeldelse fra en interesseorganisasjon vedrørende spredning av barnepornografi. Utgangspunktet er at det foreligger mistanke om en straffbar handling. Politiets fremste oppgave er å finne gjerningsmannen, dvs den person som har begått datainnbruddet / databedrageriet eller tilbudt/besittet/sendt de barnepornografiske bildene.

På basis av loggdata fra datamaskinen til offeret, vil politiet normalt kunne finne IP-adressen til den maskin som tilsynelatende har vært benyttet til den straffbare handling. Her reiser det seg flere problemer:

4.2.1. Gjerningspersonen har brukt oppringt linje:

Politiet er avhengig av at tilbyderen faktisk har logget bruken av IP-adressene og oppbevart logginformasjonen. I tillegg må tilbyderen gi informasjonen til politiet.

Logging: De gamle telebedriftene hadde tradisjon for logging av sine tjenester, blant annet av hensyn til sikkerhet, forskning og statistikk. Tilbydere med utspring i slike televerk har derfor ofte logger. Flere nye tilbydere har imidlertid gjort seg til talsmenn for en rett til anonym Internett-bruk og tilbyr Internett-tilgang uten logging av bruken. Disse tilbyderne vil ikke kunne fremskaffe de opplysningene som politiet trenger selv om de skulle få rettslig pålegg om det, simpelthen fordi de ikke registrerer opplysningene i det hele tatt[14]. Atter andre unnlater å logge fordi det innebærer en kostnadsfaktor som de ønsker å eliminere. I disse tilfellene har mangelen på logger en økonomisk og ikke en ideologisk begrunnelse.

Oppbevaring og sletting av data: Selv om tilbyderen logger bruken av tjenestene er det ikke gitt at han har opplysningene på det tidspunkt som politiet ber om

dem. Det kommer an på rutinen for oppbevaring og sletting av loggene. Praksis varierer sterkt, fra noen dager til flere år.

Utlevering av opplysninger til politiet: Hensynene til å oppnå en målrettet etterforsking på et tidlig stadium, unngå fare for bevisforspillelse og tilrettelegge for internasjonalt politisamarbeide, tilsier at politiet bør få de nødvendige opplysninger direkte fra tjenestetilbyderen, uten å måtte innhente rettslig utleveringspålegg. Denne ordningen har vi i Norge. Utgangspunktet er at opplysningene er undergitt taushetsplikt, jf teleloven § 9-3 første ledd[15]. Det er imidlertid gjort unntak for anmodninger fra politiet, påtalemyndigheten og retten, jf § 9-3 tredje og fjerde ledd. Politiet får derfor opplysningene direkte fra tilbyderen.

Kvaliteten på opplysningene: Siste problemstilling relaterer seg til *kvaliteten* på opplysningene. Via loggene kan IP-adressen på et gitt tidspunkt kobles med en brukerkonto og et telefonnummer. Ved etablering av Internett-abonnementet må kunden normalt oppgi navn, adresse og telefonnummer. Dette er abonnementsdata som lagres i kunderegisteret til tilbyderen. Informasjon knyttet til brukerkontoen er imidlertid svært upålitelig av flere grunner:

- De oppgitte kundedata er ofte falske, dvs at brukeren har oppgitt en annens eller et fiktivt navn ved etablering av kontoen. Svake eller ikke eksisterende kontrollrutiner hos tilbyderne gjør at slike opplysninger ofte godtas selv om de er åpenbart falske[16].
- Selv om de registrerte data er ekte, vet man ikke hvem som har disponert kontoen i et gitt tilfelle. Kunnskap om brukerkontoen er et utgangspunkt for etterforskingen, men man må være åpen for muligheten for at en annen enn registrert innehaver har benyttet kontoen. Dette kan skje fordi svært mange brukerkonti er hacket. Distribusjon av passord skjer i stor skala på Internett. Dessuten kan en konto brukes av flere husstandsmedlemmer, f eks bruker barna en konto registrert i farens navn.
- Som nevnt kan IP-adressen knyttes til det telefonnummer som ble benyttet ved oppringningen til Internett. Dette gir et sikrere utgangspunkt for etterforskingen. Via telefonnummeret får man rede på lokaliseringen av datamaskinen som ble benyttet. Dermed avdekker man ransakingssted/-objekt, og har et utgangspunkt for videre etterforsking. Her er bruken av mobiltelefoner med anonyme kontantkort et problem. Dersom Internett-oppkoblingen er gjort via en slik telefon har ikke leverandøren av mobiltelefonitjenesten opplysninger om identiteten til abonnenten, og det blir i praksis umulig å spore innehaveren av telefonnummeret[17].

1.1.2. Gjerningspersonen har brukt fast linje:
Kriminelle på Internett abonnerer ikke på fast linje. Grunnen er selvsagt at de enkelt kan oppspores via IP-adressen og who-is. Imidlertid kan gjerningspersonen gjøre bruk av offentlige/publike Internett-tjenester med fast linje, f eks Internett-caféer og biblioteker. Dersom et dataangrep er gjort fra et bibliotek vil IP-adressen bare identifisere datamaskinen på dette biblioteket. Deretter er det opp til tradisjonell etterforsking, f eks vitneavhør, å avdekke hvem som benyttet maskinen på det aktuelle tidspunktet. Dersom datamaskinen ble misbrukt i en travel del av åpningstiden, sier det seg selv at muligheten for å finne gjerningspersonen kan være minimal.

1.3. Tåkelegging av Internett-bruk
Internett-kriminelle kan relativt enkelt skjule identiteten til den datamaskin som brukes til den straffbare handling. Dermed kamuflerer de også seg selv. Bruk av metoder for tåkelegging er vanlig. Hensikten er å skape inntrykk av at den ulovlige handlingen skjer fra en annen datamaskin enn den reelle originator. Dette gjøres for eksempel ved at man stjeler eller låner andre datamaskiners identitet og bruker dem som mellomstasjoner overfor den som er målet for handlingen. Tåkeleggingsoperasjoner gjøres ofte ved å (mis)bruke servere i forskjellige land, noe som vanskeliggjør etterforskingen ytterligere. Bruk av slike metoder kan selvsagt skje uavhengig av om brukeren/gjerningspersonen har fast eller oppringt linje.

II. Rettslige betraktninger

1. Telekommunikasjonsdirektivet
Det har vært hevdet at EU-direktivene begrenser medlemsstatenes adgang til å pålegge offentlige tilbydere å logge bruken av tjenestene og oppbevare dataene, samt at det stilles ubetingede krav til å anonymisere bruken av tjenestene og identiteten til brukerne.

Telekommunikasjonsdirektivet oppstiller konkrete regler på området. Direktivet artikkel 5 nr 1 lyder:

> *"Medlemsstatene skal ved hjelp av nasjonale regler sikre fortrolighet for telekommunikasjon som foregår via et offentlig telenett eller offentlig tilgjengelige teletjenester. De skal særlig forby enhver annen person enn brukerne, uten samtykke fra vedkommende bruker, å avlytte, oppfange, lagre eller på andre måter bryte inn i eller overvåke telekommunikasjon, unntatt dersom denne virksomheten er tillatt i henhold til lov, i samsvar med artikkel 14 nr 1".*

Fortrolighetskravet antas å innebære krav om at kommunikasjonens innhold er fortrolig og at brukernes identitet holdes fortrolig. Konfidensialitet om identite-

ten innebærer nødvendigvis også konfidensialitet om hvilket abonnement som har vært benyttet ved en oppkobling.

Artikkel 6 nr 1 og 2 lyder:

> *Nr 1 "Trafikkopplysninger om abonnentene og brukerne som behandles for å opprette samtaler, og som lagres av leverandøren av et offentlig telenett og/eller yteren av en offentlig tilgjengelig teletjeneste, skal slettes eller gjøres anonyme så snart samtalen er avsluttet, med forbehold for bestemmelsene i nr 2, 3 og 4."*
>
> *Nr 2 "Opplysninger nevnt i vedlegget kan behandles med henblikk på utarbeiding av abonnentregninger og betaling for samtrafikk. En slik behandling er tillatt bare inntil utløpet av tidsrommet da regningen kan bestrides i medhold av lov eller betalingsinnkreving kan foretas".*

Bestemmelsen tillater registrering og lagring av trafikkdata i den grad det er nødvendig for å utarbeide abonnentregninger og betale for samtrafikk. Hvilke trafikkdata det er tale om er omhandlet i et vedlegg til direktivet. Dessuten kan opplysningene registreres og lagres for visse andre formål som har med drift og sikkerhet ved tjenesten å gjøre, jf henvisningen til punktene 3 og 4. Dataene skal imidlertid slettes eller gjøres anonyme så snart de ikke er nødvendige for de nevnte formål, jf punkt 1.

Kravet om at logging skal skje av hensyn til fakturering, innebærer at det ikke kan skje logging dersom kunden faktureres i henhold til en fast avgift – abonnementsavgift - og ikke etter bruk. Dette er en stadig vanligere betalingsbetingelse. Det samme gjelder dersom kunden forskuddsbetaler for bruken ved kjøp av kontantkort, noe som er vanlig ved mobiltelefoni.

Artikkel 5 og 6 setter dermed altfor snevre begrensinger på registrering av identitet, logging og oppbevaring, i forhold til politiets behov.

Det ser imidlertid ut til at politiets behov for opplysninger kan imøtekommes til tross for disse reglene. Det følger for det første av at Telekommunikasjonsdirektivet ikke regulerer *"statens virksomhet på det strafferettslige området"*, jf artikkel 1 nr 3[18]. Dessuten inneholder artikkel 14 nr 1 en viktig bestemmelse. Bestemmelsen lyder:

> *"Medlemsstatene kan treffe lovgivningstiltak for å begrense rekkevidden av de forpliktelser og rettigheter som er fastsatt i artikkel 5 og 6...,dersom en slik begrensning er nødvendig for statens sikkerhet, forsvar, offentlig sikkerhet, forebygging, etterforsking, avsløring og rettslig forfølging av straffbare handlinger*[19] *eller uautorisert bruk av telekommunikasjonssystemet, som fastsatt i artikkel 13 nr 1 i direktiv 95/46/EF [Personverndirektivet]"*[20]

Telekommunikasjonsdirektivet legger dermed opp til et flersporet system, hvor det på den ene siden legges strenge begrensninger på tilbydernes adgang til å registrere og oppbevare opplysninger, mens det på den annen side åpnes for at opplysningene skal kunne tilgjengeliggjøres for politiet. Hvordan et slikt system rent praktisk skal organiseres gir direktivet ikke anvisning på.

Artikkel 14 nr 1 stiller imidlertid krav om at begrensninger i rekkevidden av de forpliktelser og rettigheter som artikkelen etablerer, må gjøres ved *"lovgivningstiltak"* og begrensningene må være *"nødvendig ...for avsløring og rettslig forfølgning av straffbare handlinger"*.

Lovgivningsteknikken er parallell til EMK artikkel 8 nr 2, som gjelder inngrep i privatlivets fred og korrespondansefortroligheten. Direktivet tar forøvrig uttrykkelig hensyn til EMK, med en referanse til konvensjonen i fortalen punkt 2. Siden EMKs regler gjelder i medlemsstatene uavhengig av hva som står i Telekommunikasjonsdirektivet, kan man kanskje tolke henvisningen i fortalen og utformingen av artikkel 14, slik at ethvert inngrep i Telekommunikasjonsdirektivets regler forutsettes å reise spørsmål i forhold til EMK[21].

2. EMK artikkel 8

2.1 Utgangspunktet

EMK artikkel 8 lyder:

> *Nr 1 "Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse".*
>
> *Nr 2 "Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter".*

Registrering av identiteten til abonnenter, logging og oppbevaring av opplysninger om bruken av tjenestene må antas å være inngrep i respekten for privatliv og korrespondanse. Spørsmålet er om inngrepet kan rettferdiggjøres i henhold til vilkårene i annet ledd. I så tilfelle må tre krav være tilfredsstilt, dvs at inngrepet må være nødvendig i et demokratisk samfunn, at inngrepet skjer med hjemmel i lov og at det skjer for de formål som er spesifisert i annet ledd.

På bakgrunn av erfaringene beskrevet i punkt I.4, kan det ikke være tvilsomt at første og siste vilkår, nemlig at inngrepet er nødvendig for å forebygge kriminalitet, er oppfylt. Det er helt på det rene at politiet er avhengig av tilgang til abonnements- og loggdata for å ha rimelig oppklaringsmulighet ved etterforsking av IKT-kriminalitet. Under norske forhold er det bare spørsmål om lovskravet er oppfylt.

2.2. Plikt til å registrere abonnentforholdet?

Første spørsmål gjelder opplysning om abonnentens identitet. Teleloven § 3-4 første ledd (d), gir Telemyndigheten kompetanse til å fastsette krav til *"kunderegister og nummeropplysning"*. Krav kan fastsettes i form av forskrift, vilkår i konsesjon eller pålegg til tilbyderne. En relevant bestemmelse finnes i hvert fall

i teleforskriften[22] § 2-7, som pålegger tilbyderen *"å føre oversikt over sine abonnenters navn, adresse og tilordnet telefonnummer"*. Denne bestemmelse sammenholdt med teleloven § 3-4 første ledd (d), ser ut til å kunne hjemle et krav om at tilbyderne skal ha oversikt over kundenes identitet. Det er da et tankekors at salg av anonyme kontantkort og tilbud om anonym Internett-tilgang kan foregå, idet tjenestene ser ut til å være i strid med den uttrykkelige bestemmelsen i teleforskriften[23].

2.3. Plikt til registrering og oppbevaring av trafikkdata?
Neste spørsmål er om det gjelder noe lovhjemlet krav om logging og oppbevaring av opplysninger om bruk av tjenestene. Teleloven § 3-4 første ledd (i), gir Telemyndigheten kompetanse til å stille krav til *"lagring og utlevering av opplysninger"*. Denne bestemmelsen ses ikke å være fulgt opp i teleforskriften, og så vidt vites har Telemyndigheten ikke benyttet seg av muligheten til å gi pålegg om slik logging og oppbevaring. I så fall gjelder det ingen generell plikt for tilbyderne til å logge og oppbevare opplysninger om bruken av tjenestene. Siden EMK henviser til et materielt lovkrav, er det neppe nødvendig med lovendring for å imøtekomme legalitetskravet i EMK artikkel 8 annet ledd. Slik plikt til logging og utlevering bør derfor kunne pålegges av Telemyndigheten.

2.4. Utlevering av opplysninger og internasjonalt politisamarbeide
Innen bekjempelse av IKT-kriminalitet er internasjonalt politisamarbeide svært viktig. Som nevnt brukes ofte tåkeleggingsteknikker, som involverer datamaskiner i flere land. Det er viktig at politiet raskt kan eliminere de mellomliggende datamaskinene og finne den som ble brukt av gjerningspersonen. Dette krever at abonnements- og logginformasjon kan utveksles på politinivå internasjonalt. Da må nasjonal lovgivning sørge for at opplysningene unntas fra taushetsplikt overfor politiet. I så måte kunne teleloven § 9-3 tredje, jf fjerde ledd, tjene som en mønsterbestemmelse for andre land[24], og for Eurparådets *Cyber-crime Convention*. Dessverre har ikke Europarådets ekspertgruppe foreslått en slik bestemmelse, etter offentlig kjente utkast å dømme. I stedet legges det stor vekt på "24x7 points of contact" på politinivå og direkte kommunikasjon mellom påtalemyndigheten i medlemslandene. Problemet er likevel at når opplysningene er taushetsbelagte for politiet er det normalt nødvendig med rettslig pålegg for å få tilgang til dem, noe som forsinker prosessen. Systemet med rettsanmodninger er helt foreldet i forhold til de krav som bekjempelse av IKT-kriminalitet stiller. Det kan ta ett halvt år å få informasjon utenom de nordiske land på denne måten. I mellomtiden forsvinner de elektroniske bevis.

Det er vanskelig å se formålet med domstolskontroll med utlevering av disse opplysningene til politiet. Dommeren må treffe sin beslutning på bakgrunn av en opplysning om at politiet etterforsker en straffbar handling og mottar for øvrig noen tekniske logger som bare datakyndige kan vurdere. Dommeren har

ingen mulighet til å kontrollere om loggene er korrekte, og noe annet vurderingstema foreligger ikke for ham å ta stilling til. Den hensiktsmessige løsning er dermed at opplysningene utleveres direkte fra tilbyderen. Tilbyderen må selvsagt ha rett til å reservere seg mot å gi ut data dersom loggene er upålitelige. Slik reservasjonsadgang følger av Teleloven § 9-3 fjerde ledd.

Politiet har i realiteten ingen mulighet til å oppklare godt planlagt IKT-kriminalitet utført via flere land uten helt andre og effektive prosedyrer for informasjonsutveksling. Utveksling av abonnements- og loggdata på politinivå bør derfor settes øverst på den internasjonale politiske agenda innen bekjempelse av IKT-kriminalitet. Spørgsmålet burde vært klart adressert i *Cyber-crime Convention.*

3. Telemyndigheten må bruke sin kompetanse

Innen Norge er ikke problemet for politiet å få opplysningene dersom de er logget, men å sikre seg at det faktisk foreligger opplysninger hos tilbyderen når man fremsetter forespørselen. Da må tilbyderen følge opp plikten til å registrere kundeforhold og bruk. Det er viktig at Telemyndigheten benytter sin kompetanse til å pålegge tilbyderne plikt til å registrere disse opplysningene, jf punkt II.2.3. Dette burde være aktuelt nå i forbindelse med behandlingen av UMTS-konsesjonen som behandles i høst. Uten et generelt pålegg vil praksis variere sterkt hos tilbyderne, noe som er svært utilfredsstillende for politiet. Da vil det vesentlige regelverket bli satt av Datatilsynet gjennom personregisterkonsesjoner. Datatilsynet har sendt forslag til nye standardkonsesjoner på høring. Høringsutkastet er en ren implementering av Telekommunikasjonsdirektivets bestemmelser, *uten* unntak for politiets behov. I tillegg har Datatilsynet foreslått en absolutt frist for sletting av opplysninger på tre måneder fra det tidspunkt bruken skjedde. Dette er alt for stramt sett fra politiets side.

4. Organisering av opplysningene

Telekommunikasjonsdirektivets åpning for et flersporet system for registrering, oppbevaring og bruk av data, skaper visse problemer rundt behandlingen av dataene. Når dataene på den ene siden skal slettes eller anonymiseres og på den annen side kunne være tilgjengelige for politiet, kan en mulig løsning være å etablere to faser for håndteringen av dem: I første fase registreres og oppbevares dataene hos tilbyderne. Når anonymiserings-/slettingstidspunktet er kommet, jf Telekommunikasjonsdirektivet, kan dataene i neste fase overføres til en institusjon som forvalter dataene til de formål som direktivet ikke dekker. I Norge kan man tenke seg at slik "andre fase behandling" ble en oppgave for Senter for Informasjonssikring (SIS), som er foreslått etablert av Sårbarhetsutvalget i innstillingen *Et sårbart samfunn* NOU 2000:4, s 70. En slik funksjon ville være forenlig med de øvrige oppgaver SIS er tiltenkt innen håndtering av sensitive rapporter om insidenter, dvs dataangrep via kommunikasjonsnett. SIS skal ha en

svært høy grad av sikkerhet og kan ivareta konfidensialiteten til de lagrede opplysninger.

5. Telelovens rekkevidde

På grunn av det store antall nye IKT-tjenester er det behov for en vurdering av om telelovgivningens regler om registrering og logging favner tilstrekkelig vidt. Loven omfatter all telekommunikasjonsvirksomhet, jf § 1-1. Telekommunikasjon er overføring av lyd, tekst, bilde eller andre data ved hjelp av lys, radiosignaler eller andre elektromagnetiske signaler i et kommunikasjonssystem for signalbefordring, jf § 1-6 (a). Kommunikasjonsnettet er telenettet. Tilbyderne av offentlig telenett er dermed omfattet av loven. I tillegg har vi en stor gruppe som kalles tjenestetilbyderne. Det er innen denne gruppen den store økningen i tjenestetilbudet har skjedd. I forbindelse med innhenting av opplysninger om bruk av IKT-tjenester har ØKOKRIM erfart at det hersker betydelig forvirring innen bransjen selv, om hvorvidt de er undergitt teleloven eller ei. Dette er avgjørende for om utleveringsprosedyren i teleloven § 9-3 tredje jf fjerde ledd, skal kunne benyttes.

Teleloven § 1-6 (d) definerer *"teletjeneste"* som *"tilbud i næringsøyemed om formidling av telekommunikasjon helt eller delvis ved hjelp av overføring i telenett, som ikke er kringkasting"*.

Utviklingen i tjenestetilbudet innebærer at det finnes lag på lag med tjenester på nettene. Grensen mellom tjeneste- og innholdsleverandør er flytende og til dels visket ut. En type tjeneste er såkalt web-hotell, som er en datamaskin på Internett hvor kunden kan leie plass til en web-side. Kunden er dermed innholdsleverandør mens eieren av web-hotellet formodentlig er tjenestetilbyder (tjenesten er kapasiteten på web-serveren). Men det kan hende at kunden oppretter en interaktiv web-tjeneste, f eks en auksjonstjeneste. Dermed er innholdsleverandøren også en tjenestetilbyder, for kunder som ønsker å selge eller kjøpe noe via auksjonstjenesten. Det som tilbys er informasjon som overføres via telenettet, dvs telekommunikasjon. Betyr det at en plikt til å registrere kunder og å logge skal kunne pålegges både tilbyderen av selve telenettet, tilbyderen av web-hotellet og tilbyderen av auksjonstjenesten, eller går ikke loven så langt? I så fall, hvor går grensen?

Et annet eksempel er innehaveren av en Internett-café. Han tilbyr tilgang til Internett via sine terminaler, og som nevnt i punkt 4.2.2, er en slik terminal velegnet for å skaffe seg anonymitet på Internett. For å være sporbar må cafégjesten la seg registrere, noe som ikke skjer i dag. I dette tilfellet er innehaverens Internett-tilbyder tjenestetilbyder, men også caféinnehaveren selv, siden han gjør sine tilgangsrettigheter alment tilgjengelige. Omfattes caféinnehaveren av teleloven, eller burde han det?

Dessuten inneholder definisjonen av *"teletjeneste"* et krav om at tjenesten skal skje *"i næringsøyemed"*. Det er spørsmål om hvor velbegrunnet dette vil-

kåret er. Universiteter, store bedrifter og offentlige institusjoner tilbyr et stort antall terminaler med Internett-tilgang uten at det skjer i næringsøyemed. Kommunikasjonen skjer over det offentlige telenettet. Det skaper sårbarhet og risiko for alle andre som er tilknyttet det samme nettet. Burde ikke disse også av de nevnte grunner være undergitt krav til registrering og logging av bruk? Og hva med Internett-tilbydere som yter Internett-tilgang på ren hobby basis? Hvorfor skal disse være unntatt fra teleloven, når tjenesten er avhengig av offentlige ressurser som IP-adresser og telenett?

Etter mitt syn burde den erkjennelse vi har fått vedrørende samfunnets sårbarhet for misbruk av IKT-tjenester, tilsi at alle som har tilgang til offentlige kommunikasjonsnett, bør være sporbare. Det bør ikke spille noen rolle om bruken skjer i næringsøyemed. Man kan tenke seg innføring av et e-pass som vilkår for tilgang, og som innebærer at identiteten blir registrert når offentlig telenett er involvert i bruken. Situasjonen kan på mange vis sammenlignes med bank- og finansnæringens problem med misbruk av tjenestene for å hvitvaske økonomisk utbytte fra kriminell virksomhet. Til tross for eldgammel tradisjon og lovhjemlet plikt til sekretesse, er hele næringen blitt pålagt identitetskontroll med sine kunder og kontroll med de enkelte transaksjoner for å hindre hvitvasking. Dette har skjedd globalt, også overfor stater som har basert sin nasjonale økonomi på banksekretessen. I tillegg er bransjen internasjonalt pålagt meldeplikt om mistenkelige transaksjoner til politiet, i Norge til ØKOKRIM, jf finansieringsvirksomhetsloven § 2-17[25]. Tilstanden er ikke mindre alvorlig ved bruk av IKT-tjenester og man kan langt på vei føre samme argumentasjon for å pålegge tele- og tjenestetilbyderne tilsvarende krav.

Jeg har kanskje stilt flere spørsmål enn jeg har gitt svar i denne artikkelen, men faktum er at IKT-kriminaliteten er i stor utvikling og det er viktig å få opp bevisstheten om problemene som det reiser. Artikkelen er derfor ment som en invitasjon til en viktig og nødvendig debatt.

Noter:

[1] Det er ikke nødvendigvis tale om en bastant konflikt mellom interessene. Graden av konflikt må bestemmes konkret og det viktig å unngå fastlåste oppfatninger. Det vises til bemerkningene om dette i NOU 1997:19 *"Et bedre personvern"*, s 26 og 27.

[2] Direktiv 95/46/EF

[3] Direktiv 97/66/EF

[4] Wireless Application Protocol.

[5] Personal Digital Assistant.

[6] IP-adressene brukes i alle Internett-tjenester, f eks e-post, news, web-surf, ftp, telnet, irc, icq. Dessuten brukes teknologien i forbindelse med forbrukerelektronikk som kommuniserer digitalt via telenettet, f eks mobiltelefoner med kobling mot Internett via wap-teknologi. Bruken av domenenavn, f eks okokrim.no, og hypertekst (lenketeknologi – pek og klikk) medfører at brukeren ikke nødvendigvis må memorisere IP-adressen. Like fullt skjer kommunikasjonen fra hans server på basis av "handshake" mellom IP-adressene.

[7] Det eksakte antallet er 4 294 967 296. Antallet virker høyt, men faktum er at nummerressursen er i ferd med å bli uttømt, noe som vil skape problemer for Internetts fremtid med mindre kapasite-

ten økes. Problemet forsøkes løst ved innføring av IPv6 (IP versjon 6). Nummerressursen administreres av flere non-profit Internett-organisasjoner med IANA (Internet Assigned Numbers Authority) og Internet Corporation for Assigned Names and Numbers (ICANN) på toppen. Se f eks www.icann.org. I Norge er UNINETT administrator.

[8] Eksempler på norske tjenestetilbydere er Nextra (Telenor), Tele2 og Telia Nettjenester.

[9] I 1998 hadde f eks hadde Telenor Nextel AS 60 000 IP-adresser og ca 200 000 kunder.

[10] Fast IP-adresse kan sammenlignes med et telefonnummer.

[11] Via modem eller ISDN-linje.

[12] Brukerkonto er betegnelsen på et Internett-abonnement.

[13] Med utgangspunkt i ICANNs web-side kan man finne frem til relevant whois-base.

[14] Enkelte tilbydere skal ha utviklet tjenester som gjør det *teknisk umulig* å koble IP-adresse og bruk. Følgen er at tjenesten som sådan må nedlegges dersom tilbyderen skulle bli pålagt plikt til å logge aktivitet.

[15] Teleloven er lov av 23. juni 1995 nr 39.

[16] Man registrerer seg f eks som Dolly Duck fra Andeby.

[17] Både mobiltelefon og kontantkort kan kjøpes uten å oppgi identitet. Tidligere benyttet kriminelle miljøer ofte såkalt klonede mobiltelefoner for å oppnå anonymitet. Bruk av klonet telefon belastet kontoen til en legal bruker, som uforskyldt fikk regningen for tellerskrittene, mens den reelle bruker ikke var sporbar. Bruk av klonede telefoner har tatt slutt med overgangen til GSM og fordi mobiltelefoner med kontantkort sikrer den ønskede anonymitet. I dag prøver politiet å avdekke identiteten til brukeren av slike mobiltelefoner ved å analysere trafikkdata. Post- og Teletilsynet mottar daglig 10-15 henvendelser fra politiet om tilgang til slike data, de fleste i narkotikasaker. Det hadde ikke vært nødvendig dersom kundeforholdet hadde vært registrert hos leverandøren av mobiltelefonitjenesten.

[18] Den samme avgrensning finnes i Personverndirektivet artikkel 3 nr 2.

[19] Min understrekning.

[20] Personverndirektivet artikkel 13 er en lignende bestemmelse. Unntaket for kriminalitetsbekjempelsen står i
artikkel 13 nr 1 d.

[21] EMK er direkte gjort til en del av norsk rett, jf menneskerettsloven av 21. mai 1999 nr 30.

[22] Forskrift fastsatt ved kgl res 5. desember 1997 nr 1259, med hjemmel i teleloven.

[23] Telekommunikasjonsdirektivets fortale punkt 18, inneholder en oppfordring om tilbud av betalingsmuligheter som gir "anonym" eller "strengt privat" tilgang til offentlig tilgjengelige teletjenester. Dette punktet kan imidlertid ikke innebære noen rettslig plikt for medlemsstatene til å sørge for tjenester som medfører at abonnentene blir uidentifiserbare for politiet, slik kontantkort og flere Internett-tilbud er i dag. Uansett gjelder det generelle unntaket for virksomhet på strafferettens område.

[24] Om fortolkningen, se Rt-1999-1944.

[25] Lov av 10. juni 1988 nr 40. § 2-17 ble tilføyd ved lov 7. juni 1996 nr 30.

Adresse: ØKOKRIM
Postboks 8193 Dep
N – 0034 Oslo