

## TELEKOMBRANSJENS ROLLE I MODERNE KRIMINALITETSUTVIKLING

Av førstestatsadvokat Inger Marie Sunde, ØKOKRIM

(Stoffet i artikkelen har vært benyttet i en kronikk i *Teknisk Ukeblad nr 5, 3. februar 2000*)

Det er ingen tvil om at utviklingen i tjenestetilbudet innen telekombransjen har medført store endringer i moderne kriminalitetsutvikling. Både internett og mobiltelefoni gir brukerne mulighet for teknisk anonymitet og er dermed attraktive tjenester for kriminelle miljøer. Bruk av mobiltelefon med kontantkort (og klonede mobiltelefoner) har lenge vært vanlig i narkotikamiljøer. Internett har dessuten den store fordel at tjenesten er så rimelig at man når hele verden på gratis abonnement og lokale tellskritt. Nasjonale grenser eksisterer ikke. I nyere kriminelle miljøer, så som "hackermiljøer", vil man for eksempel bruke internett til å begå dataangrep. En kommunikasjonskanal benyttes med andre ord som angrepskanal. I tillegg vil man formidle stjålne passord og kredittkortnumre og dermed øke sårbarheten for ofrene. Piratkulturen er stor på internett. Dette er en virksomhet som er ulovlig i de fleste land. I en ØKOKRIM-sak sommeren 1998 ble en snekker domfelt for å ha solgt 29 000 piratdekkert kort på 11/2 år. Både koder og kort var formidlet via internett. Saken sier noe om problemets størrelse bare i Norge.

Internett har også skapt et verdensomspennende marked for barnepornografi. Den enkle tilgjengeligheten medfører at pedofile bygger opp store private billedarkiv. Både i Norge og utlandet ser vi at samlingene er på titusener av bilder, ja helt opp til et par hundre tusen, alt sirlig klassifisert etter alder, kjønn og type overgrep. Nye bilder er mest populære. Forutsettes en normal sammenheng mellom etterspørsel og tilbud betyr det at internett bidrar til en vesentlig forøkning i seksuelle overgrep mot barn. KRIPOS har i sin trusselvurdering for 1999 opplyst at sexmisbruk av barn er blitt en industri i en rekke land. Internettspredning er større integritetskremløse for barn enn den papirbaserte spredningen. Papirkopier er forgjengelige og opplag tross alt begrensede. De digitale bildene vil være tilgjengelige for alltid siden det er umulig å slette dem hos alle besitterne. Offeret risikerer gjennom hele livet å finne misbruksbilder av seg selv på internett.

Telekombransjen inntar tilsynelatende en svært passiv holdning i forhold til sin viktige rolle i kriminalitetsutviklingen. Mens det er behov for en rekke tiltak toer bransjen sine hender og viser til yringsfriheten og transportørens begrensede ansvar for det innhold han frakter. Situasjonen minner om den som tidligere gjaldt finansnæringen. Bransjen ble i stor utstrekning misbrukt til hvitvasking av utbytte fra kriminelle handlinger, men distanserte seg fra ansvar på samme måte som telekombransjen gjør nå. Finansnæringen har imidlertid internasjonalt blitt pålagt et rapporteringsregime til politiet om mistenkelige transaksjoner, og utvidet plikt til å kontrollere og registrere identiteten til sine kunder ("hvitvaskingsreglene").

Telekombransjen er selvsagt livredd for et juridisk spredningsansvar. Men prinsippet om transportansvaret settes nå stadig oftere på prøve i barnepornografisaker ved domstolene verden over. Mer interessant er det kanskje å registrere bransjens tilsynelatende passivitet på det teknologiske plan. Det finnes tekniske filtre som kan blokkere kanaler med forbudte titler, f eks *dad&daughtersex, preteensexpics, bestiality.sex, rape&torture* osv. Dessverre benytter neppe alle internetttilbydere slike filtre. Et annet problem er at de tekniske løsninger er for dårlige, slik at blokkering forholdsvis lett unngås. Et velkjent knep er feilbokstaving, f eks *preeteensexpics* eller *bestialty*. Filteret vil dermed ikke blokkere gruppen. Et annet knep er å smugle ulovlige bilder inn på kanaler med "uskyldige" navn, f eks *asparraques* eller *cucumber*. For hindre omgåelse av filterne må internettleverandørene i tillegg sette av ressurser til manuell kontroll. Dette koster penger. Men er det forsvarlig å tilby stadig billigere internettaksess, for ikke å si gratis tjenester, dersom man ikke samtidig har økonomi til å foreta kontroll mot ulovlig innhold? Og hvilket ansvar tar store norske bransjeaktører for å løfte disse problemene internasjonalt?

Et annet viktig spørsmål gjelder kontroll med kundeidentitet og registrering og oppbevaring av loggdata. Politiet er ofte avhengig av slike opplysninger, og i internettetforskning er de avgjørende for å spore opp gjerningspersonene. Jeg tar ikke til orde for registrering av innholdet. Behovet gjelder registrering av *bruken* av tjenestene, av hvem, hvorfra og når. Her er dagens regelverk mangelfullt. Hvorfor gjelder det forskjellige regler for oppbevaring av loggdata for mobiltelefoni kontra fast telefon? For internettleverandørene ser det ut til å mangle regelverk overhodet. ØKOKRIM har nå tatt initiativ til å skaffe oversikt over dette brokete feltet hvor reglene så vidt forstås, ofte er hjemlet i Datatilsynets konsesjoner til de enkelte selskap.

Hensynet til personvernet blir bestandig ført med styrke mot krav om registrering. Man bør da merke seg at dagens regler og praksis er utviklet uten hensyntagen til politiets behov, kanskje

fordi telekombransjen tilhører samferdselssektoren, som er fokusert på andre spørsmål enn kriminalitetsbekjempelsen. Personvern hensynet må balanseres mot hensynene til en effektiv kriminalitetsbekjempelse og hensynet til ofrene for kriminelle handlinger. Fokuserer man ensidig på personvernet blir ofrenes interesser satt til side og de kriminelle går fri. Det har vært hevdet at politiets behov representerer en *sekundærbruk* som ikke kan begrunne et slikt inngrep i personvernet. Dette syn sto kanskje sterkere før. På FNs 10. konferanse innen kriminalitetsforebyggende arbeide i april, vil telekombransjens rolle i kriminalitetsutviklingen bli belyst, herunder behovet for registrering og utlevering av opplysninger. Videre har Høyesterett i en nylig avsagt kjennelse i en sak mellom Telenor Nextel AS og ØKOKRIM, ment at utlevering av slike opplysninger til politiet, verken er i strid med EMK artikkel 8 om privatlivets fred eller EUs personverndirektiv. Parallellen til "hvitvaskingsreglene" viser etter min mening at det ikke er tale om å overtre noen ny grense for personvernet. Kanskje er det klokt av bransjen å være føre var og sørge for nødvendige tiltak fremfor å vente til innskjerpede kontrollkrav fremtvinges av seg selv?