

## **"ON LINE CRIME" – BEVISFØRSEL OG STRAFFERAMME I DATAKRIMSAKER**

Av førstestatsadvokat Inger Marie Sunde, ØKOKRIM

(Artikkelen har vært publisert i *Rett & Slett nr 1, 2000, Justis- og Politidepartementet*)

ØKOKRIMs datakrimteam arbeider med flere interessante felt innen IKT-kriminalitet (IKT = informasjons- og kommunikasjonsteknologi). Bruken av internett har skapt et nytt kriminologisk uttrykk, nemlig "on-line crime". Typiske eksempler er spredning av barnepornografi og helerivirksomhet på internett, og dataangrep som begås via nettet. En ny alvorlig trussel er pedofile som bruker pratekanalene på internett til å komme i kontakt med barn og avtale møter med dem. I USA/Canada har ca 800 barn forsvunnet på denne måten. Sverige har allerede en sak hvor en voksen mann ble domfelt for seksuelle overgrep mot to småjenter han hadde fått kontakt med via internett.

"On-line crime" som fenomen har interesse uansett hvilken type straffesaker man arbeider med. Internett bidrar til å forsterke kjente trekk ved kriminalitetsutviklingen, både at den blir mer internasjonal og mer organisert. Via internett kan de kriminelle kommunisere anonymt og kryptert på lokale tellskritt verden over. På denne måten kan man enkelt organisere en narkotikaleveranse fra Colombia til Norge. Kommunikasjonen kan avlyttes teknisk sett, men er innholdet kryptert vil de avlyttede (kopierte) data være verdiløse for politiet. Som man ser stilles politiet overfor nye store utfordringer.

### **Dataangrep – ny kriminalitetsform – for lav strafferamme**

Dataangrep omfatter flere typer straffbare handlinger som alle har dataressursen (den datalagrede informasjon eller maskinkapasiteten/tjenestene) som objekt for handlingen. Med "dataangrep" forstås vanligvis datainnbrudd (strl § 145, 2), misbruk av dataressurser (strl §§ 261 og 393), skadeverk (strl § 291 m fl), herunder endring/sletting av data og avskjæring av kommunikasjonsadgang (denial of service), og til slutt, avlytting, både data og teletrafikk (strl § 145, 2 og § 145 a).

I Norge antas det at mer enn halvparten av husstandene og ca 80% av bedriftene har internettilgang. Norge har også et meget aktivt hackermiljø. Dette er selvsagt ikke bundet av nasjonale grenser, men inngår som en naturlig del i de internasjonale hackermiljøer på internett. Her utveksles programvare ("tools") som brukes til dataangrep og man samarbeider om angrep. F eks har vi saker hvor gjerningspersonen har delt dataskjermen i to, slik at han mottar råd og veiledning via pratekanal på den ene og utfører hacket på den andre. Dessuten utveksles passordlister og informasjon om interessante steder (servere) å angripe.

Næringslivet oppfatter dataangrep som et alvorlig problem. Bortsett fra faren for lekkasjer av bedriftssensitiv informasjon, medfører dataangrep at bedriften ikke kan stole på sitt datasystem. Det er vanlig at hackerne legger inn skjult programvare (trojanske hester) som stadig skaper ny sårbarhet hos offeret. Datasystemet må derfor reinnstalleres, noe som forårsaker driftsavbrudd og i verste fall går direkte ut over den økonomiske virksomheten. På toppen av det hele kommer regningen fra de innleide datakonsulentene som skal rette opp feilen. På denne bakgrunn må strafferammen på fengsel inntil 6 måneder for datainnbrudd anses å være altfor lav, noe som også synes å fremgå ved en sammenligning med innbrudsregelen i strl § 147, hvor den ordinære strafferammen er fengsel inntil ett år.

ØKOKRIM ser dataangrep som en del av problemkomplekset rundt angrep mot informasjonssikkerheten. Korrupsjon/økonomisk utroskap er tilgrensende kriminalitetsfelt. Videre er det klart at dataangrep kan forekomme i kombinasjon med vinningskriminalitet som databedrageri og informasjonsheleri (eks kjøp av kredittkortnumre stjålet ved innbrudd i databaser).

Samfunnets "IT-sårbarhet" vies betydelig oppmerksom om dagen. Dataangrep er en kjerneproblemstilling i dette, og politiet har bare sett toppen av isfjellet. Et tiltak mot "IT-sårbarhet", bortsett fra de krav som selvsagt må stilles til sikkerhetstiltak i næringslivet (og offentlig sektor), er å sørge for tilstrekkelig kompetanse (dataingeniører) og en hensiktsmessig organisering som setter politiet i stand til å etterforske og oppklare denne type overtredelser. Foreløpig er det bare ØKOKRIM som har gjort en skikkelig satsing på dette felt.

### **Analysen –"computer forensics" - bevisituasjonen**

Bruken av PC, datanettverk, personlige "organizere", mobiltelefon osv gir politiet et vell av interessante sporsteder. I ØKOKRIMs økonomisaker (og selvsagt i IKT-krimsakene) tas det obligatorisk databeslag. Datakrimteamet har en godt bistandstilbud til lokalt politi i forbindelse med sikring og analyse av databeslag. De senere årene har vi mottatt i overkant av 60 bistandssaker pr år. Tallet burde vært ti (kanskje hundre?) ganger høyere, men det er et faktum at politiet ofte lukker øynene for datautstyret på ransaking, fordi politistasjonen mangler et skikkelig opplegg for å håndtere et slikt beslag. Etter hvert er det en del polititjenestemenn som har kompetanse til å sikre beslag, dvs lage en speilkopi og påse at originalmediet forblir intakt. Imidlertid mangler det mye på analysekompetansen. ØKOKRIM har denne kompetansen og i ferd med å videreutvikle bistandskonseptet for å dekke dette behovet.

"Analyse" betyr prosessen forbundet med å finne den informasjonen i beslaget som kan brukes som bevis i straffesaken. Internasjonalt er dette feltet i ferd med å utvikle seg til en vitenskap under etiketten "computer forensics".

Ved omtale av analysen fokuseres det gjerne på problemene, nemlig om man kan finne bevis i skjult informasjon, f eks gjenskape slettede / skjulte filer, dekryptere, lese hvit skrift på hvit bakgrunn eller sort på sort ("ghosting") osv. Slike oppgaver krever selvsagt både erfaring og teknisk kompetanse. Det er vel så viktig å fokusere på mulighetene: Man har gjerne beslaglagt veldig mye informasjon som er åpent tilgjengelig og har dermed veldig mange bevismuligheter i beslaget. Problemet er hvordan man skal avgrense analysen. Her er vanlig etterforskererfaring og påtalemessig ledelse like viktig som den tekniske kompetansen, men man trenger alt sammen. Poenget er at man må ha en formening om hvilken informasjon som kan ha betydning som bevis i saken, slik at man kan planlegge hvilke søk man ønsker foretatt. Ønsker man f eks informasjon om kundekretsen til en narkotikalager så kan man kanskje velge bare å se på eposten. Dersom man etterforsker et giftmord vil navn på visse giftstoffer være viktige (slik man så i Thallium-saken nylig) og da lager man f eks en søkestreng med "Thallium" og ser bort fra resten av datainformasjonen. Systematisk gjennomgang av innholdet på gjerningspersonens PC kan også si mye om hans interesser og bygge opp en profil som har stor betydning ved troverdighetsvurderingen.

Dersom man i et tverrfaglig miljø planlegger denne tekniske etterforskningen har man best muligheter til å oppnå et godt resultat. Det er gledelig å registrere at enkelte politidistrikt har begynt å organisere seg med tanke på skape slike tverrfaglige miljøer. ØKOKRIM skal f eks være vertskap denne våren for en gruppe bestående av to etterforskere og en påtaleansvarlig. De skal hospitere for å lære metode for sikring, analyse og utarbeidelse av dokumentutdrag med databevis. Ved slik helhetlig tankegang fra politidistriktets ledelse søker muligheten for målrettet etterforskning og tilrettelegging av databevisene med tanke på presentasjon i retten.

### **Telekombransjens rolle i moderne kriminalitetsutvikling**

Utviklingen i "on-line crime" har medført at telekombransjen er blitt en sentral aktør i moderne kriminalitetsutvikling. Enten man er på sporet av en hacker eller en pedofil som har spredt bilder på internett, er politiet avhengig av opplysninger fra internettilbyderne for å spore opp gjerningspersonen. Det må være et krav fra politiets side at tele- og internettilbyderne oppbevarer logger i tilstrekkelig lang tid (6 måneder bør være et minimum) og utleverer oppkoblingsinformasjon raskt etter forespørsel fra politiet. I en prinsipp sak mellom Telenor Nextel AS og ØKOKRIM avsa Høyesterett kjennelse den 20. desember 1999, hvor ØKOKRIM ble gitt medhold i at internettilbyderne plikter å gi oppkoblingsinformasjon direkte til politiet med hjemmel i teleloven § 9-3. Avgjørelsen er veldig viktig for politiet. Men den er et slag i luften dersom det viser seg at tilbyderne ikke har tatt vare på loggene sine eller ikke har logget i det hele tatt. I dag er reglene på dette feltet uharmoniserte og mangelfulle. ØKOKRIM har derfor tatt initiativ overfor myndighetene for å få gjennomgått regelverket med sikte på å få etablert et pliktsett for telekombransjen som ivaretar politiets behov på tilfredsstillende måte.