Datakriminalitet – forberedelseshandlinger som selvstendig forbrytelse

Artikkelen er basert på en høringsuttalelse til NOU 2007:2 Lovtiltak mot datakriminalitet – Delutredning II

Den internasjonale utvikling og Norge

Europarådets konvensjon om cybercrime trådte i kraft 01.07.2004 og konvensjonen er ratifisert av 22 stater og 21 stater har undertegnet konvensjonen uten ratifikasjon (juli 2007). Mexico og Costa Rica har søkt om tilslutning og er invitert av Europarådet. Norge har vedtatt bestemmelser i straffeloven §§ 12, 145, og 145b og straffeprosessloven §§ 199a og 215a for at konvensjonen kunne ratifiseres den 4.11.2005.

En rekke europeiske land har gjennomført lovtiltak mot datakriminalitet. Etter at Europarådets konvensjon ble vedtatt har blant annet følgende land gjennomført lovtiltak: Tyskland, Sverige, Island, England, Nederland, Danmark, Frankrike, Belgia, Bulgaria, Estland, Italia, Polen og Romania. Europarådet har anbefalt lovtiltakene i Romania som en modell.

Av FN-organisasjoner er det ITU (International Telecommunication Union) i Geneve som har vært mest aktiv med å fremme en global harmonisering av straffelovgivning om cybercrime. Basert på Europarådets konvensjon om cybercrime og anbefalinger fra FN organisasjoner, EU, G8-statene, Organisasjonen for Amerikanske stater (OAS), Asian Pacific Economic Cooperation (APEC), Det Britiske samveldet, Association of Southeast Asian Nations (ASEAN) og OECD foregår det for tiden en global harmonisering av nasjonale straffe- og straffeprosessuelle bestemmelser som angår datakriminalitet.

På grunnlag av Europarådets konvensjon skapes nå forutsetninger for en global rettshåndhevelse basert på felles prinsipper for straffbarhet og straffeforfølgning. Ved å ratifisere eller slutte seg til konvensjonen, eller implementere de standarder og prinsipper som den inneholder, forsikrer statene seg at de nasjonale bestemmelser er tilfredstillende. Den harmonisering av nasjonale straffe- og straffeprosessuelle bestemmelser som nå foregår reduserer mulighetene for "data havens", stater med jurisdiksjon hvor datakriminalitet helt eller delvis er straffritt. I en global etterforskning og straffeforfølgning må de enkelte lands prosessbestemmelser også være tilpasset hverandre. Et effektivt internasjonalt samarbeid er avgjørende i etterforskningen av den globale datakriminalitet og sikring av elektroniske bevis i slike saker.

Forberedelseshandlinger som selvstendige forbrytelser

I høringsuttalelsen til NOU 2007:2 om lovtiltak mot datakriminalitet fremmes et alternativt lovutkast til straffebestemmelser i den spesielle del i ny straffelov. I lovutkastet foreslås at det også i Norge vedtas en særskilt bestemmelse som gjør forberedelseshandlinger med data og datasystemer straffbare som selvstendige forbrytelser. Det har vært en lovgivningspolitisk tradisjon at forberedelseshandlinger ikke skal være straffbare. Men i de senere år har det vært nødvendig å gjøre unntak i flere forhold, senest lovforslag om forebygging av terrorvirksomhet og straffeloven § 145 b. Denne bestemmelse bør for øvrig i forbindelse med vedtakelse av ny straffelov utvides til og også omfatte de øvrige forberedelseshandlinger som er nevnt i Europarådets konvensjon om cybercrime artikkel 6. Endringen bør være i overensstemmelse med justisdepartementets forslag i Ot.prp. nr 40 (2004-2005). Dataprogrammer eller andre innretninger som er særlig egnet til å begå straffbare handlinger som retter seg mot data eller datasystemer (hackerverktøy) bør medtas i bestemmelsen. Det antas i dag ikke straffbart å gjøre datavirus og hackerverktøy tilgjengelig for andre på et nettsted, selv om en med sikkerhet kan si at de vil bli brukt til å begå andre former for datakriminalitet av andre gjerningsmenn.

Informasjons og kommunikasjonsteknologien er inne i en voldsom utvikling med fildeling, to veis kommunikasjon, nettsamfunn som Facebook, YouTube, og Myspace. Kriminelle bruker også nye aktiviteter som botnets, phishing, pharming, spam, identity-theft og spyware. Flere av disse aktiviteter brukes som forberedelse til straffbare handlinger. Behovet for å straffesanksjonere produksjon, besittelse og andre disposisjoner over slike er åpenbart tilstede.

Både svensk og dansk rett har bestemmelser som rammer forberedelseshandlinger. Den danske straffelov § 21 rammer "handlinger som sikter til å fremme eller bevirke utførelsen av en forbrytelse". Bestemmelsen ble brukt i en dom i København byrett av 11.april 2007 hvor en mann ble idømt fengsel i 3 år og 6 måneder.

Svensk rett ble endret den 1. juli 2001 ved at bestemmelsen om forberedelse til brott ble endret til å omfatte "befattning med något som er særskilt egnat att anvendas som hjelpmedel vid ett brott". Endringen tok sikte på at straffeansvaret ikke bare omfattet befatning med fysiske gjenstander, men også at befatning med immaterielle objekter kunne være straffbar som en forberedelse. Som eksempel ble det i motivene for lovendringen særskilt vist til datavirus og annen programvare som er fremstilt utelukkende med det formål å foreta uberettiget tilgang til data eller annen datakriminalitet.

Den tradisjonelle lære om grensen mellom den straffrie forberedelse og forsøk på straffbare handlinger har sin vesentlige betydning i forhold til fysiske handlinger med personer og materielle gjenstander. Gjennomslagskraften er ikke like vesentlig overfor immaterielle objekter som data. Aktiviteter som phishing, botnets og spam har hovedsakelig et meget begrenset lovlig bruksområde og er særlig egnet til å benyttes som hjelpemidler for straffbare handlinger.

En særskilt bestemmelse om straff for forberedelseshandlinger kan øke tilliten til, og bruk av elektronisk kommunikasjon. Dette vil trygge samfunnets bruk av informasjons- og kommunikasjonsteknologi. Jeg har overfor Justisdepartementet foreslått følgende bestemmelse:

> *Enhver befatning med data i et datasystem som er særlig egnet til å anvendes som hjelpemiddel til en straffbar handling, straffes som forberedelse til straffbar handling.*

Enkelte merknader til lovutkastet i NOU 2007:2

Av hensyn til den teknologiske utviklingen bør bestemmelser i straffeloven være mest mulig teknologisk nøytrale. Bruk av uttrykk som "internett" er tillegg upresist og hører ikke hjemme i en straffebestemmelse.

Definisjoner av data, dataprogram, datasystemer, databasert informasjon og elektronisk kommunikasjon er av teknologisk karakter og hører ikke hjemme i en straffelov. Det er eventuelt naturlig å plassere slike definisjoner i spesiallovgivningen hvor fremtidig utvikling lettere lar seg tilpasse ved bruk av forskriftsverk.

Det er en sikker oppfatning i norsk rettspraksis og teori at data ikke er en gjenstand. Lagringsmedia kan være gjenstander men ikke data i seg selv. Stortinget har utvetydig klargjort dette i sitt vedtak til en ny straffelov første del, og har i sine merknader til legaldefinisjonen av gjenstand i § 12 uttalt: "Informasjon i datasystemer m.v. skal fortsatt ikke regnes som gjenstand".

Data er en elektronisk representasjon av informasjon og det er lovteknisk tradisjon for å bruke uttrykkene "data" eller "informasjon". Uttrykket "databasert informasjon" er derfor uheldig. Informasjonen i seg selv kan ikke lagres eller overføres. Informasjon oppstår først i et menneskes bevissthet når data blir sett, hørt, følt eller på annen måte brakt innenfor rekkevidden av sanseapparatet, se Knut S. Selmer, (Lov og rett 1995 side 149-150). Benyttelse av betegnelsen "datamodifikasjon" synes i tillegg også noe gammelmodig.

Begrepet tyveri er i norsk strafferett definert i straffeloven § 257 og forutsetter at en gjenstand borttas. Når data ikke er gjenstand kan ikke definisjonen av tyveri anvendes. Etter alminnelig forståelse må en gjenstand være av fysisk beskaffenhet, og immaterielle objekter faller utenfor begrepet. Betegnelsene informasjonstyveri, datatyveri og identitetstyveri bør ikke benyttes.

Konklusjon

I den globale harmonisering av lovgivning om datakriminalitet som nå foregår er det viktig at Norge tilpasser seg sine internasjonale forpliktelser. Lovtiltak må gjennomføres i overensstemmelse med internasjonalt godkjent standarder og

prinsipper. Lovutkastet i NOU 2007:2 tilfredstiller ikke disse krav. Det er beklagelig at NOU 2007:2 ikke inneholder noen oversikt eller henvisning til fremmed rett. Jeg er ikke kjent med at det foreligger lovtiltak i andre land av tilsvarende art.

Lovutkastet anbefales derfor ikke.

Høringsuttalelsen fra undertegnede med et alternativt lovutkast er i sin helhet tilgjengelig på www.cybercrimelaw.net

Stein Schjølberg
Sorenskriver i Moss tingrett