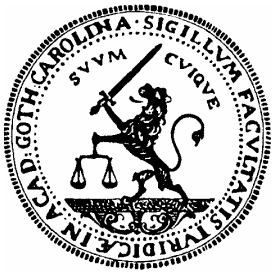


JURIDISKA FAKULTETEN
vid Lunds universitet

Isak Rydlund

Otillåtet eller inte?
En analys av dator- och datarelaterade gärningar ur ett brottsbalksperspektiv

Examensarbete
20 poäng

Per-Ole Träskman

Straffrätt

Ht 2004

Innehåll

Sammanfattning

Vår vardag påverkas och är beroende av att information är åtkomlig i världsomspännande datanätverk. Denna information måste också vara korrekt samt i vissa fall oåtkomlig för obehöriga. Genom hacking, wardriving, sniffing, portscanning och DoS attacker kan en hacker orsaka enorma skador inte bara för samhället utan också för enskilda personer och företag. Men är dessa gärningar brott?

Brottet dataintrång regleras i 4 kap. 9c § BrB, denna bestämmelse som har sitt ursprung i Datalagens 21 § har under de senaste trettio åren enbart genomgått smärre förändringar. Lagstiftaren önskade utforma paragrafen på ett sätt som skulle göra den framtidssäker. Genom att göra paragrafen teknikneutral ansåg man ha lyckats med detta. Nu trettio år senare kan vi se att denna intention ej till fullo uppfyllts.

Dataintrång och därmed också hacking, kan delas upp i två kategorier; interna och externa. Dessa två kategorier kan sedan delas in i två undergrupper; ren och oren hacking. Gemensamt för dessa är att gärningsmannen berett sig tillgång till upptagning för automatisk databehandling. Vad just upptagning för ADB innebär är något som orsakat och fortfarande orsakar problem vid rättstillämpningen. Datas kvasimateriella karaktär medför vidare att gärningar, som vid angrepp på fysiska objekt skulle bedömas som stöld eller skadegörelse inte kan anses utgöra dessa brott.

Brottsbalkens 4 kapitel reglerar flera gärningar som kan sättas i samband med hacking: 4 kap. 9c § BrB - dataintrång, 4 kap. 8 § BrB - brytande av telehemlighet och 4 kap. 9 § BrB - intrång i förvar. Av dessa kan enbart 4 kap. 9c och 8 §§ BrB anses direkt tillämpliga på hacking. Dessa två paragrafer och deras korresponderande osjälvständiga brott kan inte sägas vara tillräckliga i dagens samhälle. Paragraferna innehåller flera brister som inte gör dem tillämpliga på ett sätt som vore önskvärt.

Glädjande är dock att domstolarna inte verkar anse det problematiskt att använda sig av dataintrångsregleringen. Ej heller vid mål med internationell koppling uppstår problem. I de analyserade fallen kan dock en genomgående trend skönjas; domstolarna är ovilliga att bestämma påföljden till annat än dagsböter.

Dataintrång eller hacking är ett ökande internationellt problem. Genom Europarådets konvention om Cyberbrottslighet och Europeiska unionens råds rambeslut om angrepp mot informationssystem har dator- och datarelaterade gärningar flyttats upp på prioritetsordningen. Sverige kommer med anledning av dessa vara tvunget att genomföra ett förhållandevis omfattande lagstiftningsarbete.

Förord

När filmen Wargames gick upp på biograferna 1983 formligen exploderade antalet intrångsförsök i datasystem runt om i världen. När jag för första gången såg filmen kunde jag inte hjälpa att fascineras av det som utspelade sig på bioduken, att man med sin egen dator kunde ta sig in i hemliga militära system och nästan utlösa ett tredje världskrig var för mig något nytt. Nu ett antal år senare vet jag att filmen, i många avseenden, inte är helt verklighetstrogen. Men faktum kvarstår att handlingen i filmen inte är helt tagen ur luften. Samma anläggning som David i filmen hackar sig in i har i verkligheten, vid flera tillfällen, blivit utsatt för mer eller mindre lyckade intrångsförsök.

Datorer och datoriserade system blir mer och mer en del av våra liv, vad händer när dessa system blir utsatta för intrång och attacker kan vi läsa om i tidningarna ganska regelbundet. Men är alla gärningar som dessa hackers gör sig skyldiga till olagliga?

När det talas om dator- och datorrelaterade brott används ofta uttrycket ”Gamla brott i nya kläder”. Men stämmer detta verkligen? Är det verkligen gamla brott? Är det överhuvudtaget brott? Jag vill med denna uppsats försöka ge dem som är intresserade av dator- och datorrelaterad brottslighet en god grund att stå på, både vad avser tekniska såväl som juridiska aspekter.

Jag har under arbetet, när problem och frågor har uppstått, fått hjälp av flera personer och skulle härmed vilja tacka Elisabet Åkerberg, hovrättsassessor vid Hovrätten över Skåne och Blekinge, Håkan Jevrell, sakkunnig i justitiefrågor vid Moderata Samlingspartiets riksdagskansli samt min syster Maria Dupont för hennes synpunkter och all uppmuntran som hon har givit mig under arbetets gång.

Lund, mars 2005

Isak Rydlund

Förkortningar

ADB	Automatisk databehandling
BrB	Brottsbalken
BRÅ	Brottsförebyggande rådet
CERT/CC	CERT® Coordination Center
CSI	Computer Security Institute
DARPA	Defence Advanced Research Project Agency
DataL	Datalagen
DHCP	Dynamic Host Configuration Protocol
DN	Dagens Nyheter
DNS	Domain Name Server
DSU	Datastraffrättsutredningen
EkomL	Lag om elektronisk kommunikation
FBI	Federal Bureau of Investigation
HKV	Högkvarteret
HTTP	Hypertext Transfer Protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
IP	Internet Protocol
IT	Informationsteknologi
KTH	Kungliga Tekniska Högskolan
MAC	Media Access Control
NJA	Nytt Juridiskt Arkiv
OSK	Offentlighets- och sekretesslagstiftningskommittén
Prop.	Proposition
PTS	Post- och telestyrelsen
PuL	Personuppgiftslagen
SIS	Standardiseringskommissionen i Sverige
SOU	Statens offentliga utredningar
SU	Stockholms Universitet
TCP	Transmission Control Protocol
UU	Uppsala Universitet
WiFi	Trådlöst nätverk
WAP	Wireless Access Point – Trådlös access punkt

1 Inledning

1.1 Bakgrund

Det moderna samhället blir mer och mer beroende av den informationsteknologiska infrastrukturen. Samtidigt som användningen av datorer och datorsystem ökar, ökar också missbruket. Missbruk i form av intrång, virusspridning, kartläggning och avlyssning är något som de flesta datoranvändare säkerligen har kommit i kontakt med, de flesta utan att märka det. Men är allt missbruk brottsligt?

I svensk lag reglerades brottet dataintrång för första gången 1973, paragrafen som genomgått enbart smärre förändringar finns sedan 1998 införd i brottsbalkens fjärde kapitel. Paragrafen tar sikte på de missbruk som lagstiftaren kunde förutse 1973 och gavs en teknikoberoende utformning i syfte att vara framtidssäker. Nu 31 år senare är den mer aktuell än någonsin tidigare, men är denna paragraf tillräcklig än i dag? Täcker den in alla former av gärningar som man kan sätta i samband med datorintrång? Finns det andra paragrafer som kan vara bättre lämpade att använda sig av?

1.2 Syfte

Syftet med denna uppsats är att närmare granska lagstiftningen kring dator- och datarelaterade brott som inte är förmögenhetsbrott. Avsikten är att studera den nuvarande lagstiftningen i syfte att utröna vilka gärningar som täcks in, samt utröna hur de relevanta paragraferna tillämpas i praxis. Med detta som bakgrund är min intention att bedöma effektiviteten av dessa lagregler, undersöka relevanta internationella konventioner och avtal samt om behov föreligger föreslå reformer. Vidare kommer en genomgång av tekniska aspekter relevanta för datorrelaterad brottslighet att genomföras.

1.3 Frågeställning

För att utröna huruvida den svenska lagstiftningen på området är adekvat bör den första frågan vara; vilka typer av handlingar är aktuella vid datorintrång? När väl denna fråga har besvarats blir följdfrågan; täcks dessa in av lagstiftningen? Innan en genomgång av eventuella lagstiftningsbehov kan göras måste en översyn av praxis ske. Vad säger statistiken om förekomsten av datorintrång? Vad säger domstolspraxis? Är de gärningar som begås att anses som datorintrång? Om lagstiftningen inte korresponderar med de gärningar som begås, hur borde i så fall lagstiftningen se ut? Samt slutligen vad görs på det internationella planet och hur påverkar detta svensk lagstiftning?

1.4 Avgränsning

Uppsatsen behandlar datorintrång främst externa sådana, ur ett svenskt juridiskt perspektiv. Uppsatsen tar avstamp i brottsbalkens 4:e kapitel och de relevanta bestämmelser som finns där. Europarådets konvention om IT-relaterad brottslighet samt Europeiska Unionens råds rambeslut om angrepp mot informationssystem kommer att behandlas ur ett komparativt perspektiv med den gällande svenska lagstiftningen, detta i syfte att utröna eventuella lagstiftningsbehov som föreligger.

Immaterialrättsliga frågor kommer inte att beröras under arbetets gång.

1.5 Material

Det material som ligger till grund för detta arbete är främst förarbeten, doktrin samt rättsfall. Vad avser litteratur har jag inte enbart använt mig av juridisk utan även till mycket stor del datorinriktad sådan. Detta då stora delar av den juridiska litteraturen är föråldrad vad avser den tekniska utvecklingen på datorområdet. Internet har visat sig vara mycket behjälpligt vid informationssökning varvid mycket av bakgrundsinformationen är hämtad från Internetkällor. Flera institutioner bland annat BRÅ har utarbetat rapporter samt sammanställt statistiskt materiel som har varit till mycket hjälp i mitt arbete. Då datorbrottslighet är hett nyhetsstoff i dagstidningar finns en uppsjö av artiklar som berör uppsatsens område. Dessa har jag använt mig av i den utsträckning de har varit relevanta. Jag har även fått hjälp av riksdagens utredningstjänst att ta fram statistik, samt genomfört intervjuer med personal på Moderata Samlingspartiets riksdagskansli.

1.6 Metod och disposition

Uppsatsens metod är både av deskriptiv och analyserande karaktär. De deskriptiva delarna återfinns framför allt i uppsatsens inledande kapitel, men även i de delar som behandlar internationella åtaganden. Egen analys presenteras fortlöpande i uppsatsen. Metoden som använts är traditionell juridisk metod. Uppsatsens inledande kapitel följs av en redogörelse för IT-begrepp och hur dessa påverkar tillämpning av gällande rätt. Detta i syfte att ge läsaren en bakgrund till den problematik som uppstår vid tillämpning av gällande rätt på dator- och datarelaterade brott. Därefter följer en kort redogörelse för tekniken bakom datornätverk i allmänhet och Internet i synnerhet. Efterföljande kapitel presenterar brottet dataintrång samt definierar olika typer av dataintrång och gärningar som kan utgöra led i detta brott, syftande till att ge läsaren en god grund för den analys som genomförs i senare kapitel. De därefter följande fem kapitlen ger en utförlig redogörelse för den gällande lagstiftningen gällande dator- och datarelaterade brott. Häri presenteras de olika reglernas bakgrund, rekvisit samt tillämpningsområde. Kapitel tio är en kort sammanställning i

tabellform över tillämplig gällande lagstiftning. Från kapitel elva har uppsatsen en mer analyserande karaktär, varigenom ett antal typfall presenteras och analyseras utifrån gällande rätt. I kapitel tolv presenteras statistik över dator- och datarelaterade brott, detta i syfte att utvärdera förekomsten av dator- och datarelaterade brott i Sverige. Den internationella statistik som presenteras syftar till att sätta den nationella statistiken i ett större perspektiv. Syftet med redogörelsen och analysen av praxis i kapitel 13 är att belysa domstolarnas ställningstagande i samband med denna typ av mål. Stor vikt har lagts vid domstolarnas straffmätning och ställningstagande vid bestämmande av brottets svårighetsgrad. Det följande kapitlet redogör för de internationella åtaganden Sverige har i samband med Europarådets konvention om Cyberbrottslighet, samt Europeiska Unionens råds rambeslut om angrepp mot informationssystem. Detta syftande till att möjliggöra en analys om några och i så fall vilka förändringar av gällande lagstiftning Sverige måste företa för att uppfylla sina åtaganden. Häri ges också en kort kommentar till regeringens proposition om antagande av rambeslutet. I de två avslutande kapitlen presenteras egna åtgärdsförslag baserade på de slutsatser författaren dragit under arbetets gång. Den avslutande analysen skall ses dels som en presentation av dessa slutsatser och dels som en avslutande kommentar till arbetet i sin helhet.

2 IT-begrepp och dess betydelse för tillämpning av gällande lagstiftning

Att det inom olika områden används specialbegrepp är något som vi alla har kommit att acceptera. Begrepp som används inom juridik har ofta ett klart och avgränsat tillämpningsområde, deras betydelse är oftast klara och entydiga. Motsvarande kan sägas gälla inom IT-världen.

Problem uppstår dock när dessa två begreppsvärldar kolliderar, speciellt tydligt blir detta inom straffrätten. Juridik i allmänhet, men straffrätt i synnerhet förlitar sig på att uttryck skall vara begränsade i sina tillämpningsområden. Inom straffrätten är detta speciellt viktigt, då man här är begränsad i tillämpningen av lagar och förordningar på grund av legalitetsprincipen. Legalitetsprincipen som uttrycks i brottsbalkens första kapitel första paragraf stadgar att:

Brott är en gärning som är beskriven i denna balk eller i annan lag eller författning och för vilken straff som sägs nedan är föreskriven.
(Lag 1994:458)

”Denna princip utgår från förutsättningen att ett ords eller begrepps betydelse utgör gränsen för möjligheten att tolka den aktuella straffbestämmelsen”. [1] Legalitetsprincipen begränsar således möjligheten att utöka ord och begrepps tillämpningsområde inom straffrätten. När det uppstår begreppskollision mellan vedertagna juridiska begrepp och nya begrepp som exempelvis inom IT-världen uppstår frågan om lagstiftningen är direkt tillämplig, eller om ny lagstiftning fordras.

Ett flertal exempel där en sådan kollision har uppstått kommer att belysas de kommande sidorna.

[1] Silvander, Dator- och Datarelaterade brott, s.88.

3 Datornätverk[2]

3.1 Bakgrund

Under 1970-talet skapades vad som i dag kallas för Internet[3] av forskare inom DARPA[4]. Det revolutionerande med detta datornätverk var det faktum att olika typer av datorer från olika tillverkare kunde kommunicera med varandra genom att använda ett speciellt protokoll kallat TCP/IP. Från att ha varit ett projekt som syftade till att säkerställa kommunikationer vid ett eventuellt kärnvapenangrepp mot USA har de delar av ARPANet som möjliggjorde kommunikationen spridits till att vara en oavhängig beståndsdel i näst intill samtliga datanätverk som finns i dag.

3.2 TCP

TCP eller Transmission Control Protocol är enkelt uttryckt det sätt som datorer kommunicerar med varandra på Internet. Man kan jämställa det med ett gemensamt språk för datorer som används när information skall skickas från en dator till en annan.

3.3 IP

Internet Protocol är det sätt som datorer identifieras på ett TCP/IP nätverk. Varje dator tilldelas ett unikt nummer en så kallad IP-adress (IP-nummer). Denna IP-adress kan antingen vara fast, eller så kan den vara ett tillfälligt lån så kallad dynamisk. IP-nummer jämställs ofta med telefonnummer, vilket är en ganska bra analogi. När en dator vill kommunicera med en annan dator via ett nätverk används nämligen IP-numret för att identifiera avsändaren samt mottagaren.

Som tidigare nämnts tilldelas varje dator på ett TCP/IP nätverk ett unikt IP-nummer, detta sköts normalt av en central DHCP server. Detta medför att man kan vilseleda nätverket gällande sitt IP-nummer, så kallat *Spoofa*, genom att själv specificera detta.[5]

---

[2] Kapitlet bygger på lärdomar dragna under kurserna Informations- och datasäkerhet/ Säkra IT-system, Datasäkerhet 2/ Computer forensics, Datakommunikation vid KTH samt kursen Informationssäkerhet vid Blekinge tekniska högskola.

[3] Internet var tidigare känt som ARPANet.

[4] Defence Advanced Research Project Agency.

[5] Detta genomförs genom att man beordrar datorn att sända en felaktig MAC adress till DHCP servern. DHCP servern som tror att datorn den kommunicerar med är en annan tilldelar ett IP-nummer som istället borde ha tilldelats den rättmätige innehavaren av den specifika MAC adressen.

3.4 TCP/IP kommunikation

När data sänds på ett nätverk delas trafiken upp i paket, detta sker helt transparent för användaren. Dessa paket sätts sedan samman till en sammanhängande dataström hos mottagaren. Paketen sänds till alla datorer på nätverket men enbart den dator som är den avsedda mottagaren kommer att godkänna dem för mottagning, alla andra datorer kommer att ignorera dem. Detta möjliggörs av den information som varje paket innehåller. Varje paket innehåller information om; den sändande datorns MAC adress[6], sändande och mottagande dators IP adress, en TCP header, en HTTP header, samt själva informationen. Ett paket godkänns inte för mottagning om datorns och paketets MAC adress inte stämmer överens. Normal storlek för ett paket är runt 1500 bytes.

3.5 Router

En router är enkelt förklarat en speciell dator som kommer ihåg vilka datorer (eller nätverk) som är anslutna till den. Routern skickar paket som skall till en viss dator i dennes riktning, om routern är den sista innan den mottagande datorn skickar den paketet direkt till denna.

3.6 DNS-server

En Domain Name Server (DNS) lagrar information om var en viss dator befinner sig i nätverk. I Internet sammanhang är det här som WWW adressen tolkas om från exempelvis www.rydlund.com till serverns IP adress 194.47.208.147. På Internet finns det en mängd DNS-servrar som alla konstant kommunicerar med varandra för att säkerställa att man har den mest aktuella informationen om var olika servrar finns. Denna kommunikation sker utan kontroll av att informationen verkligen är korrekt, vilket som jag senare tar upp kan användas för att genomföra så kallade DoS attacker.

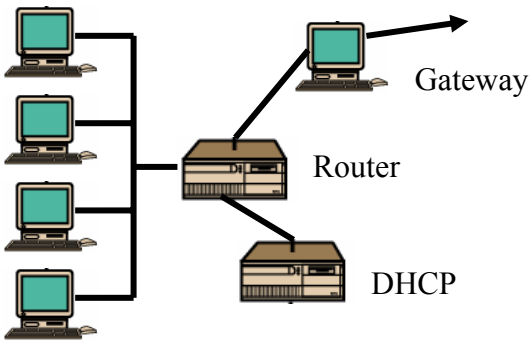
3.7 LAN, WAN och Internet

Datornätverk kan byggas upp på olika sätt, det i dag vanligaste är så kallade stjärnkopplade. Denna typ av nätverk innebär att samtliga datorer kopplas med en egen kabel till antingen en hubb, switch eller router.

Ett lokalt nätverk exempelvis på en arbetsplats kallas för LAN eller Local Area Network. Om detta LAN är i behov av kontakt med andra LAN

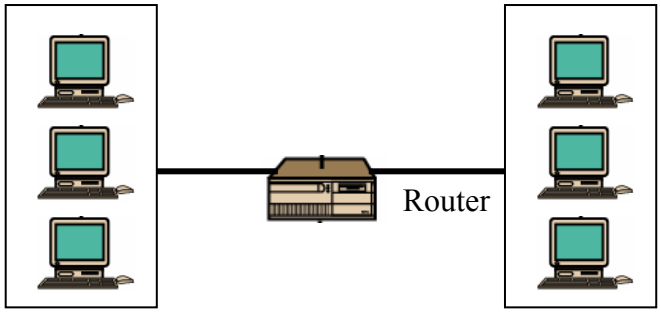
[6] En MAC adress är ett nätverkskorts individnummer. Det skall teoretiskt sett inte finnas två kort med samma nummer, i praktiken uppstår det ofta situationer där olika tillverkare har använt sig av samma individnummer för olika kort.

används en router, samt oftast en Gateway[7] som kopplingspunkt mot ett annat LAN eller Internet. Noteras bör dock att det som i allmänt språkbruk kallas att vara uppkopplad mot Internet i själva verket är att vara uppkopplad mot en ISP:s LAN eller WAN.



Local Area Network (LAN)

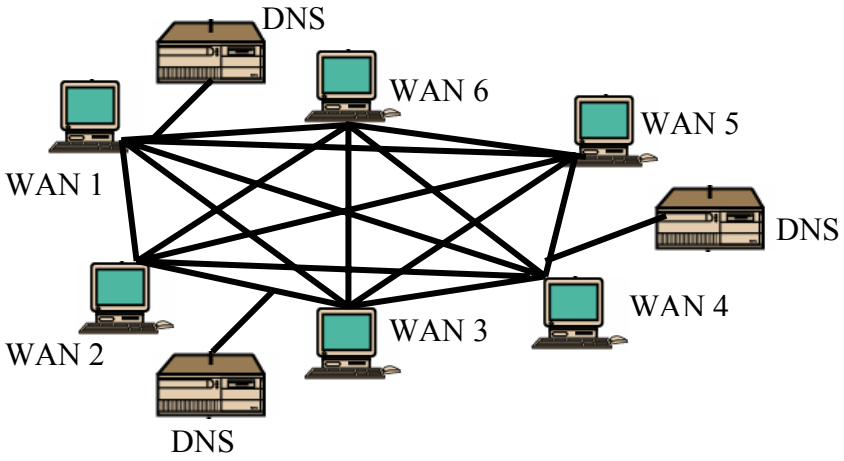
Ett WAN är inget annat än flera sammankopplade LAN. Ett företag kan exempelvis koppla samman de lokala kontorens LAN i ett stort företagsnätverk, ett företags WAN



Wide Area Network (WAN)

Internet består av flera sammankopplade WAN, samt ett antal olika DNS servrar på olika platser i nätverket. Internet är med andra ord ett gigantiskt stort WAN.

[7] En Gateway är en dator som har till syfte att vara kopplingspunkt mot ett annat nätverk. Den kan användas för att filtrera bort oönskad trafik, samt för att lastballansera trafiken.



Del av Internet

Som tidigare sagts utvecklades det som i dag kallas för Internet ur en önskan att säkerställa kommunikationer vid ett eventuellt kärnvapenangrepp. Data i nätverket sänds genom den del som är mest effektiv, om en del av nätverket slutar att fungera sänds dataströmmen en annan väg. Allt detta sker helt transparent för användaren, och är något som den normala användaren inte kan påverka.

4 Datormissbruk och datorbrott

4.1 Inledning

Det talas ofta om *datorbrott*, *IT-brott* eller *datorrelaterad brottslighet*, men vad menas med dessa ord? Många definitioner har under åren framkommit, dessa har alla gemensamt att antingen målet eller medlet för den brottsliga gärningen är en dator. Exempelvis definierade *von zur Mühlen* 1972 *datorbrott* på följande sätt ”Datorbrott är varje brottslig gärning i vilken en dator är medlet eller målet för gärningen”.[8] En expertgrupp inom OECD definierade 1983 uttrycket *datormissbruk* på följande sätt ”[med datormissbruk] förstås varje olaglig, oetisk, eller olovligt beteende som rör automatisk databehandling eller transmission av data”[9]. Datormissbruk blir därmed en beteckning på handlingar inom ett väldigt brett spektrum jämfört med den snävare termen datorbrott. I Sverige är som bekant brott en gärning som är beskriven i brottsbalken, annan lag eller författning och för vilken straff är föreskrivet.[10] I brottsbalkens 4 kap. 9c § finns bestämmelsen om dataintrång.

4.2 Interna och externa dataintrång

4.2.1 Interna dataintrång

Med interna dataintrång avses intrång som förövas av en gärningsman som finns inne i datorsystemets ägares organisation, exempelvis en anställd eller annan person som är auktoriserad att använda systemet. Denna typ av dataintrång sker vanligast genom att användaren tar sig in i datorsystem eller register som denne inte har tillåtelse att använda. Vanligast är att användaren överskrider sina befogenheter genom att exempelvis bereda sig tillgång till sekretessbelagda registerhandlingar såsom patientjournaler eller utdrag ur polisens register. Även andra obehöriga intrång kan komma ifråga, såsom att bereda sig tillgång till arbetskamraters datorer eller filer. Gemensamt för dessa handlingar är att de inte sker som ett led i deras tjänsteutövning eller ordinarie arbetsuppgifter. Denna typ av intrång har under senare tid fått stor uppmärksamhet, bland annat i samband med mordet på Anna Lindh.

[8] SOU 1992:110, s.84.
[9] Ibid.
[10] 1 kap. 1 § BrB.

4.2.2 Externa dataintrång

När intrånget genomförs av någon som inte är direkt knuten till organisationen ses detta som externt. Detta innebär dock inte att förövaren inte får ha någon koppling till organisationen, förövaren kan exempelvis vara en leverantör, kund eller före detta anställd. Antalet rapporterade externa dataintrång är förhållandevis lågt, detta beror dock sannolikt på en ovilja från organisationer att rapportera dessa till polis då det skulle medföra negativa effekter för förtroendet bland kunder och samarbetspartners, mörkertalet är med andra ord stort.[11]

4.3 Hacking

Enligt en online-ordlista definieras hacking som ”[to] gain access to (a computer file or network) illegally or without authorization”[12]. Denna definition har lett till starka protester från personer inom grupper av avancerade datoranvändare, då epitetet hacker i dessa kretsar innebär “someone who is able to manipulate the inner workings of computers, information, and technology”[13]. Inom dessa kretsar föredras termen cracker istället för hacker för att beskriva någon som gör intrång i datorer. Termen hacker har sitt ursprung i det tidiga 1970-talets MIT. Medlemmar i Modelljärnvägsföreningen kallade sig hackers efter ljudet som järnvägens växlar framkallade, ordet fick sedermera en vidare betydelse då skolan datoriserades. En hacker beskrev en person som kunde få skolans datorer att producera det resultat operatören ville. Ett hack var en elegant lösning på ett intrikat problem.[14] I denna uppsats kommer termen hacker att beskriva en person som använder sina kunskaper till att illegalt försöka ta sig in i datorsystem. Detta då det är denna betydelse som Datastraffutredningen har använt sig av.[15]

Intrång i datasystem kan ske på många sätt; *brute-force* attacker där alla vanliga ord i en ordlista används för att automatiskt gissa lösenord till ett system, stöld av lösenord från sopor eller via *social engineering*[16] eller genom att utnyttja kända buggar eller säkerhetshål i datorsystemet.

---

[11] BRÅ rapport 2000:2, IT-relaterad brottslighet, s.43.
[12] http://www.securitylex.org/glossary#hacker,%20hacking
[13] http://www.robertgraham.com/pubs/hacking-dict.html#hacking Det finns en strikt hierarki inom hacker världen; termer som white-hat, black-hat, lamer and script kiddie används för att beskriva olika kunskapsnivåer. Det finns till och med ett speciellt skriftspråk kallat 1337 sP3k (uttalas Leetspeak) som skiljer hackers från andra datoranvändare.
[14] Termen *hack* används också för att beskriva spratt spelade av studenter vid MIT. För mer information angående detta se: http://hacks.mit.edu/Hacks/
[15] SOU 1992:110, s.187.
[16] Social engineering innebär att hackern lurar legitima användare att tro att han också är en legitim användare för att på så sätt få tillgång till lösenord eller annan information om datorsystemet.

4.4 Wardriving

Wardriving är en relativt ny företeelse som syftar till att upptäcka och kartlägga trådlösa access punkter (WAP:s)[17] genom att använda bärbara datorer utrustade med trådlösa nätverkskort, GPS-mottagare[18] och speciell programvara[19].

Termen kommer från filmen *WarGames*[20], där en tonåring använder sig av sin hemdator för att ringa hundratals telefonnummer i jakten på datornätverk, denna metod kom att bli känd som *Wardialing*.

Vid wardriving är det inte nödvändigt att de facto koppla in sig på nätverket för att upptäcka det. En WAP sänder konstant ut en identitetssignal[21] i syfte att identifiera sig, det är denna signal som detekteras vid wardriving. Det är med andra ord WAP:en som initierar kommunikationen. Även om inte speciell programvara eller GPS används kan vissa operativsystem såsom WindowsXP detektera WAP:s på egen hand utan att användaren önskar detta. Genom att stänga av möjligheten för TCP/IP kommunikation kan personen omöjliggöra eventuell kommunikation med datornätverket vid wardriving. Värt att notera är att vissa operativsystem som exempelvis WindowsXP automatiskt väljer den WAP med bäst mottagning som finns i området, med andra ord kan alltså datorn själv koppla upp sig mot en WAP utan någon handling från användaren.

4.5 Sniffing

Sniffing är en form av digital avlyssning. Genom att använda speciell programvara kan en dator på ett datornätverk avlyssna, analysera och spara all information som transporteras i nätverket. Såvida nätverket som skall avlyssnas inte är trådlöst, måste datorn vara fysiskt inkopplad på nätverket.

Genom sniffing kan all trafik på ett datanätverk avlyssnas. Om så önskas kan MAC samt IP-adresserna för sändande och mottagande dator extraheras och användas för att *spoofa*[22]. Genom att *spoofa* kan data omdirigeras till hackerns dator alternativt kan data sändas och uppfattas som legitim trafik. Det är viktigt att komma ihåg att hackern måste befinna sig på samma fysiska nätverk (antingen genom att vara inkopplad med sladd eller trådlöst) för att sniffing skall kunna genomföras. Det är alltså inte möjligt att befinna sig i Lund och sniffa trafik i Umeå. En hacker är troligtvis främst intresserad av att sniffa fram lösenord och användarnamn, men även kreditkortsnummer och annan känslig information kan vara intressant.

---

[17] Wireless Access Points.
[18] Global Positioning System – Satellit baserat positionsbestämningssystem.
[19] Vanligt förekommande programvaror är Netstumbler, Kismet och iStumbler.
[20] Paramount 1983.
[21] Även kallad Beacon.
[22] Spoofing innebär att man ändrar nätverkskortets MAC adress.

4.6 Portscanning

I moderna datornätverk används oftast TCP/IP protokollet för kommunikation mellan olika datorer. En viktig del i detta är vad som kallas för portar. Portar kan jämföras med dörrar in till en dator, varje process i en dator som kommunicerar på ett nätverk har ett visst portnummer. Dessa portar kan antingen vara stängda, öppna eller gömda. Vid portscanning letar man efter öppna alternativt stängda portar. Öppna portar kan i vissa fall användas för att ta sig in i datorsystemet, stängda portar kan användas för att identifiera vilka programvaror som körs i systemet och därmed hjälpa vid identifiering av möjliga säkerhetshål och buggar vilka kan utnyttjas för intrång. Portscanning medför vanligtvis ingen skada, men kan vara ett första steg i ett intrångsförsök.[23]

4.7 DoS

Denial of Service (DoS) attacker är också kända som *the ping of death* eller *nuking*. DoS är ett samlingsnamn för attacker som syftar till att undanhålla en viss funktion för legitima användare. Funktionen kan vara ett program, en webbsida eller ett helt datorsystem.

DoS åstadkoms genom att man sänder felaktig-, stora mängder eller information med otroligt kort intervall och därigenom skapar proppar i kommunikationssystemet. Det vanligaste sättet att genomföra DoS attacker är genom att sända så kallade ping[24]. Genom att antingen förändra ping-paketens sammansättning, exempelvis genom att sätta måldatorn som både sändare och mottagare kan man skapa en oändlig loop som överbelastar datorn, eller genom att sända ofantliga mängder ping-paket (flera tusen per sekund) få datorn att helt enkelt inte hinna med att svara varvid datorn överbelastas. Ytterligare sätt kan vara att sända paket som är större än tillåtet varvid såkallad fragmentering uppstår. Då hopsättning av fragmenterade paket tar stora systemresurser i anspråk, kan man vid upprepad utsändning av dylika snabbt överbelasta en dator.

En DoS attack kan antingen genomföras från en eller flera datorer (så kallad *Distributed Denial of Service attack* - DDoS). Vid DDoS attacker utnyttjas oftast datorer vars legitima användare är helt ovetande om vad som pågår (så kallade *Drones*). Kontroll över dessa *drones* åstadkoms oftast genom vissa typer av virusangrepp.

Ett exempel på vad DDoS attacker kan få för följder är den attack som en kanadensisk 15-åring kallad *mafiaboy* genomförde i februari 2000. Attacken

[23] PTS, Analys av hotbilder för IT-incidenter, s.9.
[24] Ett ping är ett paket som förutom den normala informationen (förklarat i 3.2) även innehåller en begäran att mottagaren skall sända ett svarspaket tillbaka.

riktade sig mot webbsidor baserade i USA såsom CNN, Yahoo, Ebay, Amazon.com, Excite, och Etrade. Skadan som uppstod vid denna attack som utnyttjade minst 54 datorer som *drones* uppskattades till 1.7 miljarder USD.[25]

[25] http://www.fbi.gov/pressrel/pressrel01/mafiaboy.htm samt http://news.bbc.co.uk/1/hi/sci/tech/1541252.stm

5 Brottsbalken 4 kapitlet 9c §

5.1 Inledning

Gärningen dataintrång regleras i 4 kap. 9c § BrB. Paragrafens text är i stort sett samma som fanns i Datalagens[26] 21 § fram till 1998 då denna ersattes av Personuppgiftslagen (PUL)[27] och den relevanta bestämmelsen flyttades till brottsbalken. Paragrafen är till sin utformning teknikneutral, det vill säga ingen specifik teknik åsyftas i paragrafen.

9 c § Den som i annat fall än som sägs i 8 och 9 §§ olovligen bereder sig tillgång till upptagning för automatisk databehandling eller olovligen ändrar eller utplånar eller i register för in sådan upptagning döms för dataintrång till böter eller fängelse i högst två år. Med upptagning avses härvid även uppgifter som är under befordran via elektroniskt eller annat liknande hjälpmedel för att användas för automatisk databehandling.
(Lag 1998:206)

4 kap. 9c § BrB innehåller i sig själv inte något subjektivt rekvisit. Detta har sitt ursprung i det faktum att paragrafen flyttades i stort sätt utan ändringar från 21 § Datalagen[28]. När paragrafen flyttades till brottsbalken fick den automatiskt ett subjektivt rekvisit av 1 kap. 2 § BrB.

Paragrafen innehåller ej heller något skada/vinnings rekvisit. Grunden till detta är oklart, en möjlig anledning är att lagstiftaren ville att paragrafen skulle kunna användas även när förfarandet inte kan anses ha orsakat någon ekonomisk skada.

5.2 Data

Begreppet data är av central betydelse i paragrafen. Svenska akademiens ordlista definierar data såsom; ”uppgifter, fakta, material för maskinell eller manuell informationsbehandling”.[29] Denna definition är dock inte densamma som åsyftas i 4 kap. 9c § BrB. När Offentlighets- och sekretesslagstiftningskommittén 1972 utkom med sitt betänkande ”Data och integritet”[30] definierade man data som uppgifter som matats in i en datamaskin och som kan lagras däri eller överflyttas till kringutrustning eller andra datamaskiner, detta sker inte i visuellt läsbar form utan enbart i

[26] SFS 1973:289.
[27] SFS 1998:204.
[28] SFS 1973:289.
[29] Svenska akademiens ordlista över svenska språket, 1999. Enligt National Encyklopedins fjärde band 1990 är data en ”representation av fakta, begrepp eller instruktioner i form lämpad för överföring, tolkning eller bearbetning av människor eller maskiner”.
[30] SOU 1972:47.

maskinläsbar form. Denna definition kan i dag tyckas något föråldrad. När datastraffutredningen utkom med sitt betänkande definierade man begreppet data på ett något annorlunda sätt ”data […] är representationen av fakta, begrepp eller instruktioner i en form lämpad för överföring, tolkning eller bearbetning utförd av människor eller av automatiska hjälpmedel”[31]. Kravet på enbart maskinläsbarhet har fallit bort och istället har man sett data som representationen av den ursprungliga informationen. Inga vidare krav på hur denna representation skall förete sig uppställs utan man talar senare om ”datas kvasimateriella karaktär”,[32] Data kan både vara ett konkret såväl som ett abstrakt föremål och därmed också ”ha en existens fristående från en viss bärare”[33].

5.3 Skyddsobjekt

5.3.1 Upptagning

Paragrafens skyddsobjekt är upptagning för automatisk databehandling. Upptagningsbegreppet har sin utgångspunkt i begreppet handling såsom det har definierats (eller rättare sagt inte definierats i tryckfrihetsförordningen).[34] Departementschefen godtog dock inte att begreppet upptagning fick en traditionell fysisk utgångspunkt, han uttryckte istället sin önskan att begreppet upptagning i Datalagens mening skulle avse ”själva informationsinnehållet, dvs. den uppgift som fixerats på det tekniska mediet […] [en] uppgift som fixerats på någon form av datamedium och som antingen finns i eller kan matas in i en datamaskin […] läsbar endast med ADB-teknik.”.[35]

OSK valde dock att utgå från det traditionella handlingsbegreppet varpå kravet på fixering medför att upptagningen är knutet till ett fysiskt objekt, och inte avser informationen så som fristående objekt.[36] Skillnaden mellan handling och upptagning valde OSK att precisera på så sätt att information som inte kräver ADB utrustning för att läsas är att anses som handling. För att en upptagning skall anses föreligga skall ADB utrustning krävas för avläsning. Således faller information som lagrats på magnetband, hårddiskar, ROM minne samt andra dylika informationsbärare som inte är läsbara utan annan utrustning under upptagningsbegreppet, numera obsoleta informationsbärare såsom hålkort torde däremot falla under handlingsbegreppet då dessa är läsbara utan annan utrustning.

Upptagningsbegreppet förutsätter som tidigare nämnt att data är fixerad, hur lång denna fixering måste vara är inte preciserat i något av lagförslagen.

---

[31] SOU 1992:110, s.83.
[32] Ibid, s.96.
[33] Ibid, s.96.
[34] SOU 1972:47, s.50.
[35] Prop. 1973:33, s.75.
[36] Ibid, s.23.

Dock torde den tid som data måste vara fixerad inte vara alltför kort för att falla under begreppet, exempelvis torde data i så kallat cache- samt RAM-minne inte ses som fixerad.[37] Det inbyggda kravet på fixering i upptagningsbegreppet medförde att datatrafik mellan två eller flera datorer inte ansågs som upptagning något som 1986 ledde till att 4 kap. 9c § BrB utvidgades till att även avse ”uppgifter under befordran via elektroniskt eller annat liknande hjälpmedel för att användas för automatisk databehandling”[38]. *Silvander* hävdar i sin doktorsavhandling ”Dator- och Datarelaterade förmögenhetsbrott utom borgenärsbrotten” att data kan anses fixerad på en elektromagnetisk bärvåg. Det vill säga att data skall anses som fixerad även under överföring mellan två datorer. Något som klart motsades i Datastraffrättsutredningens betänkande;

> *”Objektet utgörs då av det som överförs och denna ström av signaler i form av elektroner i en elektrisk ledning eller av ljusvågor i en optisk kabel kan knappast ses som sak. […] Eftersom elektricitet inte kan ses som något konkret, uppkommer motsvarande komplikationer vid olovlig kraftavledning. Det anses inte utgöra en besittningsrubbning att avleda ström genom en olovlig inkoppling på elnätet, varför ingreppet inte kan föranleda ansvar för stöld eller egenmäktigt förfarande”*[39]

5.3.2 Automatisk databehandling

Paragrafen tar sikte på upptagning för *automatisk databehandling*, vad *automatisk databehandling* mer exakt innebär har dock inte preciserats i förarbetena. Datastraffrättsutredningen poängterade dock 1992 att även om databehandling i vidsträckt mening skulle kunna innefatta all ”hantering av data i form av siffror, bokstäver och andra tecken utan något krav på att hanteringen skall ske enligt bestämda entydiga regler”, avses numera med begreppet att en serie systematiska operationer utförs på givna data. [40] Någon entydig juridisk definition av begreppet har dock inte framkommit och det har bland annat uttryckts att en sådan definition inte är nödvändigt för ett rättssäkert och effektivt tillämpande av lagstiftningen. Detta då bland annat den snabba tekniska utvecklingen annars skulle medföra svårigheter vid tillämpningen av lagstiftningen.[41]

Flera försök att ge vägledning om vad som faller in under begreppet har dock gjorts, det tydligaste gjordes av SIS 1977. Enligt SIS avses med begreppet *automatisk databehandling* en ”databehandling som

[37] SOU 1992:110, s.109.
[38] Prop. 1985/86:65, s.31-32.
[39] SOU 1992:110, s.97.
[40] Ibid, s.83.
[41] SOU 1990:61, s.91.

huvudsakligen utförs med dator”[42]. Dator definieras såsom en ”databehandlingsapparat som utan mänskligt ingripande under körning kan utföra omfattande beräkningar med ett stort antal aritmetiska eller logiska funktioner” [43]. Noteras bör att SIS inte avsåg att skapa en juridiskt hållbar definition. SIS definition har inte heller använts i något av förarbetena till vad som nu är 4 kap. 9c § BrB, utan man har istället använt sig av den otydliga definitionen i prop. 1973:33 som enbart stadgar att informationen skall ingå eller kunna matas in i ett sådant automatiskt (databehandlingssystem) system. Propositionens definition blir således en form av cirkelresonemang vilket inte leder till någon klarhet.

5.4 Intrångssätt

4 kap. 9c § BrB ställer upp två olika intrångssätt dels att någon bereder sig tillgång till, och dels att någon ändrar, utplånar eller i register för in uppgifter.

När Förmögenhetsbrottsutredningen 1983 gjorde en översyn av lagstiftningen gällande datorintrång försökte man att precisera innebörden av intrångssätten i Datalagens 21§ (numer 4 kap. 9c § BrB). Man delade in gärningen i fyra olika typer baserat på angreppsobjekt och gärningens utförande:[44]

- Outputen från databehandlingsprocessen förvanskas genom att ett program ändras, eller att oriktiga uppgifter inmatas.
  - Denna typ av gärning kan innebära en förmögenhetsskada uppstår eller utnyttjas för att åstadkomma en sådan skada. Vidare kan den ha till syfte att dölja en redan förorsakad skada. Oftast torde denna typ av handlingar kunna falla under brottsrubriceringar såsom; bedrägeri, trolöshet mot huvudman eller förfalskningsbrott.
- Skadegörande handlingar riktade mot mjukvara.
  - Denna typ av handlingar torde även kunna falla under 12 kap. 1 § BrB – skadegörelse.
- Obehörig tillgång till program eller data.
  - Torde även kunna rubriceras som företagsspioneri[45] alternativt spioneri[46] om den skadegörande handlingen riktar sig mot ett riksintresse.

[42] SIS handbok SIS 142 motsvarande definition med smärre redaktionella justeringar finns i SIS Dataordbok SS 011601 utgåva 4, årgång 1989.
[43] Ibid.
[44] SOU 1983:50, s.174-185.
[45] 3§ Lag om skydd för företagshemlighet (1990:409).
[46] 19 kap. 5 § BrB.

- Angrepp mot den fysiska datorn eller tillbehör.
  - Denna typ av angrepp kan dels vara av typen skadegörelse, stöld eller egenmäktigt förfarande. Om anläggningen är av vikt för samhället torde även 13 kap. BrB om allmänfarliga brott vara tillämpligt. Även 10 kap. 7 § BrB om olovligt brukande torde vara tillämpligt i vissa fall, exempelvis vid så kallad tidsstöld.

5.4.1 Bereder sig tillgång

När lagregleringen om dataintrång utformades under 1970-talet var det troligaste scenariot att någon bröt sig in i ett utrymme där en dator eller terminal förvarades och genom denna beredde sig tillgång till informationen i systemet.[47] I dagens samhälle där globala nätverk används i allt större utsträckning torde detta vara det minst troliga scenariot. Enligt 4 kap. 9c § BrB är det själva beredandet av tillgång till upptagning för automatisk databehandling som är straffbelagt, hur detta *beredande av tillgång* kan ske är inte specificerat. Man kan dock dra paralleller mellan begreppet *bereda sig tillgång till* och innebörden av begreppet *tillgripa* i 8 kap. brottsbalken. Enligt *Silvander* torde det vara så att det i grunden ”uppstår någon form av ’besittningsrubbning’ i samband med gärningsmannens förfarande”[48].

Att inte specificera exakt hur beredandet skall utföras för att vara straffbelagt är en av anledningarna till paragrafens teknikneutralitet. I dag är det troligaste scenariot antingen att en person som har tillåten fysisk access till datorn eller terminalen obehörigen bereder sig tillgång till uppgifter eller att någon utifrån genom ett datornätverk i någon form bereder sig tillgång till uppgifter. Att någon utifrån bereder sig tillgång till uppgifter genom att avlyssna såkallat röjandesignaler (RöS) är en annan möjlighet.[49]

För att som i 4 kap. 9c § BrB *bereda sig tillgång till upptagning* krävs inte att gärningsmannen de facto har tillgodogjort sig innehållet i upptagningen, eller att någon specifik effekt har uppstått som exempelvis skada. Det räcker för att straffbarhet skall föreligga att gärningsmannen har haft möjlighet att tillgodogöra sig innehållet.[50] Även indirekt tillgång såsom när en gärningsman använder uppgifterna som ett led i att få tillgång till andra uppgifter anses som dataintrång. Om någon oavsiktligt får tillgång till uppgifter för ADB upptagning föreligger ingen brottslig gärning, uppsåt krävs i alla led.[51]

[47] SOU 1992:110, s.187.
[48] Silvander, Dator- och datarelaterade förmögenhetsbrott utom borgenärsbrotten, s 213.
[49] För mer om RöS se kap. 9.1.
[50] Holmqvist m.fl., Brottsbalken en kommentar Del I studentutgåva 3, 4:49.
[51] 1 kap. 2 § BrB.

5.4.2 Ändrar, utplånar eller i register för in

Även om en gärningsman har behörighet att ta del av uppgifter för automatisk databehandling är det straffbart att ändra, utplåna eller i register föra in uppgifter om dennes behörighet inte täcker även detta förfarande.

En ändring kan antingen vara kvantitativ eller kvalitativ. En kvantitativ ändring är när mängden förändras antingen temporärt eller permanent, exempelvis genom att en gärningsman raderar eller lägger till data. En kvalitativ ändring innebär att datas integritet förändras. Även när en process för automatisk databehandling förändras på så sätt att den resulterar i en felaktig utmatning anses det vara en kvalitativ förändring.

Utplåning av upptagning för automatisk databehandling är även det kriminaliserat, detta oavsett om utplåningen är temporär exempelvis genom att gärningsmannen kopierar upptagningen för att sedan radera originalet, eller om upptagningen utplånas totalt.

Även obehörigt införande av uppgifter för automatisk databehandling i ett register är kriminaliserat. Denna gärning lades till i paragrafen i samband med att personuppgiftslagen infördes.

5.4.3 Olovligen

För att ansvar för dataintrång skall anses föreligga skall handlingen ha företagits olovligen. Detta innebär att en handling som företas med medgivande från en person som är behörig att förfoga över intresset inte är straffbar.[52] Detta blir bland annat aktuellt vid så kallade Pen- eller Redteam tester, där syftet är att testa säkerheten. Sedvanliga regler för att bestämma om samtycket är giltigt är givetvis tillämpliga även här. [53]

5.4.4 Subsidiaritet och regelkonkurrens

Enligt paragrafens första mening *Den som i annat fall än som sägs i 8 och 9 §§ olovligen…* är den subsidiär till 4 kap. 8 och 9 §§ BrB, någon ytterligare konkurrensregel finns inte. När paragrafen flyttades över till brottsbalken från Datalagen uttalades dock att eventuell konkurrens skall lösas ”enligt sedvanliga principer”. [54]

[52] Prop. 1993/94:130, s.39.
[53] För ytterligare diskussion om samtyckes ansvarsbefriande verkan rekommenderas Jareborg, Straffrättens ansvarslära.
[54] Prop. 1997/98:44, s.149.

Jareborg tar i ”Straffrättens gärningslära” upp problemen med konkurrens och subsidiaritet mellan dataintrång enligt dess tidigare placering i Datalagens 21 § och brottsbalken, även om denna exemplifiering i vissa fall är obsolet visar den på de problem som fortfarande finns efter att bestämmelsen flyttats till brottsbalken;

> *”Dataintrång innefattar ofta ett förmögenhetsbrott, såsom stöld eller trolöshet mot huvudman. Särskilt svårt att besvara är frågan när utplåning av en upptagning för automatisk databehandling också utgör skadegörelse. Olovligt brukande av en dataterminal kan vara brott enligt 8:8 eller 10:7”*[55]

[55] Jareborg, Straffrättens gärningslära, 1995, s.179.

6 Brottsbalken 4 kapitlet 8 §

6.1 Inledning

8 § Den som olovligen bereder sig tillgång till ett meddelande, som ett post- eller telebefordringsföretag förmedlar som postförsändelse eller telemeddelande, döms för brytande av post- eller telehemlighet till böter eller fängelse i högst två år.

(Lag 1993:601)

6.1.1 Olovligen bereder sig tillgång

Då både begreppen *olovligen* och *bereder sig tillgång* analyserats uttömmande under 5.4.1 och 5.4.3 kommer jag ej att ytterligare beröra dessa här.

6.2 Telemeddelande

I lagen om elektronisk kommunikation[56] anges att med telemeddelande avses bland annat data eller annan information som förmedlas med hjälp av radio eller genom ljus eller elektromagnetiska svängningar i en särskilt anordnad ledare.

6.3 Datatransmission

I ljuset av definitionen av telemeddelande står det klart att även datatransmissioner täcks in av 4 kap. 8 § BrB. Något som också uttalades av OSK i deras utredning, ”Tappning av datatransmission från televerkets ledningar kan bestraffas jämlikt 4 kap. 8 § BrB, men om ledningarna tillhör registerföraren själv eller åtminstone disponeras uteslutande av honom själv kan meddelandet knappast sägas bli ’befordrat genom allmän befordringsanstalt’ ”.[57] Om meddelandet inte är befordrat genom allmän befordringsanstalt torde istället bestämmelsen om dataintrång i 4 kap. 9c § BrB bli tillämplig.[58]

[56] 6 kap. 19 § 3st, Lag om elektronisk kommunikation (2003:389).
[57] SOU 1972:47, s.96.
[58] SOU 1992:110, s.179.

På samma sätt som i 4 kap. 9c § BrB är det inte nödvändigt att gärningsmannen har tagit del av telemeddelandet för att straffansvar skall anses föreligga, det är tillräckligt att gärningsmannen olovligen har berett sig tillgång till meddelandet.

När gärningen rör ett telemeddelande och inte en postförsändelse bör brottsbenämningen brytande av telehemlighet användas.[59]

6.4 Tidsram

4 kap. 8 § BrB är tillämpligt så länge som meddelandet är under befordran, det vill säga från det att meddelandet avlämnats tills dess utlämnande.[60] För datakommunikationer är detta intervall oftast mycket kort, däremot kan ett flertal kopior s.k. *cache-kopior*[61] finnas kvar i olika delar av systemet under längre tid. Ett annat exempel är e-mail meddelande som kan *förvaras* under flera dygn i sändande och mottagande e-mail servers, utan att meddelandet för den del torde anses som utlämnat till mottagaren.

6.5 Undantag

4 kap. 8 § BrB kriminaliserar som tidigare sagt *avlyssning* under vissa förutsättningar. Ett undantag från förbudet att bereda sig tillgång till telemeddelande som befordras av telebefordringsföretag via radio finns dock i 6 kap. 17 § 3st. EkomL. Detta undantag behandlas utförligt i uppsatsens 9:e kapitel.

[59] Holmqvist m.fl., Brottsbalken en kommentar Del I studentutgåva upplaga 3, 4:36.
[60] SOU 1992:110, s.117.
[61] Cache-kopior är kopior av data som lagras i olika delar av ett nätverk för att öka snabbheten i överföringen. Genom att lagra information som redan har hämtats från en annan del av nätverket lokalt behöver man inte hämta in informationen på nytt, utan kan leverera den redan cachade informationen. Detta är speciellt viktigt på Internet, där nätverket snabbt skulle nå sin maxkapacitet om caching inte skedde.

7 Brottsbalken 4 kapitlet 9 §

7.1 Inledning

9 § Den som, utan att fall är för handen som i 8 § sägs, olovligen bryter brev eller telegram eller eljest bereder sig tillgång till något som förvaras förseglat eller under lås eller eljest tillslutet, dömes för intrång i förvar till böter eller fängelse i högst två år.

(Lag 1962:700)

7.2 Skyddsobjekt

Skyddsobjektet i 4 kap. 9 § BrB är ”brev, telegram eller något som förvaras tillslutet”. Till skillnad från 4 kap. 8 § BrB finns ingen inbyggd begränsning i tid för paragrafens tillämplighet, så länge ”något” förvaras förseglat, låst eller eljest tillslutet är paragrafen tillämplig. Kravet på förvaring torde dock medföra att exempelvis telemeddelande som inte förvaras faller utanför tillämpningsområdet.

7.3 Förseglat, under lås, eljest tillslutet

Paragrafen kriminaliserar gärningen att bereda sig tillgång till något som förvaras förseglat, under lås eller eljest tillslutet. Vad detta innebär i IT-världen har inte blivit utrett i någon större utsträckning. Klart är att om någon öppnar en låda eller dylikt där exempelvis disketter eller hårddiskar förvaras gör sig skyldig till intrång i förvar.[62] Frågan återstår dock om data som exempelvis är skyddat av kryptering eller lösenord kan anses som under lås eller eljest tillslutet. OSK:s betänkande[63] tog upp frågan om intrång i förvar möjligen skulle föreligga om någon beredde sig tillgång till en datamaskins minne, man betvivlade dock att så var fallet med tanke på legalitetsprincipen och den analogi mellan förvar och datorns minne som man då skulle vara tvungen att göra.[64] Silvander[65] gör motsvarande bedömning av paragrafens räckvidd när det gäller data, han menar att för att paragrafen skall vara tillämplig måste upptagningen vara inlåst rent fysiskt, att enbart kryptera eller lösenordsskydda data skulle enligt detta ej vara tillräckligt.

[62] SOU 1992:110, s.178.
[63] SOU 1972:47.
[64] SOU 1992:110, s.178.
[65] Silvander, Dator- och datarelaterade förmögenhetsbrott utom borgenärsbrotten, s 301.

8 Brottsbalken 4 kapitlet 9b, 10 §§

8.1 Inledning

10 § För försök, förberedelse eller stämpling till människorov, människohandel för sexuella ändamål, olaga frihetsberövande eller försättande i nödläge och för underlåtenhet att avslöja sådant brott döms till ansvar enligt vad som sägs i 23 kap. Detsamma gäller för försök eller förberedelse till olaga tvång som är grovt eller till dataintrång som om det fullbordats inte skulle ha varit att anse som ringa.

Lag (2002:436)

Försök och förberedelse till dataintrång är enbart straffbart om brottet om det fullbordats inte skulle ansetts som ringa. Denna paragraf lades till brottsbalken samtidigt som Datalagens 21 § flyttades dit. Bestämmelsens del om dataintrång var tidigare intagen i Datalagens 21 § andra stycke, den infördes efter påpekande i ett remissvar på OSK:s betänkande från den juridiska fakulteten vid Stockholms Universitet angående de stora värden i form av information som finns att skydda inom IT-världen.[66] Propositionen ger ingen ytterligare information om hur bestämmelsen skall tillämpas, utan hänvisar enbart till Datastraffutredningens[67] och Datalagkommitténs[68] utredningar.

Ansvar för försök till gärningar som är kriminaliserade redan på försöksstadiet regleras i 23 kap. 1 § BrB.

9 b § Om någon anbringar tekniskt hjälpmedel med uppsåt att bryta telehemlighet på sätt som sägs i 8 § eller att utföra brott som sägs i 9 a §, dömes för förberedelse till sådant brott till böter eller fängelse i högst två år, om han ej är förfallen till ansvar för fullbordat brott.

Lag (1975:239)

Vad gäller brytande av post och telehemlighet är enbart förberedelse, inte försök, kriminaliserat.

8.2 Försök till dataintrång

Ansvar för försök föreligger om gärningsmannen påbörjat utförandet av brottet och det antingen förelegat fara för brottets fullbordan, eller om denna fara endast varit utesluten på grund av tillfälliga omständigheter.

[66] SOU 1992:110, s.199 samt prop. 1973:22, s.68.
[67] SOU 1992:110.
[68] SOU 1997:39.

Lagstiftarens tanke har varit att endast försök som är värda att tas på allvar skall vara straffbara. DSU ansåg att detta tänkande torde revideras något när det gäller brott i IT-miljö, detta på grund av de stora kostnader som kan drabba den som utsätts för försök till brott. Kostnader som kan uppstå vid kontroll av system i syfte att fastställa om eller vilken skada gärningsmannen åsamkat systemet.[69] Man ansåg dock inte att det fanns ett behov av att kriminalisera försök till ringa dataintrång.[70]

8.3 Förberedelse till brytande av telehemlighet

För att ansvar för förberedelse till brytande av telehemlighet skall föreligga krävs att ”någon anbringar tekniskt hjälpmedel med uppsåt att bryta telehemlighet”[71]. Detta krav på teknisk apparatur har sin grund i motiven till bestämmelsen, man påpekade att ”angrepp på annans integritet med teknisk apparatur typiskt sett försiggår i olika moment. Först anbringas den och sedan används den.”[72] Man ansåg vidare att det ligger i sakens natur att det kan bli svårt att styrka att apparaturen verkligen har använts för att avlyssna när man påträffar dylik apparatur ”under sådana omständigheter att man kan utgå från att anbringaren haft uppsåt att i hemlighet avlyssna” [73], man torde därför kunna utgå ifrån att ”den har använts för detta ändamål”[74].

Datastraffutredningen ansåg att bestämmelsen ”kännetecknas av en nära anpassning till de förutsättningar ny teknik för med sig”[75] detta då den dels är teknikneutral och dels då det i samband med IT-brott ofta inte finns bevisunderlag som tillräckligt styrker ”hur långt ett angrepp eller intrång fortskridit”[76].

8.4 Förberedelse till dataintrång

Ansvar för förberedelse till brott stadgas i 23 kap. 2 § BrB. I och med ändringen som infördes i 23 kap. 2 § BrB den 1 juli 2001 täcks numera även IT-brottsverktyg in. Den tidigare uppräkningen av gärningar och objekt som konstituerade förberedelse ersattes av en mer generell bestämmelse som tar sikte på ”något som är särskilt ägnat åt att användas som hjälpmedel vid brott”[77]. I förarbetena tas som exempel särskilt upp datorprogram och annan mjukvara.[78]

[69] SOU 1992:110, s 199.
[70] Ibid.
[71] 4 kap. 9b § BrB.
[72] SOU 1992:110, s 199.
[73] Ibid.
[74] Ibid.
[75] SOU 1992:110, s 200.
[76] Ibid.
[77] 23 kap. 2 § BrB.
[78] Prop. 2000/2001:85, s 50.

Även sammanställningar av koder och annan information kan utgöra ett hjälpmedel i paragrafens mening, dock fordras då att informationen är nedtecknad eller lagrats på annat sätt, detta då ren kunskap aldrig kan anses som ett hjälpmedel för att begå brott.[79]

[79] Prop. 2000/2001:85, s.50-51.

9 Trådlös kommunikation – Avlyssning

I enlighet med 2 kap. 6 § RF är varje medborgare skyddad gentemot det allmänna vad avser hemlig avlyssning, upptagning av telefonsamtal eller andra förtroliga meddelanden. Den enskilde är dock inte skyddad gentemot annan än statlig avlyssning vad avser etersändningar, den folkrättsliga principen om den ”fria etern” är allenarådande.[80] I 6 kapitlet 17 § i Lag om Elektronisk kommunikation som trädde i kraft 25 juli 2003 stadgas just att avlyssning av eterkommunikation av enskild med hjälp av radiomottagare inte är brottsligt.[81] Med hänsyn till principen om *lex specialis derogat legi generali* är det således inte olagligt att avlyssna etertrafik som exempelvis trådlös datorkommunikation. Detta oavsett om det är ett telebefordringsföretag eller ett privat radionätverk, och täcker därmed in både 4 kap. 8 § BrB och 4 kap. 9c § BrB.[82] Denna lucka i lagen är något som även Datastraffutredningen uppmärksammade i sin utredning.[83]
Det finns dock en begränsning i hur man får handskas med avlyssnade telemeddelande, det är aldrig tillåtet att sprida den avlyssnade informationen vidare till tredjeman enligt 6 kap. 23 § EkomL om denna inte från början uppenbarligen var avsedd för allmänheten.[84]

9.1 Röjande signaler – RöS

RöS kallas signaler som naturligt och oavsiktligt uppstår i teknisk utrustning. Exempel är elektromagnetiska fält från monitorer, datakablage och strömkablage. Det är praktiskt möjligt att med hjälp av särskild utrustning avlyssna de operationer som en dator utför genom att läsa av förändringar i det magnetiska fältet som uppstår genom exempelvis återmatning i strömförsörjningskablar. Detta kan göras på förhållandevis stora avstånd.

I svensk lagstiftning finns det i dag inget straffstadgande som skulle kunna vara tillämpbart på denna typ av avlyssning. Röjande signaler kan knappast anses vara kommunikation vare sig i lagens mening eller dagligt tal. Det är inte riktade mot en definierbar mottagare och utnyttjar inte heller något särskilt anordnat kommunikationsnät. Detta är något som det har riktats skarp kritik mot, bland annat från Datastraffutredningen.[85]

[80] SOU 1991:107, s 49 ff. samt SOU 1992:70, s 81 ff.
[81] Lag om Elektronisk kommunikation (2003:389).
[82] Prop. 2003/04:164. s 11.
[83] SOU 1992:110, s 196.
[84] Lag om Elektronisk kommunikation (2003:389).
[85] SOU 1992:110, s 190 ff.

10 Sammanställning av gällande lagrum

4:8 § BrB	**4:9c § BrB**	**6:17 § EkomL**	**4:9 § BrB**
Den som olovligen bereder sig tillgång till meddelande	Den som olovligen bereder sig tillgång till upptagning för ADB	Den som med radiomottagare bereder sig tillgång till etersändning	Den som bryter försegling, lås eller tillslutning och olovligen bereder sig tillgång till meddelande .
Döms till böter eller fängelse i högst två år	Döms till böter eller fängelse i högst två år	Begår ej brott	Döms till böter eller fängelse i högst två år

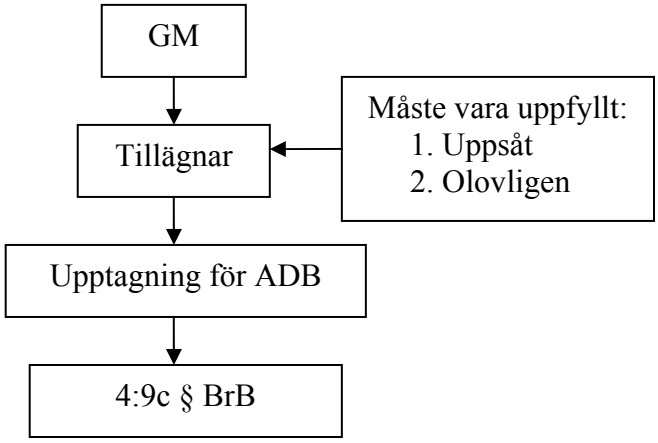
4:9b § BrB	**4:10 § BrB**
Den som anbringar tekniskt hjälpmedel med uppsåt att bryta telehemlighet	Den som försöker eller förbereder icke ringa dataintrång
Döms till böter eller fängelse i högst två år	Döms till böter eller fängelse i högst två år

11 Typfall

11.1 Inledning

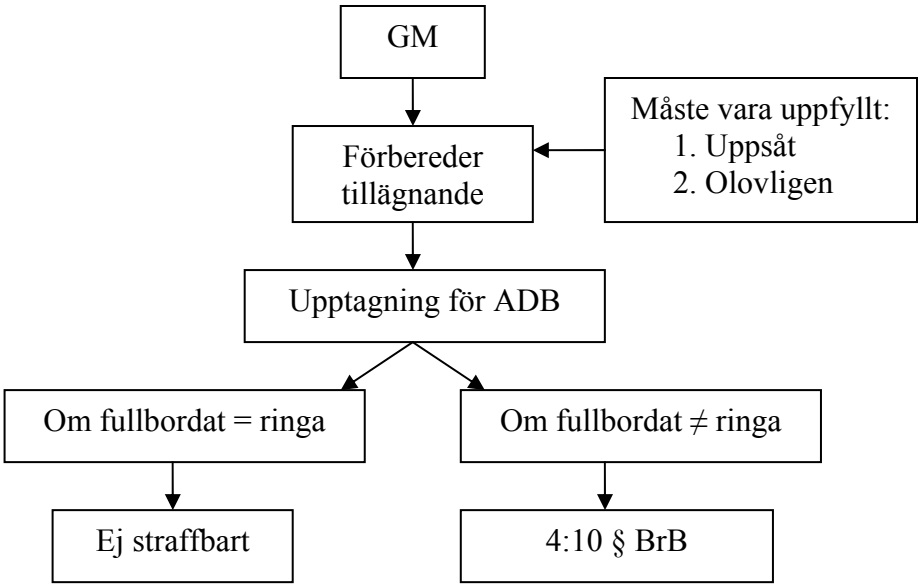
I syfte att belysa de olika lagrummens tillämpning och räckvidd vid olika typer av gärningar presenterar jag nedan ett antal typfall. Typfallen kan ses som generella händelseförlopp vid olika typer av dator- och datarelaterade gärningar.

11.2 Hacker



Gärningsmannen hackar sig in i ett datanätverk genom att koppla upp sig via en extern uppkoppling och därifrån ta sig in i en dator. Gärningsmannen anses genom detta förfarande ha olovligen tillägnat sig upptagning för ADB, detta oavsett om han tagit del av information eller data i den hackade datorn eller ej.

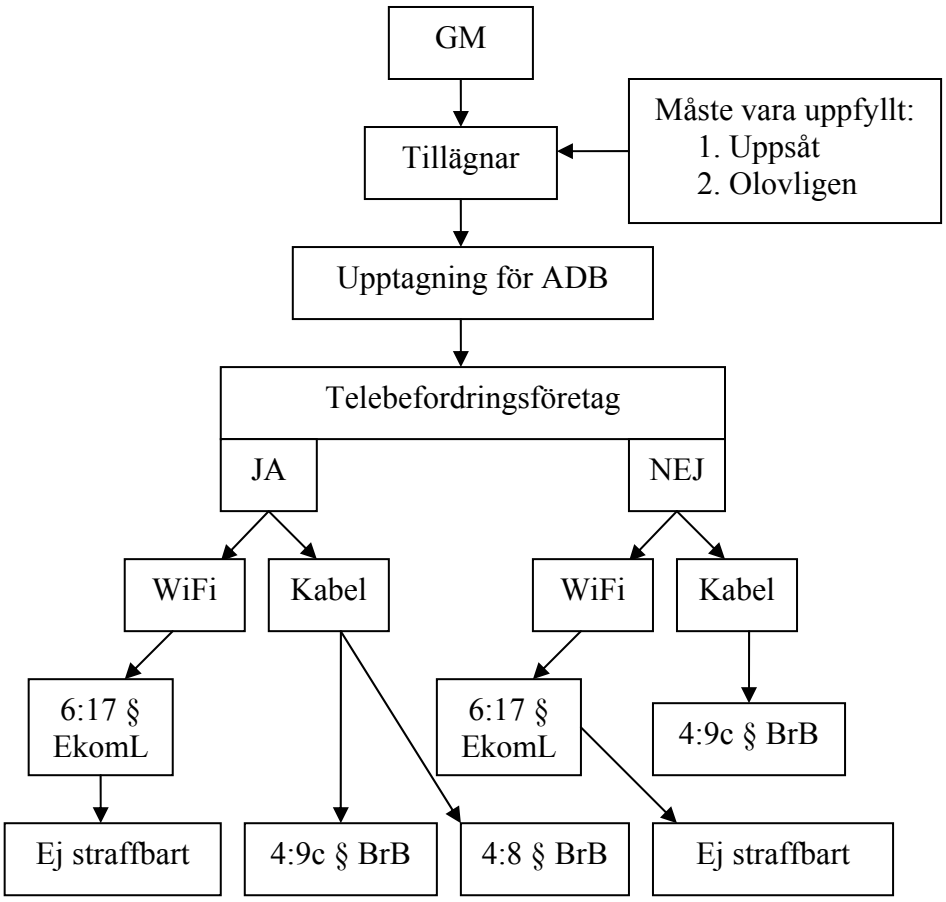
11.3 Portscan



Gärningsmannen sänder via sin dator ut ett stort antal ping- eller ICMP-paket till en eller flera IP-adresser i syfte att kartlägga de datorer som svarar. Om handlingen syftar till att förbereda dataintrång och detta dataintrång om fullbordat ej skulle ansets som ringa, torde gärningsmannen göra sig skyldig till förberedelse till dataintrång. Om gärningen ej är att anses som förberedelse till dataintrång är den ej kriminaliserad.

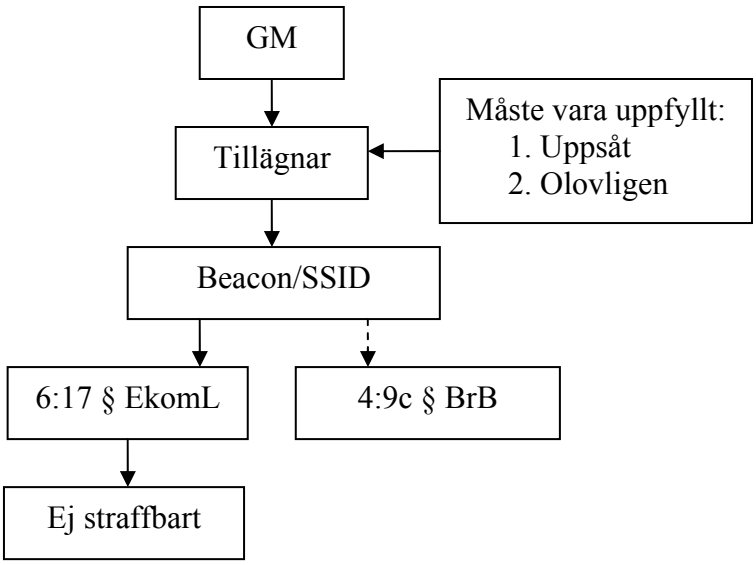
Det torde enligt mig vara mycket svårt att enbart baserat på att gärningsmannen utfört portscanning av ett antal måldatorer fastställa bortom rimligt tvivel att det är förberedelse till dataintrång. Ytterligare stödbevisning torde krävas.

11.4 Sniffing



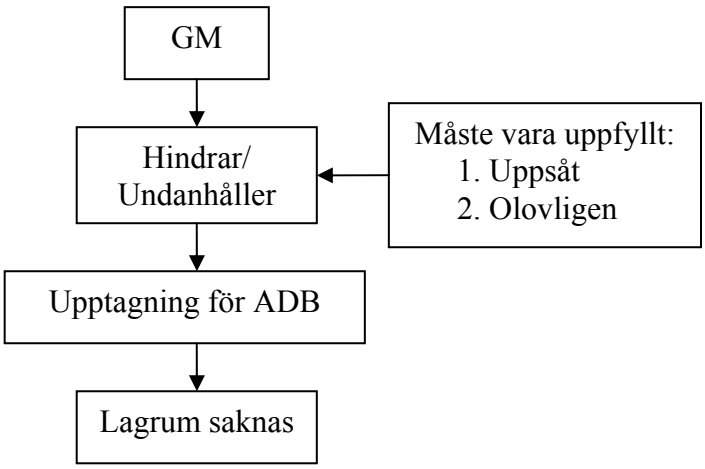
Gärningsmannen tillägnar sig upptagning för ADB genom att avlyssna nätverkstrafik. Beroende på om trafiken som avlyssnas befordras av ett teleförmedlingsföretag, eller i ett privat nätverk kan 4 kap. 8 § BrB bli tillämplig. När det gäller sniffing av trådlösa nätverk (WiFi) torde detta inte vara kriminaliserat med tanke på stadgandena i 6 kap. 17 § EkomL.

11.5 Wardriving



Gärningsmannen tillägnar sig signaler från en AP genom att avlyssna radiosignaler. Signalerna (Beacon) torde i sig inte anses som upptagning för automatisk databehandling och faller därmed utanför 4 kap. 9c § BrB tillämpningsområde. Även om signalerna skulle anses som upptagning för automatisk databehandling så är 6 kap. 17 § EkomL tillämplig varvid förfarandet att mottaga signalerna inte är otillåtet. Däremot kan vidarespridande av dessa signaler vara olovligt.

11.6 DoS (DDoS)



Gärningsmannen hindrar eller undanhåller upptagning för automatisk databehandling genom att förhindra kommunikation mellan klient och server. Då gärningen inte innebär beredande av tillgång till upptagning för automatisk databehandling och då upptagningen inte på något sätt ändras eller förstörs kan gärningen varken anses som dataintrång eller skadegörelse. Gärningen torde således ej vara straffbar.

12 Statistik

12.1 Nationell

Brottsförebyggande rådet (BRÅ) för kontinuerlig statistik över begångna brott i Sverige. Deras statistiska underlag lider dock av vissa brister exempelvis saknas vissa år, samt att fram till året 1999 räknades både brott mot Datalagens 21 § och 22 § samman i statistiken. Jag fann vidare vissa diskrepanser vid jämförelsen mellan de statistiska uppgifterna i BRÅ:s rapport 2000:2 och statistiken som presenteras på deras webbsida.[86] Detta faktum har medfört att jag har lagt störst tilltro till de uppgifter som jag har fått från riksdagens utredningstjänst[87], och mindre tilltro till de uppgifter Brottsförebyggande rådet har publicerat. Vid eventuella diskrepanser har jag använt uppgifterna från riksdagens utredningstjänst.

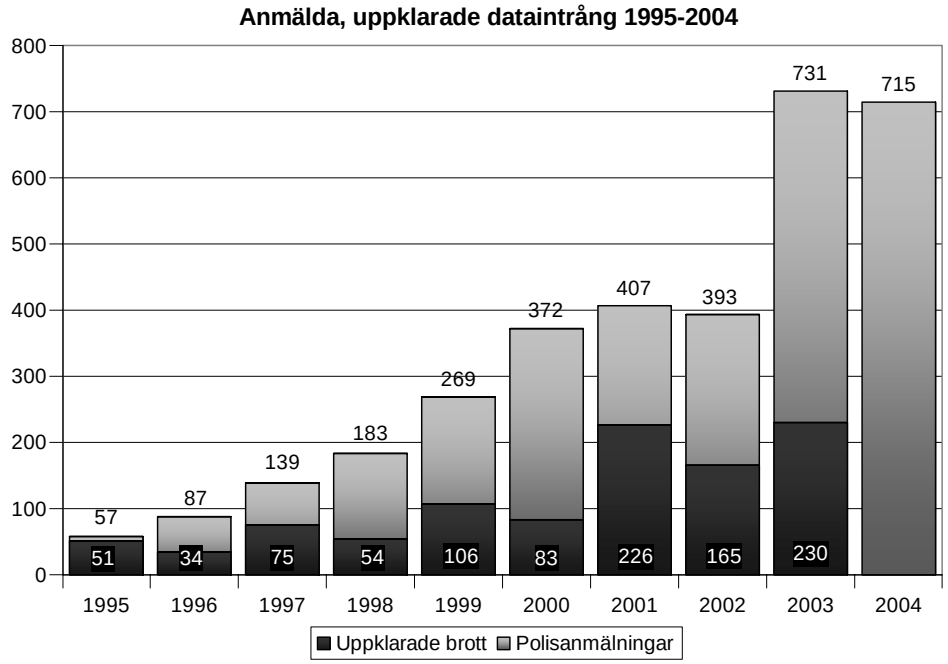
Den statistik som finns bryter inte ned brottet dataintrång i gärningar, dvs. det sätt på vilket intrånget har skett. Det är därför, utifrån statistiken, inte möjligt att redogöra för vilka olika gärningar t.ex. datavirus, olovlig åtkomst eller stöld av information som har konstituerat brottet dataintrång.[88] Inte heller återger statistiken vilken typ av anmälare det är fråga om t.ex. privatperson, myndighet eller företag. Detta är något som BRÅ under de senaste åren har uppmärksammat och ser som ett problem, man har därför utarbetat ett förslag som skulle innebära en utökad möjlighet att märka brottsfallen, detta nya system kan dock tas i drift tidigast 2006 enligt Barbro Loogna tillförordnad chef på BRÅ:s statistikenhet.[89]

Enligt Brottsförebyggande rådet är benägenheten att anmäla IT-brottslighet låg. I deras rapport 2000:2 kom man fram till att endast 12 procent av de tillfrågade företagen rapporterade IT-incidenter (om virus-incidenter exkluderas stiger anmälnings viljan till 35%). Detta leder till att statistikens riktighet kan ifrågasättas. Ett antal olika anledningar till varför företagen inte rapporterar IT-incidenter angavs, en av de mest framträdande var rädslan för negativ publicitet.[90]

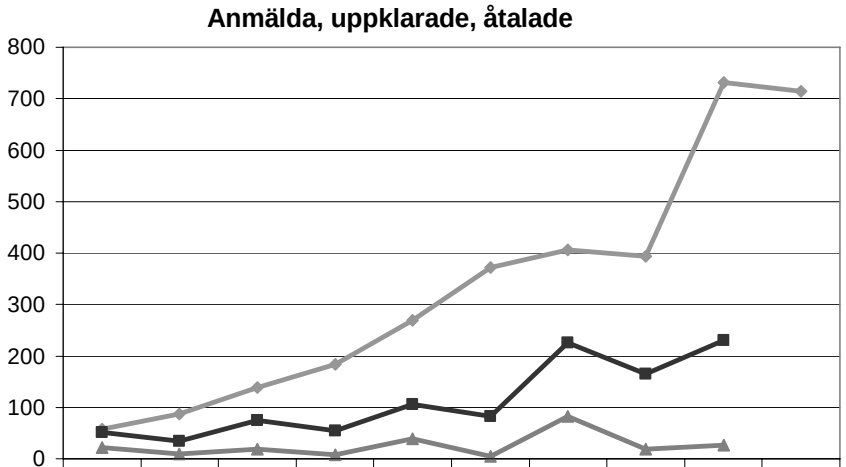
Då data för anmälda och uppklarade brott publiceras årsvis, är data för uppklarade brott under 2004 ej inkluderade.

---

[86] Vid jämförelser mellan olika tabellutdrag via www.bra.se samt BRÅ rapporten 2000:2 IT-relaterad brottslighet, upptäcktes att under samma år varierade siffrorna på både anmälda och uppklarade dataintrång med mellan ca 2 till 200 fall beroende på år. Denna diskrepans har rapporterats till BRÅ.
[87] Riksdagens utredningstjänst, PM Dataintrång, Dnr 2004:2450, 2004-12-20.
[88] Ibid.
[89] Carlsson T, Svensk polis klarar inte internationella IT-brott, NyTeknik 030430.
[90] BRÅ rapport 2000:2, IT-relaterad brottslighet, s.43.



Källa riksdagens utredningstjänst samt Brottsförebyggande rådet[91]



	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004
Polisanmälningar	57	87	139	183	269	372	407	393	731	715
Uppklarade brott	51	34	75	54	106	83	226	165	230	
åtal	22	10	19	8	39	5	83	19	26	

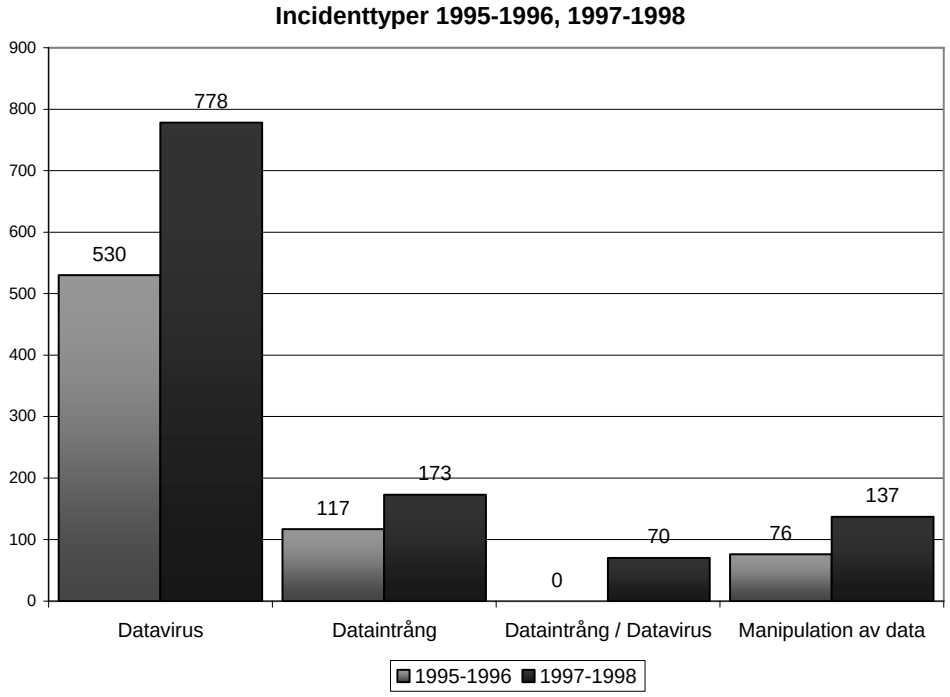
Källa riksdagens utredningstjänst samt Brottsförebyggande rådet[92]

Av statistiken kan man generellt säga att; antalet dataintrång stadigt ökar, antalet uppklarade brott ökar (dock ej i samma takt), samt att antalet åtal ligger kvar på i stort sätt samma nivå som för åtta år sedan.

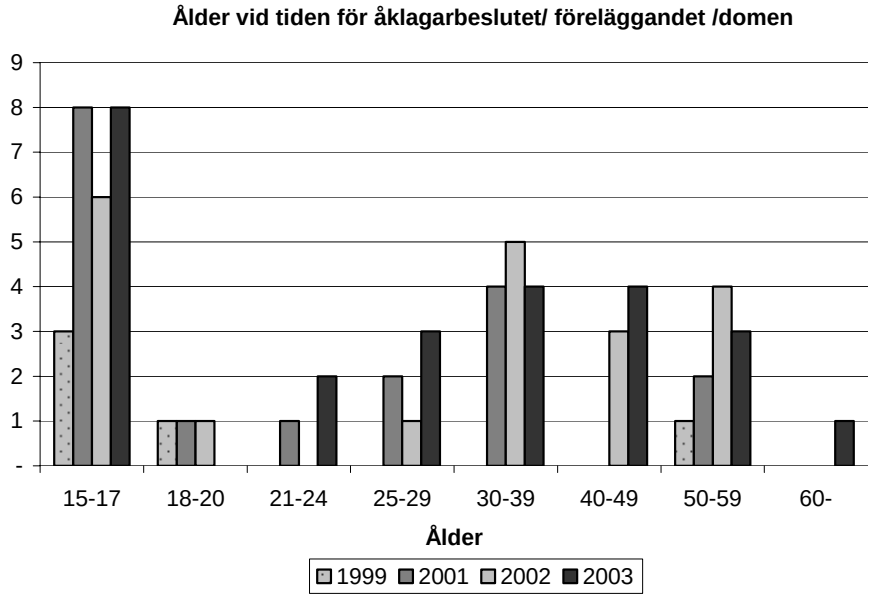
Att polisen har fått ökade resurser och kompetens att utreda IT-brott har med andra ord inte lett till fler åtal, vad detta beror på är svårt att säkert säga.

[91] http://www.bra.se samt riksdagens utredningstjänst, PM Dataintrång, Dnr 2004:2450, 2004-12-20.
[92] Ibid.

En möjlig orsak kan vara att åklagare och domstolarna fortfarande inte har tillräcklig kompetens på detta område, varvid strafföreläggande är enklare att utmäta än att föra saken till prövning i en allmän domstol.



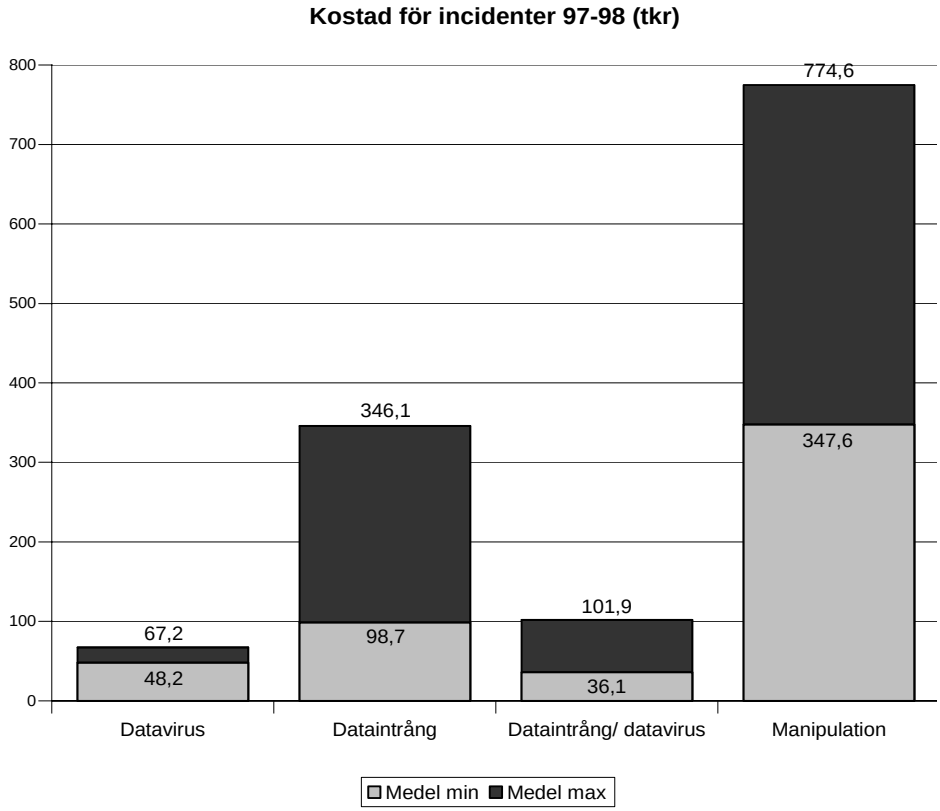
Källa Brottsförebyggande rådet[93]



Källa Brottsförebyggande rådet[94]

Dataintrång begås av förhållandevis unga gärningsmän, något som påverkar påföljden vid straffmätning.

[93] BRÅ rapport 2000:2, IT-relaterad brottslighet, s.22.
[94] http://www.bra.se



Källa Brottsförebyggande rådet[95]

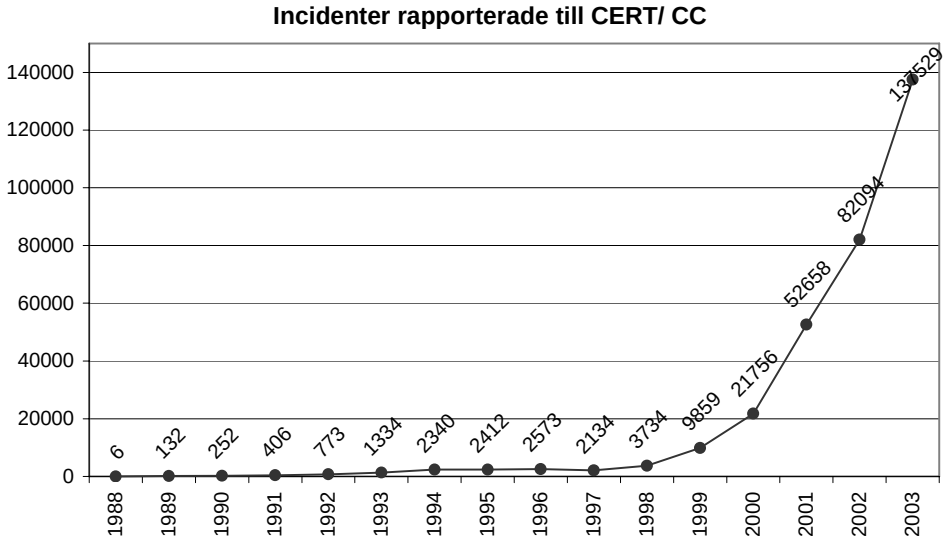
Enligt Lars Emanuelsson Korsell vid BRÅ är de uppgifter som ligger till grund för uppskattningen av kostnaderna för incidenter under 1997-1998 mycket osäkra.[96]

12.2 Internationell

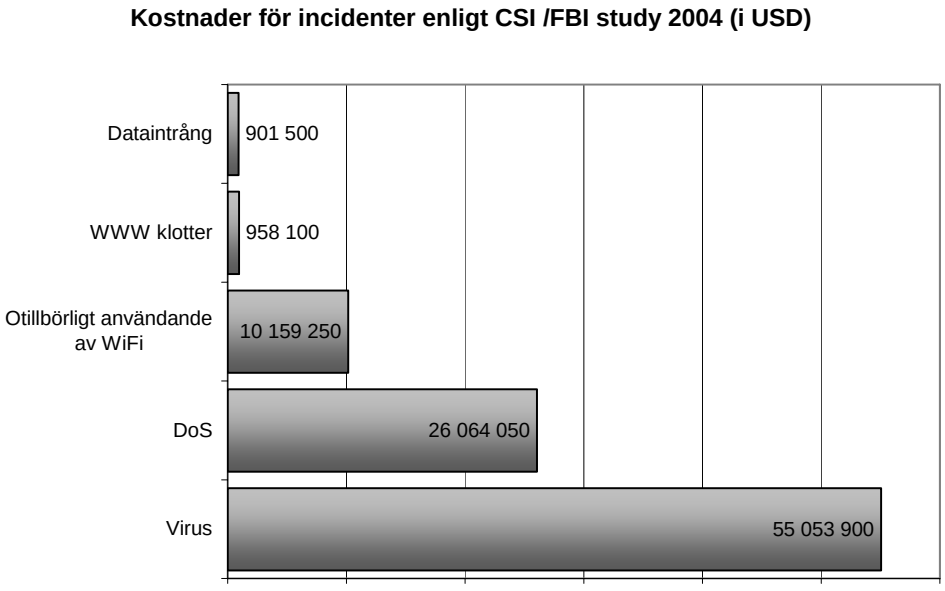
Internationellt förs statistik av både privata och statliga aktörer, revisionsbyråer såsom *Price Waterhouse Coopers* och *Computer Security Institute* och statliga aktörer såsom *CERT/CC* och *FBI* publicerar mer eller mindre årlig statistik sedan ett antal år tillbaka.
Jag har valt att ta med ett urval av denna internationella statistik då den visar att datorrelaterad brottslighet är ett ökande globalt problem.

Även denna statistik lider av benägenheten hos dem som utsatts för IT-incidenter att inte polisanmäla eller rapportera dessa till exempelvis *CERT/CC*, varvid även denna statistiks riktighet kan ifrågasättas.

[95] BRÅ rapport 2000:2, IT-relaterad brottslighet, s.22.
[96] Riksdagens utredningstjänst, PM Dataintrång, Dnr 2004:2450, 2004-12-20.



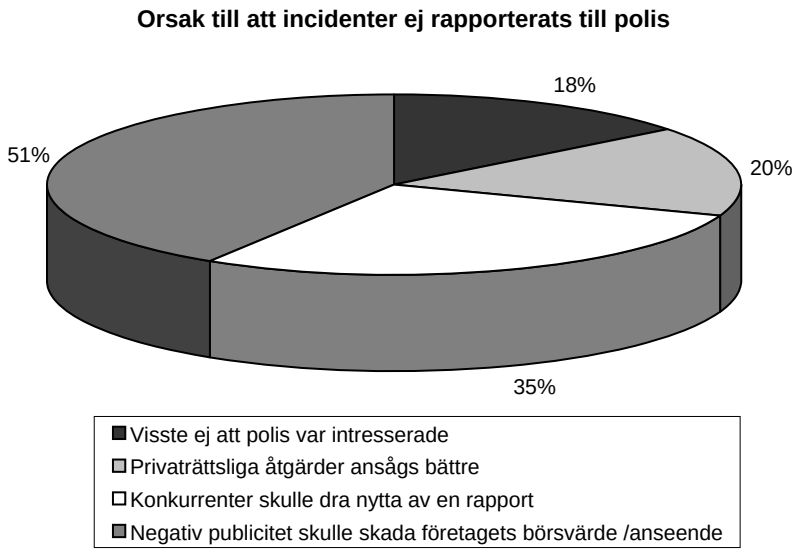
Källa CERT/CC[97]



Källa CSI/FBI Computer Crime and Security Survey[98]

Även internationellt sett har dataintrången ökat de senaste åren. En intressant observation är att kostnaden för dataintrång är ungefär 61 gånger mindre än för virusangrepp. Detta trots att det finns mycket bra skydd mot datavirus på marknaden i dag.

[97] http://www.cert.org/stats/cert_stats.html
[98] 2004 CSI/FBI Computer Crime and Security Survey.



Källa CSI/FBI Computer Crime and Security Survey[99]

Även utomlands är viljan att anmäla IT-incidenter låg, Här är det dock tydligare än i BRÅ rapporten[100] att anledningen till den låga anmälningsviljan är det tänkta hot mot företagets ekonomiska värden som en anmälan skulle kunna medföra.

[99] 2004 CSI/FBI Computer Crime and Security Survey.
[100] BRÅ rapport 2000:2, IT-relaterad brottslighet.

13 Praxis

13.1 Inledning

Då relativt få fall av dataintrång både anmäls och leder till åtal är antalet rättsfall begränsat. Då denna uppsats främst är inriktad på externa dataintrång har jag valt att främst analysera dylika rättsfall, jag har dock tagit med ett fåtal fall av interna dataintrång detta för att få en bas för komparation.

Av de åtal som leder till fällande domar är det ytterst få som överklagas, vad detta beror på går ej att utröna. Detta leder till problem vid värdering av vilken vikt man kan lägga vid gällande praxis.

13.2 Interna

Av de fall av dataintrång som polisanmäls är andelen så kallade interna dataintrång klart överrepresenterade. Interna dataintrång sker ofta inom myndigheter, flera uppmärksammade rättsfall har under åren rört personal inom rättsväsendet, landstingen och försäkringskassorna. Att just dessa är överrepresenterade i statistiken kan bland annat förklaras med att de kontrollsystem som finns verkligen fungerar. Vidare torde det vara så att myndigheter i allmänhet är mer benägna att anmäla dataintrång än företag och privatpersoner.

Nedan presenteras tre fall av interna dataintrång, dessa tre rättsfall är enligt min mening representativa för det stora flertalet interna dataintrång.

13.2.1 Polisen[101]

En polisman KW gjorde slagningar på vissa personer i polisens olika ADB register i syfte att kontrollera om dessa personer fanns upptagna i dessa register. Resultatet från slagningarna utlämnades sedan till en annan person (PF), som använde dessa i utförandet av vissa säkerhetstjänster i ett företag där PF och KW:s hustru var firmatecknare. KW erkände slagningarna, men bestred att slagningarna inte hade samband med tjänsten som kriminalinspektör och att han skulle ha lämnat ut uppgifterna till PF.

Tingsrätten fann det utom tvivel att KW genomfört slagningarna som åklagaren gjort gällande. Det faktum att en lista med de personer som KW enligt loggarna gjort slagningar på också påträffats hos PF medförde att tingsrätten fann att åtalet även i detta avseende skulle anses som styrkt.

[101] Stockholms tingsrätt B 7618-00, 2002-11-21.

Frågan kvarstod då om slagningarna gjorts i samband med fullgörande av KW:s arbetsuppgifter. Tingsrätten besvarade denna fråga på följande sätt; ”Redan det förhållandet att KW lämnat ut informationen till PF och att denne använt sig av den för att fullgöra vissa uppdrag talar med viss styrka för att KW också inhämtat informationen i annat syfte än att fullgöra sina uppgifter”[102] KW ansågs därmed ha ”olovligen berett sig tillgång till polisens ADB-register och har därigenom gjort sig skyldig till dataintrång”[103]. Att KW i stor omfattning hämtat och lämnat ut uppgifter ur polisens ADB-system var något som tingsrätten ansåg medförde att dataintrånget skulle anses vara av allvarligt beskaffenhet.
Då KW även dömdes för brott mot tystnadsplikt samt tjänstefel är det omöjligt att isolera påföljden för dataintrånget, den totala påföljden blev villkorlig dom samt etthundra dagsböter à trettio kronor. Enligt tingsrätten som även fick medhåll av hovrätten[104] var brotten inte av sådan art och straffvärdet inte sådant att annan påföljd än fängelse var uteslutet.

13.2.2 Arrestvakten[105]

En arrestvakt som hade behörighet att göra slagningar i polisens UTS 1 och 2 register hade hämtat ut uppgifter angående sig själv och två andra personer, samt de två sistnämnda personernas bilar åtalades för tjänstefel alternativt dataintrång. Genom att göra slagningar i registren ansåg tingsrätten att arrestvakten beredde sig tillgång till upptagningar till automatisk databehandling.

Enligt tingsrätten stod det ostridigt att slagningarna i registren inte hade samband med utövande av hans tjänst, varvid ansvar för tjänstefel ej kunde anses föreligga.

Arrestvakten hade fått utbildning i hur slagningar i registren fick ske, bland annat hade meddelats att ”man inte fick slå på sig själv och att man inte fick göra slagningar som inte hade med tjänsten att göra”[106]. Detta faktum medförde enligt tingsrätten att ”han insåg att slagningarna gjordes olovligen”[107]. Tingsrätten dömde därför mannen för dataintrång och påföljden bestämdes till trettio dagsböter à etthundra kronor.

13.2.3 Socialsekreteraren[108]

LG, en socialsekreterare, åtalades 2002 för dataintrång bestående av att hon genom att öppna en personakt i socialförvaltningens datasystem för individ-

[102] Stockholms tingsrätt B7618-00, 2002-11-21, s.13-14.
[103] Ibid.
[104] Svea hovrätt B10958-02, 2003-09-01.
[105] Eskilstuna tingsrätt B506-02, 2002-04-16.
[106] Ibid, s.5.
[107] Ibid, s.6.
[108] Katrineholms tingsrätt B61-02, 2002-06-12.

och familjeplacering vid cirka 65 tillfällen berett sig tillgång till upptagning för automatisk databehandling.

LG bestred ansvar, men erkände att hon vid högst tio tillfällen berett sig tillgång till registret utan att detta krävts eller haft samband med hennes tjänsteutövning. LG hävdade vidare att hon skulle gå fri från ansvar på grund av straffrättsvillfarelse. Enligt LG fanns hon ej vid sin dator vid 24 av de tillfällen åklagaren hävdat att akterna öppnats av henne, samt att då hennes lösenord fanns skrivet på en lapp bredvid datorn någon annan kunde ha utnyttjat hennes login-uppgifter när hon ej var där.

Tingsrätten fann att LG:s påstående om att någon annan skulle ha utnyttjat hennes användarnamn och lösenord framstod som uppenbart osannolikt och att det därmed skulle lämnas utan avseende. Man fann därmed att det var styrkt att det var LG som öppnat akten vid 65 tillfällen utan samband med tjänsteutövning på det sätt som den systemlog som åberopats som bevis utvisade.

LG var behörig att ta del av uppgifterna om detta behövdes för hennes tjänsteutövning, i detta fall fann dock tingsrätten att så ej var fallet. Genom att LG berett sig tillgång till uppgifterna av privata skäl fann tingsrätten att LG handlat olovligen, varvid förutsättningarna för ansvar för dataintrång förelåg. Tingsrätten gjorde även bedömningen att LG haft uppsåt att olovligen ta del av uppgifterna då det måste ha stått klart för henne att hon inte fick ta del av uppgifterna utanför tjänsteutövningen för privata skäl.

Angående rättsvillfarelsen fann tingsrätten att LG inte kunde frikännas från ansvar på denna grund. Man beaktade däremot den ”allmänna nonchalans beträffande det interna iakttagandet av sekretesskydd och skydd mot dataintrång”[109] som synes ha förekommit på socialförvaltningen. Detta ledde till att påföljden bestämdes till ”ett förhållandevis lågt dagsbotsstraff”[110] trots att det rörde sig om ”ett stort antal tillfällen under relativt lång tid”[111].

LG överklagade till Svea hovrätt[112] som uttalade att LG måste ha insett, på grund av sitt arbete som socialsekreterare och då hon var utbildad socionom att ”hon inte hade rätt att utom tjänsteutövningen och av privata skäl ta del av sekretessbelagda uppgifter i datasystemet”[113]. Man ansåg därmed att hon med uppsåt handlat olovligen och fastställde därför tingsrättens dom.

[109] Ibid, s.4-5.
[110] Ibid, s.5.
[111] Ibid, s.5.
[112] Svea hovrätt B7095-02, 2003-12-16.
[113] Ibid, s.4.

13.3 Externa

Enligt statistik från bland annat BRÅ ökar antalet externa dataintrång stadigt.[114] Vad som är anmärkningsvärt är att antalet fällande domar inte ökar i samma utsträckning. Vid externa dataintrång är det av förklarliga skäl svårare att spåra förövaren än vid interna dataintrång, något som kan vara en av anledningarna till att antalet åtal inte ökat i samma utsträckning som antalet polisanmälningar.

De externa rättsfall som presenteras här nedan är enligt mig ett representativt urval av gällande praxis.

13.3.1 Tjuvsurfarna 1[115]

Två tonåringar PB och JL åtalades 2001 för dataintrång och bedrägeri[116] respektive dataintrång och bedrägligt beteende[117]. PB och JL hade genom att utnyttja en tredje parts användaridentitet samt lösenord vid upprepade tillfällen loggat in på dennes Internetkonto hos en ISP. PB och JL lämnade därmed oriktiga uppgifter om sina identiteter och beredde sig tillgång till en upptagning för automatisk databehandling vilket ledde till skada för ISP:n (den tredje parten hölls skadelös av ISP:n) och vinning för PB och JL.

PB och JL erkände ansvar för ”bedrägeri respektive bedrägligt beteende under påstående att dataintrånget konsumerades av dessa brott.”[118]

Tingsrätten ansåg det ostridigt att PB och JL handlat enligt åklagarens gärningsbeskrivningar, åtalet avseende bedrägeri samt bedrägligt beteende ansågs därmed styrkt. Ansvar för dataintrång kunde däremot inte anses föreligga, detta då enligt tingsrätten 4 kap. 9c § BrB om dataintrång i likhet med den tidigare bestämmelsen i 21 § Datalagen skall ses som en paraplybestämmelse. Enligt tingsrättens bedömning skulle därför dataintrånget konsumeras av brotten bedrägeri och bedrägligt beteende. Åtalet bifölls därför endast avseende PB vad avsåg bedrägeri och JL vad avsåg bedrägligt beteende. Påföljden för PB bestämdes med hänsyn till ”det kvalificerade sätt som bedrägeriet utförts på”[119] till villkorlig dom i kombination med fyrtio dagsböter à trettio kronor, vad avsåg JL bestämdes påföljden till fyrtio dagsböter à trettio kronor

Den del av domen som avsåg ansvar för dataintrång för PB och JL överklagades till Svea hovrätt av åklagaren.[120] Hovrätten delade tingsrättens bedömning vad avsåg rubriceringen av bedrägeribrotten, däremot var man

[114] BRÅ rapport 2000:2, IT-relaterad brottslighet, samt www.bra.se
[115] Gotlands tingsrätt B114-01, 2001-06-14, s.5.
[116] 9 kap. 1 § BrB.
[117] 9 kap. 2 § BrB.
[118] Gotlands tingsrätt B114-01, 2001-06-14, s.5.
[119] Ibid, s.6.
[120] Svea hovrätt B5413-01, 2002-11-25.

av en annan uppfattning vad gällde bedömningen av konkurrensen mellan de olika bedrägeribrotten och dataintrånget.

Man påpekade bland annat att enligt ”förarbetena till 4 kap. 9c § […] förhållandet mellan brottet dataintrång och övriga brottsbalksbrott får avgöras enligt sedvanliga principer för bedömningen av konkurrens mellan överlappande straffstadganden i brottsbalken”[121]. Man påtalade vidare att enligt samma förarbete avser bestämmelsen om dataintrång att ”skydda det datalagrade materialet”[122], och att således skilda skyddsintressen för de olika straffbuden (bedrägeri/bedrägligt beteende och dataintrång) förelåg vilket medförde att verklig konkurrens mellan straffbuden fick anses föreligga.

Hovrätten fann att vid jämförelse mellan straffskalorna för de olika brotten, bedrägeribrott allmänt sätt, var att anses som svårare än dataintrång medan i sin tur dataintrång fick anses som svårare än bedrägligt beteende. Man fann därför att PB skulle dömas för bedrägeri medelst dataintrång och JL för dataintrång och bedrägligt beteende. Detta ledde till att JL fick ett något strängare straff sextio dagsböter à trettio kronor.

13.3.2 Tjuvsurfarna 2[123]

Tre tonåringar DE, SS och TK åtalades 2002 vid Nacka tingsrätt för dataintrång och bedrägligt beteende (DE och SS) samt dataintrång och bedrägeri (TK).[124] Samtliga åtalade nekade till gärningarna men medgav skadeståndsanspråken.

DE och TK hade via Internet genom en för dem okänd person fått tillgång till användaruppgifter till Internet konton hos en ISP. DE och TK erkände att de hade använt ifrågavarande uppgifter för att ansluta till Internet, att kostnaden för detta skulle drabba någon enskild hade man knappt reflekterat över, utan båda anförde att de trodde att kontona tillhörde ”något stort företag”[125] och att man inte skulle ha gjort samma sak om man vetat att det drabbat någon enskild. SS anförde att han inte mindes att han skulle ha använt någon annans internetkonto, och att någon av hans kompisar som ofta var hos honom kunde ha använt uppgifterna. SS var dock ”beredd att ta på sig betalningsansvar”[126].

---

[121] Ibid, s.6.
[122] Ibid, s.6.
[123] Nacka tingsrätt B 565-02, 2002-04-19.
[124] Målsägare i detta fall var samma som i det tidigare refererade tjuvsurfar fallet. Företaget som vid denna tid var en av Sveriges största leverantörer av Internet hade själva blivit utsatta för dataintrång varvid en stor mängd användarnamn med tillhörande lösenord hade blivit stulna. ISP:n valde att hålla alla drabbade användare ansvarslösa, och polisanmälde alla upptäckta fall av olovlig användning.
[125] Nacka tingsrätt B 565-02, 2002-04-19, s.6-7.
[126] Nacka tingsrätt B 565-02, 2002-04-19, s.7.

Tingsrätten gjorde bedömningen att även om DE och TK medgivit att man i ”syfte att sänka sina egna internetkostnader”[127] loggat in med hjälp av de angivna användaruppgifterna, kunde uppsåt inte styrkas. Det av åklagaren hävdade eventuella uppsåtet ansåg tingsrätten inte vara styrkt då DE och TK inte gav intryck av att vara likgiltiga inför att internetkontot egentligen tillhörde en privatperson. Åtalet mot DE och TK ogillades således.

Vad gällde SS ansåg tingsrätten att det inte kunde anses som styrkt att det var SS som loggat in på internetkontot med hjälp av användaruppgifterna, varvid även åtalet mot SS ogillades.

Då de tilltalade medgivit skadeståndsyrkandena beslutades att samtliga skulle betala skadestånd enligt respektive yrkande (DE - 638 kronor, TK – 8145 kronor, SS – 165 kronor).

Domen avseende DE och TK överklagades till Svea hovrätt[128], där åklagaren återigen yrkade på ansvar för dataintrång och bedrägligt beteende för DE, samt dataintrång och bedrägeri för TK. Även nu bestred de åtalade ansvar med hänvisning till att de saknat uppsåt.

Enligt Svea hovrätt var bägge införstådda med att uppkoppling mot Internet medför vissa kostnader i olika led. För att ansvar för bedrägeri enligt 9 kap. 1 § 2st BrB skall kunna föreligga krävs att en gärningsman olovligen har påverkat resultatet av en automatisk informationsbehandling eller liknande automatisk process, samt att detta medför vinning för honom och skada för annan. Det finns inget krav att gärningsmannen skall veta vilken den drabbade är.

Enligt hovrätten var TK:s, och DE:s gärningar sådana att ansvar för bedrägeri respektive bedrägligt beteende skulle föreligga, det faktum att DE hävdade att han inte skulle ha begått gärningen om han känt till att någon enskild person drabbats saknade enligt hovrätten betydelse.

Då enligt hovrätten intrång i en automatisk databehandling krävs för att en gärning enligt 9 kap. 1 § 2st BrB skall komma till stånd skall inte ansvar enligt 4 kap. 9c § BrB samtidigt utdömas. Påföljden för DE bestämdes till åttio dagsböter à trettio kronor, för TK till trettio dagsböter à trettio kronor.

13.3.3 Fragglarna[129]

Två män dömdes år 2000 för två fall av dataintrång. Åtal hade väckts för fyra fall av dataintrång, men enbart två av dessa ansågs kunna bindas till de

[127] Ibid.
[128] Svea hovrätt B5647-02, 2002-10-07.
[129] Södertälje tingsrätt B1260-99, 2000-02-28.

två åtalade gärningsmännen. Vidare åtalades männen även för bedrägeri samt häleri.

De två männen hade utnyttjat en dator placerad vid ett företag i Örebro som språngbräda[130] för att utnyttja en säkerhetsbrist i ett antal (50-100 stycken) datorsystem i USA tillhörande främst den Amerikanska staten samt försvarsmakten i syfte att olovligen berett sig tillgång till dessa. De hade därvid installerat program som möjliggjorde nedladdning av lösenord i syfte att öka sin behörighet i systemen. Männen fälldes för dessa gärningar för två fall av dataintrång.

Männen åtalades också för dataintrång i en dator placerad vid Uppsala universitet, samt en dator hos företaget *WIRE* i England. Åtalet kunde i dessa fall inte styrkas då det inte kunde säkerställas att det var dessa gärningsmän som utfört intrånget.[131]

Enligt domstolen kunde ”varken brottets art eller straffvärde tala för fängelsestraff”, Den ena mannen dömdes därför till villkorlig dom förenat med dagsböter samt den andra mannen enbart till villkorlig dom.

13.3.4 Lunarstorm[132]

SJ född 1987 åtalades 2004 för dataintrång samt sexuellt ofredande. SJ hade tillsammans med två andra i samförstånd upprepade gånger otillåtet berett sig tillträde till målsägarens ”krypin” på Lunarstorm[133]. Två av gärningsmännen var vid gärningstillfället ej fyllda femton år varvid de ej kom att åtalas.

De tre gärningsmännen hade fått tillgång till målsägarens lösenord och utnyttjade detta för att bereda sig tillgång till sidan. Väl där ändrade man målsägarens profil på ett sådant sätt att domstolen ansåg det vara sexuellt ofredande. Man sände även e-mail i målsägarens namn varvid mottagarna vilseleddes att tro att de kom ifrån målsägaren. Målsägaren bytte lösenord flera gånger under denna tid, men trion lyckades varje gång knäcka detta.

SJ ansågs inte ha varit delaktig i detta lösenordsknäckande, men i övrig ansåg de alla tre vara lika delaktiga i gärningen. SJ dömdes för dataintrång och sexuellt ofredande till vård inom socialtjänsten samt att utge skadestånd för det sexuella ofredandet.

---

[130] Att utnyttja en dator som språngbräda innebär att denna dator kommer att bli identifierad som ”anfallande dator”.
[131] I gärningsmännens lägenhet uppehöll sig flera personer som vid olika tillfällen utnyttjade männens datorer.
[132] Kalmar tingsrätt B322-04, 2004-03-25.
[133] Lunarstorm är en community för tonåringar på Internet. Krypin är benämningen på en medlems personliga sida. På denna sida presenteras personen, samt denne kan härifrån skicka och ta emot e-mail.

SJ överklagade domen och yrkade att åtalet för sexuellt ofredande skulle ogillas, att påföljden för dataintrång skulle bestämmas till böter, samt att skadeståndstalan skulle lämnas utan bifall. Göta Hovrätt fastställde både tingsrättens dom och påföljd.[134]

13.3.5 Aftonbladet/ ZEA[135]

En man född 1975 fälldes 1998 för fyra fall av dataintrång av Lunds tingsrätt. Gärningsmannen hade vid ett tillfälle olovligen berett sig tillträde till en webbserver tillhörande Aftonbladet genom att utnyttja lösenord och login som han erhållit av en okänd person på Internet. Väl inne i webbservern bytte han ut en av sidorna mot en annan, original sidan fanns dock fortfarande kvar i datorn. Gärningsmannen hade även vid tre tillfällen olovligen berett sig tillgång till företagets ZEA:s e-mail- och namnserver och däri raderat en eller två kataloger, även i detta fall fanns de raderade filerna kvar i en annan del av systemet.

Då detta mål prövades enligt Datalagens 21 § gjorde tingsrätten en bedömning huruvida gärningen var belagda med straff i brottsbalken vilket man fann att den ej var.

Vid straffmätningen uttalade tingsrätten följande; ”Tingsrätten ser allvarligt på den typ av brottslighet som [gärningsmannen] har gjort sig skyldig till. Påföljden kan inte stanna vid enbart böter.”[136] Vid invägning av gärningsmannens sociala situation och det faktum att han tidigare var ostraffad kom dock tingsrätten fram till ”efter viss tvekan, att påföljden skall stanna vid villkorlig dom jämte höga dagsböter.”[137] Påföljden bestämdes därför till villkorlig dom och etthundra dagsböter à etthundrasextio kronor.

13.3.6 KTH/SU[138]

FW född 1972 hade under maj 1995 – 5 september 1995 vid ett mycket stort antal tillfällen olovligen berett sig tillgång till upptagning för automatisk databehandling vid KTH och SU:s datorer. Genom detta hade han också fått tillgång till andra databaser kopplade till dessa datorer.

[134] Göta Hovrätt B996-04, 2004-05-28.
[135] Lunds tingsrätt B1914-97, 1998-02-05.
[136] Ibid, s.3.
[137] Ibid.
[138] Stockholms tingsrätt B11-7613-95, 1996-05-10.

FW som studerade datasäkerhet vid UU blev nyfiken på praktiska tillämpningar av sina teoretiska kunskaper, han fick via kontakter på Internet tillgång till lösenord och annan information som möjliggjorde för honom att via sin egen dator och ett modem koppla upp sig mot datorer tillhörande KTH samt SU. Inne i systemen beredde han sig inte bara tillgång till information som var allmäntillgänglig för legitima användare av systemet, utan även krypterade lösenordslistor som han senare dechiffrerade samt övervaknings- och säkerhetsrelateradeprogram. Han tilldelade även sig själv så kallad ROOT-behörighet[139] i systemet. Han hade vidare även kopplat upp sig mot de andra databaser som var kopplade gentemot KTH och SU:s system. Den information han tillförskansat sig i systemet hade han varken utnyttjat för eget bruk eller spridit vidare.

FW bestred åtalet med hänvisning till att ”databasernas innehavare skulle ha inbjudit till kommunikation.”[140] Tingsrätten ansåg att FW måste ha insett att enbart behöriga företrädare för KTH samt SU ägde rätt att dela ut lösenord och konton för att möjliggöra inloggning i systemet, han måste också ha insett att de personer han fått denna information av på Internet ej var behöriga att företräda KTH och SU. FW ansågs därför skyldig till dataintrång enligt 21 § Datalagen[141].

Åklagaren hade yrkat på villkorlig dom jämte böter för FW, något som inte tingsrätten biföll av tre anledningar: 1. FW var tidigare ostraffad. 2. FW hade inte otillbörligen utnyttjat erhållen information eller spridit denna vidare till tredjepart. 3. Säkerhetssystemen var bristfälliga, vilket möjliggjorde för FW att komma så långt som han gjorde. Att KTH och SU var tvungna att lägga ned ett stort arbete för att förändra sina datasystem efter FW:s intrång ansåg inte tingsrätten talade för annat än bötesstraff, utan uttalade att ”Det har dock ej klarlagts i vilken omfattning nedlagt arbete hänför sig till en sådan allmän höjning av datasäkerhet vid nämnda institutioner och underhåll av system som alltid måste göras”[142]. Tingsrätten bestämde påföljden till femtio dagsböter à trettio kronor.

13.3.7 Spray[143]

JE född 1979 åtalades 1998 för två fall av dataintrång mot Högskolan i Gävle samt mot Spray Interactive Media, vidare åtalades han för ett fall av försök till utpressning gentemot Spray Interactive Media.

JE erkände dataintrång i Högskolans dator under tiden 20 juli – 16 december 1996 (åtalspunkt 1), syftet med intrånget var att få tillgång till Internet. Tingsrätten fann åtalet styrkt. Vad avser åtalspunkterna för dataintrång i Spray Interactive Media:s dator (åtalspunkt 2) samt försök till

[139] ROOT-behörighet är den högsta behörigheten i datasystem baserade på UNIX.
[140] Stockholms tingsrätt B11-7613-95, 1996-05-10, s.4.
[141] SFS 1973:289.
[142] Stockholms tingsrätt B11-7613-95, 1996-05-10, s.5.
[143] Gävle tingsrätt B12-97, 1998-11-27.

utpressning (åtalspunkt 3) bestred JE ansvar under påstående att dataintrånget inte skett olovligen och att ”han haft en uppgörelse med Spray om att mot ersättning göra en översyn av datasäkerheten hos bolaget”[144], han gjorde även gällande att brottsprovokation förekommit.

JE fick via Internet kontakt med ST som arbetade för Spray, de samtalade om datasäkerhet och han fick uppfattningen att han av ST fick tillåtelse att försöka bereda sig tillgång till Spray:s datorer i syfte att testa säkerheten. Han gjorde detta och hittade därvid ett antal säkerhetshål. Han påtalade detta för ST och hävdade att han skulle vara en lämplig kandidat för att göra en säkerhetskontroll av systemet. Man kom överrens om att man skulle mötas på Spray:s kontor i Stockholm. Enligt JE var han av uppfattningen att han skulle utföra denna säkerhetskontroll vid detta tillfälle. Vid mötet som spelades in av en person från polisen med hjälp av en dold bandspelare ansåg JE att man ”ville blåsa honom”[145] varvid han bland annat uttalade att om han ej fick ersättning för arbetet skulle han kanske sprida ut att Spray hade dålig säkerhet. Mötet avslutades dock med att ett kontrakt upprättades mellan Spray och JE om att JE mot en ersättning av 10 000 kronor skulle utföra säkerhetsarbete för Spray:s räkning. Åklagaren hävdade att JE genom olaga hot förmått Spray att ingå avtalet med honom, medan JE förnekade att avtalet tillkommit genom hot.

Tingsrätten fann att det vid mötet förekommit hotfulla uttalanden från JE:s sida. Dock fann tingsrätten att dessa uttalanden var grundade i att JE levde i tron att det förelåg en överenskommelse mellan honom själv och Spray och att JE därför ansåg att om ”Spray inte höll sin del av överenskommelsen behövde han inte vara lojal.”[146] Detta stöddes enligt tingsrätten av det som framkommit vid förfrågan från Spray till JE om att komma till deras kontor. Tingsrätten fann därför att åtalet vad avsåg försök till utpressning (åtalspunkt 3) skulle ogillas.

Vad avsåg åtalspunkt 2, dataintrånget mot Spray ansåg tingsrätten att det var utrett att JE tagit sig in i Sprays server, man fann vidare ingenting i bevisningen som stödde JE:s påstående om att han av ST fått tillåtelse att göra detta. Man ansåg därför åtalet styrk i denna del.

Påföljden för de två fallen av dataintrång blev sextio dagsböter à trettio kronor.

13.3.8 SCIFI m.fl.[147]

Två män EW, född 1979 och AH, född 1982 stod 1998 åtalade för flera fall av dataintrång som skett under 1996-1997. Samtliga åtalspunkter utom åtalspunkt 3 och 5 kombinerades med enskilda anspråk, den totala summan

[144] Gävle tingsrätt B12-97, 1998-11-27, s.4.
[145] Ibid.
[146] Ibid.
[147] Umeå tingsrätt B108-98, 1998-06-02.

för skadeståndsanspråken för bägge tilltalade var 25 900 Finska Mark samt 56 400 kronor. Vid åtalet tillämpades Datalagens 21 §.

EW åtalades för följande gärningar[148]:

- Att olovligen berett sig tillträde till det finska företaget SCIFI International Communication OY:s datorer. EW tillskansade sig där ROOT behörighet och installerade ett snifferprogram. (åtalspunkt 1)
- Att olovligen berett sig tillträde till Länsstyrelsernas gemensamma Internetserver och däri olovligen ha genomfört förändringar i webbserver samt på deras hemsida på Internet. (åtalspunkt 2)
- Att olovligen ha berett sig tillträde till en privatpersons dator uppkopplad via Lindköpings universitet, samt däri installerat ett snifferprogram. (åtalspunkt 3)

AH åtalades för följande gärningar:

- Att olovligen berett sig tillträde till det finska företaget SCIFI International Communication OY:s datorer. AH tillskansade sig där operator behörighet och gjorde förändringar i datorn. (åtalspunkt 1)
- Att olovligen vid ett stort antal tillfällen berett sig tillgång till upptagning för automatisk databehandling vid Swedish Institute of Computer Science (SICS) i syfte att få tillgång till Internet. (åtalspunkt 5)
- Att olovligen vid ett stort antal tillfällen berett sig tillgång till upptagning för automatisk databehandling vid det norska företaget System Sikkerhet A/S i syfte att få tillgång till Internet. (åtalspunkt 6)

Åtalspunkt 1. Både EW och AH erkände att man berett sig tillträde till SCIFI:s dator, men bägge bestred ansvar då det rörde sig om en så kallad IRC-server som var öppen för allmänheten. EW hävdade att han inte mindes om han skaffat sig ROOT behörighet eller lagt in ett snifferprogram, men erkände att det antagligen var så. AH erkände att han med hjälp av ett lösenord han hade fått via en IRC kanal laddat ned en kommando fil från SCIFI:s dator samt gjort ändringar i denna i syfte att öka sin behörighet. Domstolen fann att åtalet styrkt i AH:s fall, men att EW:s ”uppgifter var alltför obestämda för att det enbart genom dessa skall anses tillförlitligen styrkt att han vidtagit de åtgärder som åklagaren påstått.”[149] Åtalet ogillades därför på denna punkt.

Åtalspunkt 2. EW erkände gärningen, vilket stöddes av den övriga utredningen. Domstolen fann därför åtalet styrkt

[148] EW åtalades också för narkotikabrott.
[149] Umeå tingsrätt B108-98, 1998-06-02, s.6.

Åtalspunkt 3. EW kunde varken erkänna eller förneka gärningen med hänvisning till att han ej mindes. Enligt EW kunde ingen annan ha använt hans dator under den aktuella tiden. Domstolen fann med stöd av spårnings- och loggningsuppgifter från privatpersonens dator samt Telia att intrånget haft sitt ursprung i EW:s dator, åtalet ansågs därför styrkt.

Åtalspunkt 5. AH erkände att han utnyttjat ett av annan person installerat program på SICS:s i syfte att få tillgång till Internet, men bestred att han därigenom berett sig tillgång till upptagning för automatisk databehandling. Han anförde vidare att han ej kunnat få tillgång till dokument eller filer på datorns hårddisk och att han enbart syftade att få tillgång till dess host name ”egoboy”. Domstolen fann ej att det som AH anförde vederlagt. Istället fann man att han genom sina uppgifter styrkt att han berett sig tillgång till upptagning för automatisk databehandling såvitt det gällde det program han använt i SICS:s dator för att komma i förbindelse med Internet. Åtalet ansågs därmed styrkt.

Åtalspunkt 6. AH erkände gärningen, vilket styrktes av spårningsrapporten från Telia. Domstolen ansåg därför åtalet styrkt.

Påföljden för EW och AH bestämdes med hänsyn till EW:s tid i häkte till böter. I EW:s fall bestämdes böterna till etthundra dagsböter à trettio kronor, i AH:s fall åttio dagsböter à trettio kronor.

13.4 Analys

De presenterade rättsfallen är exempel både på interna och externa dataintrång, samt ren och oren hacking. Att brottsrubriceringen dataintrång täcker in dessa till viss del skilda gärningar orsakar enligt min mening inga större problem, vilket också praxis visar. Vad jag däremot anser vara problematiskt är domstolarnas inställning vid straffmätningen. Man tar vid flera tillfällen mycket stor hänsyn till gärningsmannens ålder, så pass stor hänsyn att straffet enligt min mening blir för lågt. Enligt statistik från BRÅ är gärningsmän i åldrarna 15-17 år den största gruppen av förövare, att med detta som bakgrund utdöma väsentligt lägre straff på grund av ålder är enligt mig felaktigt.[150]

Vidare så synes inte domstolarna lägga någon större vikt vid de skador som åsamkas vid externa dataintrång. I både KTH/SU- och SCIFI m.fl.-fallet åsamkades skador för stora belopp, något som tingsrätten inte tillerkände någon större vikt vid straffmätningen. För brottet dataintrång finns inget skada/ vinnings rekvisit, detta innebär dock inte att eventuell skada/ vinning inte skall beaktas vid straffmätningen. En av anledningarna till att så inte sker kan vara de svårigheter att utvärdera den faktiska skadan av ett dataintrång, något som bland annat uppmärksammades i KTH/SU-fallet. Vad gäller interna dataintrång får domstolarna anses lägga större vikt vid

[150] Se kapitel 12.1.

uppkomna skador. Vi kan i både Polis- och Socialsekreterarfallet uttyda att domstolen lagt stor vikt vid det faktum att gärningsmannen antingen tagit del av sekretessbelagda uppgifter på ett obehörigt sätt, eller som i Polisfallet; spridit dessa vidare till tredjeman.

Aftonbladet/ ZEA-fallet skiljer sig klart från de övriga fallen av externa dataintrång. Här uttalar tingsrätten att man ser mycket allvarligt på denna typ av brottslighet och att man enbart efter viss tvekan kan låta straffet stanna vid villkorlig dom och stränga böter. En av anledningarna till detta kan vara att filer och kataloger raderades, samt att syftet med intrånget var att ändra information.

Angående begreppet *bereda sig tillgång till ADB* får domstolarna klart anses ha gjort bedömningen att en handling bestående i att *stjäla* Internet access är att anse som ett sådant beredande. Något jag anser vara en korrekt tolkning av begreppet.

Att datorbrottslighet är gränsöverskridande ser vi i SCIFI m.fl.-fallet, i två av åtalspunkterna är målsägaren ett utländskt företag vilka via hemlandets polis begärt lagföring av gärningsmännen. Att domstolen överhuvudtaget inte kommenterar detta faktum kan jag inte tolka på annat sätt än att man ser det som naturligt att brottet anses begånget i Sverige. Vad gäller val av påföljd kan vi återigen se att påföljden blir relativt lätt med tanke på det stora antal gärningar som anses styrkta.

Som synes är det svårt att uttyda någon klar linje i domstolarnas argumentation och värdering av gärningarnas gravhet. Jag anser att detta till viss del kan tillskrivas det faktum att det inte finns någon grov brottsrubricering.

14 Internationella åtaganden

14.1 Europarådets konvention om IT-relaterad brottslighet

Europarådets konvention om IT-relaterad brottslighet[151] som öppnades för signering den 23 november 2001 är resultatet av ett mer än tio år långt arbete med att ta fram en internationell lösning på problemet med IT-brottslighet. Det är den första internationella konventionen som berör brott som begås över Internet. Konventionens syfte är primärt att skapa en gemensam straffrättslig policy för skyddet av samhället mot cyberbrottslighet.[152]

Konventionen har blivit undertecknad av de flesta av rådets medlemmar samt vissa icke medlemmar såsom Kanada, Japan, Sydafrika samt USA. Totalt har fram till dags dato (05-01-29) trettioåtta stater undertecknat konventionen, men enbart nio stater har ratificerat densamma.[153] Frågan om Sveriges ratificering bereds just nu av justitiedepartementet.[154] Någon officiell svensk översättning av konventionen finns ännu inte varvid följande stycken är författarens egen översättning och tolkning från engelska. Ett utdrag av relevanta artiklar från den officiella versionen finns i bilaga A.

14.1.1 Art 1 – Definitioner

Konventionen definierar ett datasystem som en apparat eller anordning som består av hårdvara och mjukvara, utvecklat för att utan direkt mänsklig inblandning behandla digital data.[155] Datasystemet kan antingen vara en enskild apparat, eller vara en del i ett nätverk av sammankopplade liknande apparater. Nätverkets fysiska uppbyggnad exempelvis om det är trådbundet eller trådlöst, litet eller globalt och hur de enskilda datasystemen kopplas in och syftet med dessa är ointressant, huvudsaken är att data utbyts över nätverket.

Data är ”varje representation av fakta, information eller begrepp i en form lämplig för behandling i ett datasystem, inklusive ett program avsett att få ett datasystem att utföra en funktion.”[156] Denna definition följer ISO definitionen av data, dock har man i konventionen i syfte att förtydliga att

[151] Convention on Cybercrime, Budapest, 23.XI.2001.
[152] http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm
[153] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=19/10/04&CL=ENG
[154] Prop. 2003/04 :164, s.7.
[155] http://conventions.coe.int/treaty/en/Reports/Html/185.htm
[156] Convention on Cybercrime art 1(b).

det rör sig om data lämplig för direkt behandling i ett datasystem använt begreppet Computer data som i svensk översättning torde bli digitaldata.

14.1.2 Art 2 – Olovligt intrång

Stater som ratificerar konventionen åläggs att kriminalisera förfarande som innebär att någon uppsåtligen och olovligen bereder sig tillgång till hela eller delar av ett datasystem. För att intrång skall föreligga får stater sätta som rekvisit att någon form av säkerhetssystem skall ha kringgåtts i syfte att bereda sig tillgång till data, ett nätverk av datasystem eller annat ohederligt uppsåt.

Enligt the explanatory report[157] täcker *bereda sig tillgång till hela eller delar av ett datasystem* in tillgång till hårdvara, komponenter (delar av system), lagrad data om de installerade systemen, mappar (directories), trafik och innehålls relaterad data (contents-related data). Var och hur (trådburet eller trådlöst) någon bereder sig tillgång till systemet är irrelevant, access via LAN, WAN eller uppringdförbindelse täcks in av artikeln. Dock anses inte att enbart skicka ett e-mail eller en fil till ett datasystem som att bereda sig tillgång.

14.1.3 Art 3 – Olovlig avlyssning

Staterna skall tillse att olovlig avlyssning som sker med tekniska hjälpmedel av icke publik överföring av data till, från eller inom ett datasystem inklusive elektromagnetisk strålning kriminaliseras. Enligt the explanatory report kan sådana tekniska hjälpmedel exempelvis bestå av avlyssningsutrustning för antingen trådburen eller trådlös kommunikation, programvaror för avlyssning, lösenord eller koder. Avlyssning innebär även inspelning av trafik.

Att dataöverföringen skall vara icke publik innebär inte att informationen som överförs inte kan vara information som är allmänt känd. Det innebär enbart att de kommunicerande parterna inte önskar att överföringen av informationen skall vara tillgänglig för andra. The explanatory report tar bland annat upp krypterade tv-utsändningar som ett exempel på en dylik överföring. Att informationen överförs via ett publikt system innebär inte för den sakens skull att informationen skall anses som publik.

Överföringen kan ske antingen mellan datasystem som ägs av en eller flera personer, i ett enskilt datasystem exempelvis överföring mellan terminal och skrivare eller terminal och skärm, eller mellan en person och en terminal.[158] Även avlyssning av elektromagnetisk strålning från ett datasystem så kallade röjande signaler (RöS) täcks in av artikeln, detta trots att signalerna i sig inte anses som data under artikel 1(a), signalerna kan dock med rätt

[157] Explanatory report to the convention on Cybercrime.
[158] Ibid, section 55.

utrustning användas för att rekonstruera den data som behandlas av systemet.

Liksom i artikel 2 får en stat sätta som rekvisit för att olovlig avlyssning skall anses föreligga att personen handlar med ohederligt uppsåt eller att överföringen av data måste ske mellan olika datasystem och inte enbart inom ett system.

14.1.4 Art 4 – Olovlig datastörning

Konventionen ålägger staterna att införa bestämmelser som skapar ett skydd för data mot avsiktlig orsakande av skada, liknande det som finns för fysiska objekt.[159] Artikeln listar ett antal gärningar som skall anses som datastörning; skadande, radering, försämring, förändring samt undertryckande av data. Gemensamt för samtliga är att de skall ha utförts utan rätt för att vara straffbara. Exempelvis innebär detta att säkerhetskontroller och så kallade PEN-tests inte är att anses som olovliga. Vidare skall inte heller användande av kryptering i syfte att skapa säkra kommunikationer anses som olovlig enligt the explanatory report.[160] Trojan och virusattacker täcks däremot in under vad som skall anses som olovliga handlingar. Att använda sig av anonymiserings servrar torde inte anses som olovligt enligt rapporten, dock så står det parterna fritt att kriminalisera förfarandet att förändra eller undertrycka så kallad header information i IP-paketen för att dölja en gärningsmans identitet vid brott.[161]

Enligt den andra paragrafen har parterna till konventionen rätt att ställa som rekvisit för lagbrott att gärningen har medfört allvarlig skada.

14.1.5 Art 5 – Olovlig systemstörning

Det åligger parterna att vidta åtgärder för att kriminalisera olovlig systemstörning. För att en gärning skall anses som olovlig systemstörning måste gärningen vara uppsåtlig och allvarligt hindra det rättmätiga utnyttjandet av systemet. Exempel på dylik störning kan vara DoS eller e-mail bombningsattacker.[162] Vad som i sig skall anses som att allvarligt hindrande är upp till de undertecknande staterna att avgöra.

Enligt the explanatory report är förfarandet med *spamming* i sig inte att anses som systemstörning såvida den inte gjorts med syfte att allvarligt hindra kommunikationen. Trots detta har man genom att låta parterna själva

[159] Explanatory report to the convention on Cybercrime, section 60.
[160] Ibid, section 62.
[161] Ibid.
[162] E-mail bombningsattack är ett förfarande varvid ett stort antal e-mail skickas till en mottagare i syfte att överlasta systemet.

besluta om var gränsen går för allvarlig systemstörning lämnat dörren öppen för att även kriminalisera *spamming*.[163]

Att notera är att system i denna artikel inte enbart innebär datorsystem, även telekommunikationssystem innefattas, varvid även så kallad phone phreaking täcks in.

14.1.6 Art 6 – Olovlig användning av hjälpmedel

Artikeln föreskriver parterna att kriminalisera; produktion, försäljning, införskaffande, import, distribution eller på annat sätt tillhandahållande av hjälpmedel att begå tidigare nämnda brott. Såsom hjälpmedel skall enligt paragraf 1(a)1 anses ett föremål, designat eller anpassat i syfte att kunna användas för att begå brotten i artikel 2-5, såsom föremål anses även dataprogram. Även lösenord, accesskoder eller annan liknande data som möjliggör åtkomst till hela eller delar av ett datasystem skall anses som hjälpmedel. Detta innebär att spektrumet av hjälpmedel blir väldigt stort. I syfte att hindra att även legitima verktyg för säkerhetsarbete kriminaliseras, har man ställt upp som rekvisit att det måste finnas ett direktuppsåt att använda dessa verktyg för att begå de brott som räknats upp i artiklarna 2-5.[164]

Man har vidare lämnat det öppet för parterna att själva kräva ett minsta antal hjälpmedel innan brott föreligger. Man har även gjort det möjligt för parterna att inte införa de delar av paragraf 1 som ej rör försäljning, distribution eller på annat sätt tillhandahållande av nämnda hjälpmedel.

14.2 Analys

Convention on cybercrime är i mitt tycke en väl genomtänkt och väl genomarbetad internationell konvention. Man har inte enbart sett till dagens problem, utan man har i utformningen blickat framåt. Sveriges troliga ratificering av konventionen kommer dock att medföra ett visst behov av lagstiftningsarbete.

14.2.1 Art 1 – Definitioner

Konventionens definitioner både av data och datasystem torde väl överensstämma med de svenska definitionerna. Man har i konventionens definition av ”computer data” lagt tonvikten vid dess funktion som representation av information och att den skall vara maskinläsbar. Denna definition är mycket lik om inte identisk med den svenska ”information för

[163] Explanatory report to the convention on Cybercrime, section 67, 69.

[164] Explanatory report to the convention on Cybercrime, section 76.

automatisk databehandling". Jag ser därför inga behov av reformering av svensk lagstiftning vad gäller dessa delar.

14.2.2 Art 2 – 4 kap. 9c § BrB

Liksom i 4 kap. 9c § BrB är det i artikel 2 tillräckligt att gärningsmannen olovligen har berett sig tillgång till datasystemet för att det skall anses som olagligt. 4 kap. 9c § BrB har i förhållande till artikel 2 ett vidare tillämpningsområde, närmare bestämt intrång i upptagning som är under vidarebefordran. Detta täcks inte in i artikel 2 utan har istället tagits upp under artikel 3. Jag kan inte på något sätt finna att den svenska regleringen i 4 kap. 9c § BrB inte skulle överrensstämma och till fullo täcka in de krav som ställs på konventionsparterna i artikel 2.

14.2.3 Art 3 – 4 kap. 8, 9c §§ BrB

Som nämndes här ovan täcker 4 kap. 9c § BrB in även delar av artikel 3, huvudparagrafen i svensk lagstiftning på avlyssningsområdet är dock 4 kap. 8 § BrB Brytande av post- och telehemlighet. Enligt artikel 3 skall all uppsåtlig och olovlig avlyssning av icke publika transmissioner från, till eller inom datasystem kriminaliseras om dessa görs med tekniska hjälpmedel. Man tar specifikt upp RöS som ett exempel på en dylik transmission. Att avlyssna icke publika utsändningar på annat sätt än genom etern är redan kriminaliserat i Sverige genom 4 kap. 8 § BrB, dock så är som bekant "etern fri"[165] och avlyssning genomförd av enskild genom att ta emot radiovågor är inte kriminaliserat. Som jag tidigare har nämnt under kapitel 9 är det därför inte heller möjligt att döma någon för olovlig avlyssning genom att ta emot och bearbeta information via radiovågor från ett datorsystem. Vidare är inte heller avlyssning genom mottagning av RöS ett lagbrott i Sverige. För att Sverige skall kunna anses följa konventionen måste därför ändringar ske i lagstiftningen.

14.2.4 Art 4 – 4 kap. 9c, 12 kap. 1 §§ BrB

Olovlig datastörning är redan i dag till viss del kriminaliserat i svensk rätt genom 12 kap. 1 § BrB samt 4 kap. 9c § BrB.[166] Noteras bör dock så som diskuterats under kapitel 11.5 att förfarandet där enbart data undanhålls utan att för den del dataintrång har begåtts[167] troligtvis inte är att anses som brottsligt i Sverige, varvid ytterligare lagstiftning behövs för att uppfylla konventionens krav.

---

[165] 6 kap. 17 § i Lag om Elektronisk kommunikation.
[166] Se vidare kapitel 14.4.3.
[167] Exempelvis genom att en legitim användare som har både behörighet och befogenhet att använda systemet olovligen krypterar eller på annat sätt undanhåller data från andra legitima användare, eller genom Denial of Service attacker.

14.2.5 Art 5 – 12 kap. 1, 4 kap. 9c §§ BrB

Till skillnad från olovlig datastörning är olovlig systemstörning riktat mot datasystemet och inte mot informationen i sig. Att hindra funktionen på ett datasystem kan i vissa fall anses som skadegörelse och därmed falla under 12 kap. 1 § BrB.[168] Om det är det fysiska datasystemet som skadas faller det tveklöst under 12 kap. 1 § BrB. Att som artikeln säger skada, radera, försämra eller förändra data i ett datasystem regleras redan av 4 kap. 9c § BrB. Däremot som tidigare framförts, finns i svensk lag inte något förbud mot att enbart sända eller undanhålla data, eller i annat än register föra in uppgifter. Ej heller det förfarandet där enbart en funktion och inte hela datorsystemet hindras att fungera på avsett sätt är kriminaliserat i Sverige i dag. Enligt konventionen får dock Sverige själv bestämma hur mycket systemstörning som skall krävas för att anses som allvarlig. Sammantaget torde det vara så att det krävs ytterligare lagstiftningsarbete för att svensk lagstiftning skall följa konventionen.

14.2.6 Art 6 – 23 kap. 2 § 2st, 4 kap. 9b, 4 kap. 10, 12 kap. 5 §§ BrB

Artikeln om olovlig användning av hjälpmedel har sin motsvarighet i 4 kap. 9b, 10 §§ BrB samt 23 kap. 2 § 2st BrB, den olovliga användningen av hjälpmedel benämns i svensk rätt såsom förberedelse.

Det är redan i dag kriminaliserat under 23 kap. 2 § BrB att i vissa fall befatta sig med immateriella objekt såsom datavirus och annan programvara som ”framställts uteslutande i syfte att begå dataintrång eller andra typer av brott”[169]. Även samlingar av föremål som exempelvis koder eller lösenord torde kunna anses som hjälpmedel i svensk rätt, detta även om de enskilda koderna eller lösenorden i sig inte skulle ses som hjälpmedel. När dessa sammanställs får de dock en annan ”tyngd” som brottsverktyg.[170]

Enligt 4 kap. 10 § BrB krävs för att ansvar för förberedelse till datorintrång skall föreligga att datorintrånget om det hade blivit fullbordat inte skulle ha ansetts som ringa. Det faktum att dataintrånget skulle ha ansetts som icke ringa vid ett eventuellt fullbordande för att ansvar för förberedelse skall föreligga medför att visst lagstiftningsarbete krävs. I konventionstexten finns nämligen inget krav på grad för att ansvar skall föreligga, enbart i artikel 4 och möjligtvis i artikel 5[171] finns möjlighet för de undertecknande parterna att kräva att brottet skall resultera i allvarlig skada, detta torde motsvara den svenska normala – grova brottsrubriceringen.

---

[168] Se vidare kapitel 11.5 samt 14.4.3.
[169] Holmqvist m.fl., Brottsbalken en kommentar Del II studentutgåva 3, 23:25.
[170] Holmqvist m.fl., Brottsbalken en kommentar Del II studentutgåva 3, 23:25.
[171] […] when committed intentionally, the *serious* hindering without right of the functioning of a computer system […] [författarens kursivering].

Vad gäller olovlig användning av hjälpmedel för att begå brott som beskrivs i artikel 3 så regleras detta i 4 kap. 9b § BrB, här står det klart att den svenska lagregleringen inte står i paritet med konventionen. För att försök till brytande av post- och telehemlighet skall föreligga krävs nämligen att någon *anbringat* ett tekniskt hjälpmedel för att ansvar skall föreligga. Om enbart det tekniska hjälpmedlet innehas utan att något försök att använda det föreligger, kan ansvar inte utdömas. Vidare så som nämnts under kapitel 12.1.3 är inte alla former av avlyssning kriminaliserat i Sverige.

Såsom tidigare nämnts faller vissa av konventionens bestämmelser under den svenska brottsrubriceringen skadegörelse i 12 kap. 1 § BrB. Motsvarande som vid förberedelse till dataintrång krävs för ansvar för förberedelse till skadegörelse, att brottet vid ett eventuellt fullbordande skulle ha uppnått en viss grad av allvarlighet. I detta fall är graden grovt brott. Med hänsyn till tidigare argumentering angående de enskilda ländernas möjlighet att kräva att fullbordat brott skall anses som grovt anser jag att Sveriges lagstiftning är i behov av förändring även här.

Om man bortser från detta faktum samt de lagstiftningsbehov som tidigare diskuterats torde Sverige i övrigt uppfylla artikel 6. Man har möjligheten att enligt 2 § kräva en viss mängd av verktyg för att ansvar skall föreligga och man har också möjlighet att välja att inte tillämpa vissa delar av 1 §. Något som enligt mig man inte behöver då Sverige redan i dag har täckt in dessa delar i befintlig lagstiftning.

14.3 Europeiska Unionens råds rambeslut om angrepp mot informationssystem[172]

14.3.1 Kort om rambeslut såsom instrument

Enligt artikel 29 i Fördraget om Europeiska unionen (FEU) anges att målet för unionen skall vara att ge medborgarna en hög säkerhetsnivå inom ett område med frihet, säkerhet och rättvisa. Detta skall ske bland annat genom att utforma gemensamma insatser inom polis- och det straffrättsliga området. Genom att i enlighet med artikel 31.1 a FEU fatta gradvisa beslut som fastställer minimiregler avseende brottsrekvisit och straffsatser inom vissa områden skall medlemsländernas straffrätt harmoniseras och brottsbekämpningen effektiviseras.

En fråga om fattande om ett rambeslut kan enligt artikel 34.2 b FEU väckas antingen av en enskild medlemsstat eller av Europeiska kommissionen, beslutet om antagande av ett rambeslut vilar dock på rådet. För att ett rambeslut skall kunna antas måste det först godkännas i varje medlemsstats nationella parlament, för att sedan antas enhälligt av rådet.

[172] Rambeslut om angrepp mot informationssystem, Europeiska Unionens råd 15010/04.

Ett rambeslut är bindande för medlemsstaterna avseende resultatet som skall uppnås, men överlämnar åt varje medlem att välja form och tillvägagångssätt att uppnå målet.

Sveriges förfarande vid antagande av rambeslut har väckt mycket kritik inte enbart från riksdagspartierna, utan även från bland annat advokatsamfundet och de juridiska fakulteterna.

14.3.2 Bakgrund

Den Europeiska unionen har haft bekämpande av datorbrottslighet på programmet sedan 1998.[173] Vid Europeiska rådets möte den 3 december 1998, samt 15-16 oktober 1999 uttalade man att datorbrottslighet är ett av de områden med särskild betydelse inom straffrätten som är i behov av harmonisering. Detta ledde till att den Europeiska kommissionen presenterades ett förslag till rambeslut om angrepp mot informationssystem den 19 april 2002. [174] Efter sedvanligt yttrande[175] från Europaparlamentet den 22 oktober 2002 behandlades förslaget vid ytterligare fem tillfällen av rådets arbetsgrupp för materiell straffrätt, samt vid tre tillfällen av samordningskommittén av höga tjänstemän som inrättats i enlighet med artikel 36 i fördraget om Europeiska unionen. Den 27 och 28 februari 2003 träffades en politisk överenskommelse om innehållet i rambeslutet i rådet för rättsliga och inrikes frågor. Slutligen beslutades vid Europeiska rådets möte den 25 och 26 mars 2004 att med bakgrund av terroristattacken i Madrid den 11 mars anta en deklaration om bekämpande av terrorism, i denna deklaration slås fast att ett antal rambeslut skall antas i juni 2004 däribland det nämnda rambeslutet om angrepp mot informationssystem.[176] När väl rambeslutet har antagits enhälligt av medlemsstaterna i rådet och därefter publicerats i Europeiska unionens officiella tidning har medlemsstaterna två år på sig att införa de bestämmelser i den nationella rätten som är nödvändiga för att följa rambeslutet.[177]

Riksdagen beslutade efter skarp kritik från flera riksdagspartier den 27 oktober att godkänna utkastet till rambeslutet, främst rörde sig kritiken om det förfarande som regeringen använde vid godkännandet av rambeslut.

Rambeslutet om angrepp mot informationssystem bygger till stora delar på Europarådets konvention om IT-relaterad brottslighet[178] och är i vissa delar näst intill identisk. Rambeslutets omfång är dock klart begränsat jämfört med konventionen.

---

[173] EGT C 19, 23.1.1999, s.1-15.
[174] EGT C 203 E, 27.8.2002, s.109.
[175] Betänkande A5-0328/2002, EUT C 300 E, 11.12.2003, s.16.
[176] Att noteras bör att i skrivandes stund 2005-02-25 rambeslutet fortfarande inte antagits.
[177] Rambeslut om angrepp mot informationssystem, 15010/04, Artikel 12.
[178] Prop. 2003/04 :164, s.6.

Rambeslutet syftar till att harmonisera medlemsländernas lagstiftning vad gäller angrepp mot informationssystem för att därigenom förbättra samarbetet mellan rättsliga och andra myndigheter och bidra till kampen mot organiserad brottslighet och terrorism.

Rambeslutet bifogas i sin helhet på svenska i bilaga B.

14.3.3 Art 1 – Definitioner

I artikel 1 definieras följande begrepp:

a) informationssystem
b) datorbehandlingsbara uppgifter
c) juridisk person
d) orättmätigt

Jag kommer här att behandla definitionerna under punkterna a, b, samt punkten d.[179]

Ett informationssystem är enligt rambeslutet ”en apparat eller en grupp av sammankopplade apparater, eller apparater som hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av datorbehandlingsbara uppgifter”[180].

Datorbehandlingsbara uppgifter är förutom ”framställningar av fakta, information och begrepp i en form som lämpar sig för behandling i ett informationssystem”[181] även ”program som lämpar sig för att få ett informationssystem att utföra en viss uppgift”[182].

Orättmätigt under punkten d definieras såsom ”utan tillstånd från ägaren eller annan rättighetsinnehavare till systemet eller del av detta.”[183] En handling är vidare orättmätig om den inte medges av nationell lagstiftning.

14.3.4 Art 2 – Olagligt intrång i informationssystem

Enligt denna artikel åläggs medlemsstaterna att kriminalisera handlanden som utgör *olagligt intrång i informationssystem*. För att en handling skall anses som olagligt intrång i informationssystem krävs att gärningsmannen orättmätigt har berett sig tillgång till hela eller delar av informationssystemet och att detta intrång inte kan anses som ringa.

[179] Punkten c kommer ej att behandlas då den faller utanför denna uppsats ramar.
[180] Prop. 2003/04:164, s.8.
[181] Ibid.
[182] Ibid.
[183] Ibid.

Med definitionen i artikel 1 av informationssystem i åtanke innebär detta att intrånget skall ske utan rätt antingen i:

- en eller flera apparater som är sammankopplade eller hör samman med varandra och som utför automatisk behandling av datorbehandlingsbara uppgifter.

Eller i:

- datorbehandlingsbara uppgifter som lagras, behandlas, hämtas eller överförs med denna typ av apparater.

Enligt punkten 2 i artikeln så får medlemsstaterna ställa som rekvisit för att brott skall anses begånget att intrånget sker i en säkerhetsåtgärd.

14.3.5 Art 3 – Olaglig systemstörning

Visst handlande skall av medlemsstaterna kriminaliseras såsom *olaglig systemstörning*. Med olaglig systemstörning avses i artikel 3 en uppsåtlig och orättmätig handling som allvarligt hindrar eller avbryter driften av ett informationssystem. Detta kan ske genom att gärningsmannen; matar in, överför, skadar, raderar, försämrar, ändrar, hindrar flödet av eller omöjliggör åtkomst av datorbehandlingsbara uppgifter. Enligt artikeln står det medlemsstaterna fritt att kräva att handlingen inte är att anse som ringa för att brott skall anses begånget.

14.3.6 Art 4 – Olaglig datastörning

Medlemsstaterna åläggs enligt denna artikel att kriminalisera såsom *olaglig datastörning* handlingar som innebär att en gärningsman; raderar, skadar, försämrar, ändrar, hindrar flödet av eller omöjliggör åtkomst av datorbehandlingsbara uppgifter i ett informationssystem. Handlingarna måste för att anses som olaglig datastörning utföras uppsåtligen och orättmätigt av gärningsmannen. Det står medlemsstaterna fritt att inte kriminalisera denna typ av handlande om den skulle anses såsom ringa.

14.3.7 Art 5 – Anstiftan, medhjälp och försök

Enligt artikeln skall varje medlemsstat tillse att försök, anstiftan och medhjälp till handlingarna i artikel 3,4 (olaglig systemstörning, olaglig datastörning) är straffbara.

Vad gäller olagligt intrång i informationssystem skall medlemsstaterna tillse att anstiftan och medhjälp kriminaliseras. Det står dock varje medlemsstat fritt att välja om försök till olagligt intrång i informationssystem skall kriminaliseras.

14.3.8 Art 6 – Påföljder

Enligt rambeslutet skall medlemsstaterna tillse att gärningarna i artikel 2-5 är belagda med "effektiva, proportionerliga och avskräckande […] påföljder."[184] För olaglig systemstörning samt olaglig datastörning specificeras vidare att det maximala straffet skall vara minst ett till tre års fängelse.

14.3.9 Art 7, 8, 9 – Försvårande omständigheter samt juridiska personer

Då dessa tre artiklar till huvuddel faller utanför denna uppsats ämnesområde behandlas dessa inte. De kan dock återfinnas under appendix B.

14.3.10 Art 10 – Behörighet

Artikel 10 i rambeslutet behandlar frågan om jurisdiktion. En medlemsstat skall anses ha behörighet att pröva brott som specificeras i artiklarna 2-5 om:

- Brottet har begåtts helt eller delvis på dess territorium.
- Brottet har begåtts av en av deras medborgare.
- Brottet har begåtts till förmån för en juridisk person som har sitt huvudsäte i staten.

En stat skall vid bedömande om territoriellbehörighet föreligger, anse sig vara behörig att pröva saken om:

- Gärningsmannen var fysiskt närvarande i dess territorium när brottet begicks, detta oavsett vilket territorium som informationssystemet mot vilken gärningen riktades var beläget.
- Gärningen riktade sig mot ett informationssystem som befann sig på statens territorium oavsett om gärningsmannen fysiskt befann sig på statens territorium eller ej.

Om gärningsmannen är medborgare i en medlemsstat som inte utlämnar eller överlämnar sina medborgare skall medlemsstaten tillse att man vidtar sådana åtgärder att man, om det är lämpligt, kan väcka åtal för gärningar som beskrivs i artikel 2-5 även om gärningen begåtts av en av dess medborgare utanför landets territorium.

[184] Rambeslut om angrepp mot informationssystem, Europeiska Unionens råd 15010/04, Artikel 6.

Om gärningen faller under flera staters jurisdiktion, skall staterna samarbeta för att lösa frågan om lagföringsland. För att lösa frågan skall följande omständigheter beaktas i successivordning:

1. Den stat som har territoriellbehörighet.
2. Den stat där gärningsmannen är medborgare.
3. Den stat vars territorium gärningsmannen påträffades på.

En medlemsstat har rätt att besluta att inte tillämpa behörighet att lagföra en gärningsman baserat på medborgarskap i staten, eller vad gäller juridisk person baserat på huvudsäte i staten. Detta beslut kan antingen gälla kontinuerligt, i särskilda fall eller under särskilda omständigheter. Om en stat beslutar att göra ett dylikt undantag från behörighetsreglerna skall staten underrätta generalsekretariatet eller kommissionen.

14.3.11 Art 12, 13 – Ikraftträdande

Enligt artiklarna träder rambeslutet i kraft samma dag som det offentliggörs i Europeiska unionens officiella tidning. Medlemsstaterna har från denna dag två år till sitt förfogande för att tillse att den nationella lagstiftningen följer rambeslutet.

14.4 Analys

14.4.1 Art 1 – Definitioner

Definitionerna stämmer väl överrens med de definitioner som används både i Europarådets konvention samt i gällande svensk rätt, de har sitt ursprung i både ISO:s definition och OECD:s riktlinjer.[185]

14.4.2 Art 2 – 4 kap. 8, 9c §§ BrB

Artikeln tar sikte på uppsåtliga orättmätiga intrång i informationssystem. Både intrång i informationssystemet i sin helhet eller i del därav täcks in. Med hänsyn till definitionerna i artikel 1 får den svenska bestämmelsen om dataintrång i 4 kap. 9c§ BrB anses väl stämma överrens med artikeln, den gällande definitionen av uppgift för automatisk databehandling motsvarar rambeslutets term datorbehandlingsbara uppgifter. Vidare torde ”rambeslutets krav på att handlingen skall bestå i ett intrång”[186] anses motsvara det svenska *bereda sig tillgång*. Den svenska bestämmelsen måste därför anses som väl överrensstämmande med artikeln.

[185] KOM/2002/0173 slutlig - CNS 2002/0086, Europeiska gemenskapernas officiella tidning nr C 203 E , 27/08/2002, s.0109 – 0113.
[186] Prop. 2003/04:164, s.24.

14.4.3 Art 3 – 4 kap. 9c, 12 kap. 1, 8 kap. 8, 13 kap. 4 §§ BrB

Artikeln avser att kriminalisera handlingar som syftar till att ”uppsåtligen allvarligt hindra eller avbryta driften av ett informationssystem genom att mata in, överföra, skada, radera, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter.”[187] Den svenska bestämmelsen om dataintrång i 4 kap. 9c § BrB täcker delvis in denna typ av förfaranden. I 4 kap. 9c § BrB kriminaliseras gärningar som innebär att gärningsmannen ändrar eller utplånar en upptagning för automatisk databehandling, även att föra in uppgifter i ett register täcks in. Som tidigare nämnts i kapitel 5.4.2 finns inget krav att en eventuell förändring eller utplåning skall vara permanent för att 4 kap. 9c § BrB skall vara tillämplig. Detta innebär att paragrafen överensstämmer med artikeln vad avser denna typ av handlingar.

Att ”uppsåtligen allvarligt hindra eller avbryta driften av ett informationssystem genom att överföra eller hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter”[188] torde däremot inte täckas in av 4 kap. 9c § BrB. Detta så länge det inte görs genom att som tidigare sagts ändra eller utplåna en upptagning för automatisk databehandling. Att exempelvis genomföra en DoS attack torde inte täckas in vare sig av 12 kap. 1 § BrB eller av 4 kap. 9c § BrB. Detta då uppgifterna knappast torde anses som utplånade eller ändrade.[189] Vad avser möjligheterna att använda sig av 12 kap. 1 § BrB om skadegörelse så torde ej heller denna vara tillämplig, dels med tanke på datas kvasimateriella karaktär och dels med tanke på att med skada förutsätts att denna inte är av enbart tillfällig natur. Om däremot angreppet riktar sig mot informationssystemets materiella delar torde tillämpning av 12 kap. 1 § BrB vara möjlig. Straffstadgandet om egenmäktigt förfarande i 8 kap. 8 § BrB torde inte vara tillämplig såvida det ej rör sig om en fysisk databärare då denna gärning torde kräva ett fysiskt besittningstagande och rumslig besittningsrubbning.[190]

Om informationssystemet är att anse som en samhällsviktig resurs torde 13 kap. 4 § BrB om sabotage vara tillämpbar. Exempel kan vara DoS attacker mot en DNS huvudserver eller mot telenätet. Även attacker mot exempelvis SJ:s, kraftbolags eller telebolags datorer torde kunna falla under denna paragraf. För tillämpning av paragrafen krävs inte att skadegörelse har ägt rum, det är tillräckligt att funktionen av resursen allvarligt störs eller förhindras.[191]

---

[187] Rambeslut om angrepp mot informationssystem, Europeiska Unionens råd 15010/04, art.3.
[188] Ibid.
[189] Prop. 2003/04:164, s.25.
[190] Ibid, s.26.
[191] Holmqvist m.fl., Brottsbalken en kommentar, Del II studentutgåva 3, 13:19.

Artikeln visar på ett stort tomrum i svensk lagstiftning, något som ej torde ha kunnat förutses vid Datalagens ikraftträdande. Den snabba tekniska utvecklingen har medfört att även om bestämmelsen som numera är 4 kap. 9c § BrB gavs en teknikneutral utformning kan den varken ses som tillräckligt precis eller bred för den moderna IT-världen.
Detta sammantaget torde leda till att ytterligare lagstiftning krävs för att Sverige skall uppfylla rambeslutet vad avser denna artikel.

14.4.4 Art 4 – 4 kap. 9c, 12 kap. 1 §§ BrB

Artikeln avser att kriminalisera motsvarande handlingar som artikel 3 med skillnaden att handlingarna är riktade mot datorbehandlingsbara uppgifter. Här är det lämpligt att förtydliga att rambeslutet inte enbart avser de program som körs i datorsystemet, utan alla uppgifter som finns i systemet. Som tidigare nämnts stämmer utkastets definitioner i artikel 1 väl överens med de som används i gällande svensk rätt, varvid begreppet datorbehandlingsbara uppgifter kan likställas med begreppet upptagning för automatisk databehandling.

Man kan utläsa ur artikeln att författarna avser att straffbelägga virus och DoS angrepp. Som tidigare nämnts är det straffbelagt enligt svensk lag att olovligen ändra eller utplåna upptagning för automatisk databehandling, samt att i register olovligen föra in upptagningar. Detta innebär att gällande svensk rätt till viss del uppfyller artikelns krav på straffbarhet. Vad som inte täcks in av gällande rätt motsvarar den lucka som identifierades i kapitel 14.4.3.

Svensk rätt kan därmed inte anses uppfylla kraven enligt artikeln, varvid ytterligare lagstiftning torde krävas.

14.4.5 Art 5 – 4 kap. 9b, 10 §§ BrB

Artikeln stadgar att ”anstiftan av och medhjälp till olagligt intrång i informationssystem, olaglig systemstörning, och olaglig datastörning”[192] skall vara straffbelagt. Med hänsyn till vad som tidigare sagts om artiklarna 2,3 och 4 och deras motsvarighet i svensk lagstiftning får gällande rätt anses uppfylla kraven i artikeln vad avser de gärningar som i dag är straffbelagda enligt svensk rätt.

14.4.6 Art 6 – 4 kap. 9c, 12 kap. 1, 13 kap. 4 §§ BrB

Artikeln stadgar att straffen för de handlingar som skall vara kriminaliserade ”skall vara belagda med effektiva, proportionella och avskräckande straffrättsliga påföljder.”[193] Man stadgar att straffen för olaga

[192] Prop. 2003/04:164, s.28.
[193]Ibid, s.29.

systemstörning, samt olaga datastörning enligt artiklarna 3, 4 skall vara belagda med ett maximalt straff bestående av minst ett till tre års fängelse. Maximala straffet för dataintrång enligt 4 kap. 9c § BrB är i dag ett års fängelse, även stadgandena om skadegörelse i 12 kap. 1 § BrB samt sabotage i 13 kap. 4 § BrB uppfyller denna nivå. Detta innebär att Sverige uppfyller rambeslutets krav, vad avser de i dag straffbelagda gärningarna.

14.4.7 Art 10 – 2 kap. 1-4 §§ BrB

Artikeln föreskriver under vilka situationer ett land skall anses ha straffrättslig jurisdiktion över de tidigare beskrivna gärningarna. 2 kap. 1 § BrB stadgar att brott som begås i Sverige skall dömas enligt svensk lag och vid svensk domstol.[194] Enligt svensk rätt anses ett brott begånget där den brottsliga handlingen företogs, fullbordades eller, vid försök där brottet skulle ha fullbordats.[195] Detta innebär i praktiken att så fort någon del av den brottsliga handlingen har ägt rum i Sverige, skall hela handlingen anses som begången i Sverige. Vidare så skall enligt 2 kap. 2 § BrB brott som begås utanför Sverige av svenska medborgare dömas enligt svensk lag, vid svensk domstol. Detta oavsett om rekvisiten i 2 kap. 1,4 §§ BrB är uppfyllda eller ej. Sverige måste därför anses väl uppfylla de krav som ställs i punkterna 1a-b, 2, 3.

Avseende punkten 4 om samarbete mellan medlemsstaterna om fler än en medlemsstat skall anses ha jurisdiktion över ett brott så är detta ej i dag reglerat enligt svensk lag. Däremot så har Sverige tillträtt internationella konventioner som just reglerar denna problematik. Regeringen uttryckte i sin proposition att bestämmelsen innebär en samrådsskyldighet, att formerna för samrådet är fakultativt och att sådana formlösa samråd redan i dag förekommer. [196] Man ansåg därför inte att någon särskild reglering av frågan var nödvändig,[197] en bedömning som även jag anser vara riktig.

Enbart i ett avseende kan inte gällande svensk rätt anses uppfylla artikeln, nämligen punkten 1c. Det finns enligt svensk lag i dag ingen möjlighet för en domstol att anse sig ha jurisdiktion över en gärning som sker utomlands till förmån för en juridisk person som har sitt huvudsäte i Sverige, om inte gärningsmannen har någon anknytning till Sverige. Sverige har dock rätt att enligt punkten 5 avstå från en dylik reglering, dock måste detta anmälas till rådets generalsekretariat samt kommissionen, enligt punkten 6.

Sverige måste anses uppfylla artikelns krav på jurisdiktion i alla avseenden, utom vad avser punkten 1c.

[194] Den så kallade territorialprincipen.
[195] 2 kap. 4 § BrB.
[196] Prop. 2003/04:164, s.32.
[197] Ibid.

14.5 Kommentar till Prop. 2003/04:164

Jag vill här kort kommentera regeringens proposition 2003/04:164 om Sveriges antagande av rambeslut om angrepp mot informationssystem. Propositionen överlämnades till riksdagen den 27 maj 2004, utkastet till rambeslutet stod klart redan den 28 februari 2003 och beslut om dess antagande togs av Europeiska rådet vid dess möte den 25-26 mars 2004. Riksdagsbeslutet om propositionen togs den 27 oktober 2004.

Sammanlagt har det tagit 1 år och 3 månader för regeringen att författa en proposition och ytterligare 5 månader för ett beslut att tas av riksdagen. Detta får anses vara ett normalt tidsförhållande vid dylika ärenden. Vad som däremot slår en när man läser propositionen är den dåliga kvalité den håller. Inga konkreta förslag på förändringar i lagstiftningen ges vilket får anses som anmärkningsvärt. Vidare blev det remissförfarande regeringen använt sig av mycket kritiserat. Man har bland annat från tre av de viktigare remissinstanserna när det gäller denna fråga; PTS, HKV samt RÅ inte inhämtat något skriftligt remissvar utan enbart inhämtat ett utlåtande per telefon. Andra remissinstanser som tillfrågats har fått väldigt kort tid på sig att svara, exempelvis Advokatsamfundet som fick 10 dagar.

Den kritik som framfördes i samband med behandlingen av propositionen rör sig enbart om det förfarande som regeringen har valt att använda sig av;

> *”Advokatsamfundet har i olika sammanhang kritiserat den metod som tillämpas för antagande och genomförande av rambeslut […] kritiken har rört dels att beredningen varit bristfällig så till vida att de instanser som synpunkter inhämtats från varit få och att den tidsram som stått dessa till buds varit kort, dels att konsekvenserna av ett rambeslut inte gått att förutse på grund av att någon färdig analys av lagstiftningsbehovet och ställningstagande från regeringens sida i väsentliga hänseende inte redovisats.”*[198]

> *”Lagstiftning får inte hastas fram och riksdagen bör ges möjlighet att bedöma konsekvenserna av sina beslut. För att säkerställa rättssäkerheten och för att värna en demokratisk lagstiftningsprocess skall därför propositioner om antaganden av rambeslut innehålla förslag till följdlagstiftning.”*[199]

[198] Remissvar från Sveriges Advokatsamfund, 2004-04-28.
[199] Motion till riksdagen 2003/04:Ju31 av Rolf Olsson m.fl. (v).

> *”Sedan ett rambeslut väl godkänts finns det ingen anledning att behandla de grundläggande rättspolitiska frågor som rambeslutet kan ge anledning till. Detta skapar ett demokratiskt problem för Sveriges lagstiftande församling. Då genomförandepropositionen presenteras är riksdagens händer bundna.”*[200]

Som tidigare sagts riktades ingen kritik mot rambeslutets innehåll, något som torde tyda på konsensus angående behovet att förändra lagstiftningen på området.

Regeringen uttrycker i propositionen en önskan att de lagändringar som behövs i möjlig mån görs i dataintrångsbestämmelsen ”Bestämmelsen bör så långt det är möjligt behållas i sin nuvarande utformning och endast kompletteras med de tillägg som är påkallade till följd av rambeslutet.”[201] Exakt hur dessa tillägg skall utformas är som tidigare påtalat ej redovisat av regeringen.

[200] Motion till riksdagen 2003/04:Ju32 av Beatrice Ask m.fl. (m).
[201] Prop. 2003/04:164, s.28.

15 Åtgärdsförslag

15.1 Inledning

De nuvarande bestämmelserna i svensk lag som berör dataintrång är nära nog 30 år gamla. Under dessa 30 år har teknikens utveckling och användning ökat i en takt som ingen kunde förutspå. Även om lagstiftarnas syfte och önskan var att de lagar som berör dataintrång skulle ha en teknikneutral utformning i syfte att vara framtidssäkra, kan vi i dag konstatera att lagarna släpar efter. Den genomgång av relevant lagstiftning som jag har företagit visar på flera stora brister i svensk lagstiftning. Vissa handlingar som kan sättas i samband med data- och datorrelaterad brottslighet faller helt utanför lagarnas tillämpningsområde. Andra handlingar som i och för sig faller innanför lagarnas tillämpningsområde, ses ej som de allvarliga brott de är, något som tydliggörs vid domstolarnas straffmätning.

Ett antal åtgärder behöver vidtas för att svensk lagstiftning skall anses följa både Cyberbrottskonventionen och rambeslutet. Jag kommer i detta kapitel att ge förslag på åtgärder som jag anser vara behövliga, dels för att följa nämnda konvention och rambeslut och dels för att på ett mer effektivt sätt motverka problemet med dataintrång.

15.2 Lagstiftning

Den svenska lagstiftningen lider som tidigare sagts av luckor i dess tillämpningsområde. De enligt min åsikt två största bristerna är att hindrande av en funktion eller flöde av data inte täcks in av lagstiftningen såvida dessa inte genomförs genom att bereda sig tillgång till upptagning för ADB, ändra, radera data eller i register föra in. Detta innebär att handlingar såsom DoS och virusattacker inte är straffbara enligt svensk lag.

Vidare anser jag att faktumet att avlyssning av datatrafik via radio inte är otillåtet vara ett stort problem. Många författare har tidigare anfört att det faktum att upptagning av RöS inte är straffbart enligt svensk lag är ett av de största problemen. Detta är något jag ej kan hålla med om, dagens utveckling mot att mer och mer använda sig av trådlös teknik istället för trådburna nätverk har gjort det näst intill onödigt att använda sig av komplicerade apparatur i syfte att avlyssna data genom RöS. Det är mycket enklare att använda ett trådlöst nätverkskort och ett gratis program hämtat från Internet.

Det faktum att begreppet upptagning för ADB ej blivit klart definierat anser jag är en del av problematiken. Att inte likställa upptagningsbegreppet med det traditionella handlingsbegreppet ser jag som en nackdel. Om detta varit

fallet torde flera av dagens gällande lagrum, exempelvis 12 kap. 1 § BrB om skadegörelse och 8 kap. 8 § BrB om egenmäktigt förfarande vara tillämpliga på exempelvis virus- och DoS attacker. Med tanke på det lagstiftningsarbete som nu måste företas efter godkännandet av rambeslutet om angrepp mot informationssystem torde dock denna fråga förlora något av sin vikt.

För att Sverige skall kunna anses följa de internationella avtal som tidigare nämnts måste förändringar ske på dessa tre punkter. Om Sverige förändrar sin lagstiftning på så sätt att den uppfyller dessa internationella avtal anser jag att den resulterande lagstiftningen mer än väl uppfyller det behov som finns på området.

15.2.1 Utformning

Exakt hur lagstiftningen bör utformas är något som jag ej kan uttala mig om. Vad jag dock anser vara önskvärt är att eventuell ny lagstiftning inte genomförs genom att förändra redan gällande paragrafer i BrB. Jag ser hellre att nya paragrafer tas in i 4 kapitlet BrB, detta av tre anledningar:

1. Undvika problem vid tillämpning genom att behålla den systematik som finns i dag.
2. Genom att klart uttrycka att gärningarna berör dator- och datarelaterade brott samt i viss mån elektronisk kommunikation uppnås en klarhet vad gäller tillämplighet och avgränsning mot exempelvis 4 kap. 8 § BrB.
3. Genom att klart uttrycka vilka typer av gärningar som är otillåtna uppnås en allmänpreventiv effekt, som ej kan anses finnas i dag.

15.2.2 Grov brottsrubricering

Avsaknaden av en grov brottsrubricering vad gäller dataintrång har enligt mig medfört att domstolarnas straffmätning haltar. Man kan vid genomgång av praxis se att gärningar som inneburit stora ekonomiska skador för offret leder till motsvarande påföljd som de som ej lett till någon påvisbar ekonomisk skada.

En grov brottsrubricering skulle kunna ta sikte dels på tillvägagångssätt, ekonomisk skada eller annan skada, exempelvis kränkning av personlig integritet.

15.3 Andra åtgärder

Jag har under arbetets gång vid flera tillfällen observerat att förtroendet för rättsväsendets förmåga att utreda och lagföra denna typ av brottslighet är mycket låg. Genom att på ett tydligare sätt informera om exempelvis polisens IT-brottsrotlars uppgifter och kompetens torde detta förtroende hos allmänheten öka. Vidare torde en skärpning av de straff som utdöms vid lagföring ge signaler att denna typ av brott är något som rättsväsendet ser mycket allvarligt på.

16 Avslutande analys

Den svenska lagstiftningen på området dator- och datarelaterade brott är till stor del över 30 år gammal. Utgångspunkten vid lagstiftningen var att införa teknikneutrala bestämmelser, vilket medförde att bestämmelsen om dataintrång i 4 kap. 9c § BrB fick en väldigt allmänt hållen utformning. Lagstiftarens önskan att på så sätt framtidssäkra bestämmelsen har till viss del infriats, dock måste man med den tekniska utvecklingen som bakgrund anse den nuvarande lagstiftningen vara otillräcklig.

När 21 § Datalagen tillkom var enligt lagstiftarna det troligaste scenariot, vad avser externa datorintrång, att någon bröt sig in i ett utrymme och beredde sig fysisk access till en datorterminal eller anläggning. Med detta som bakgrund är det inte svårt att förstå varför handlingar såsom DoS och virus ej täcks in av lagstiftningen. I dag måste vi anse detta vara det minst troliga scenariot.

Att lagstiftningen fortfarande är tillämplig i många fall, såsom visats i flera rättsfall får anses bero på den allmänna utformning som tidigare påtalats.

Att Sverige nu har godkänt Europeiska Unionens råds rambeslut om angrepp mot informationssystem får ses som något väldigt positivt. Rambeslutet är ett väl genomtänkt dokument, som dels täcker in de i dag förekommande gärningarna och dels får anses som teknikneutral och framtidssäker. Det lagstiftningsarbete som nu blir aktuellt för Sverige torde medföra att lagstiftningen uppdateras och förs in i 2000-talet. En ratificering av Europarådets konvention om Cyberbrottslighet torde även den medföra positiva effekter för rättsläget, framförallt då denna sträcker sig längre än rambeslutet i många fall.

Vad gäller tillämpningen av *de lege lata* får domstolarna anses vara välbevandrade vad avser tillämpningsområdet för lagarna. Jag anser dock att kritik måste framföras vad avser straffmätningen. Då statistiken visar att huvuddelen av gärningsmännen är under 17 år torde detta även speglas vid straffmätningen. Enligt min mening lägger domstolarna allt för stor vikt vid det faktum att gärningsmännen är unga, tidigare ostraffade och att de lever under ordnade förhållande. Dataintrång kan inte jämföras med andra brott, det kräver nämligen vissa resurser både mentala och materiella, som enligt min mening inte torde finnas bland ”normala” unga lagöverträdare. Att utdöma 50 dagsböter á 30 kronor som i KTH/SU fallet kan jämföras med det straff en hacker dömdes till för dataintrång i USA 2004. Utan att någon faktisk skada kunde fastställas dömdes mannen till 9 års fängelse.

Det faktum att antalet anmälda dataintrång konstant ökar, utan att vi kan se en motsvarande ökning av antalet åtal och domar är oroande. Orsaken till denna diskrepans har jag ej lyckat klarlägga. Flera möjliga faktorer kan dock ses spela in; ovilja att anmäla, felaktig uppfattning om rättsväsendets intresse, samt polis och åklagares dåliga resurser, kan vara några anledningar. Enligt min mening kan ytterligare en anledning vara den dåliga kunskapsnivå som finns inom juridiska kretsar avseende dator- och datarelaterade gärningar, något som jag med denna uppsats hoppas råda bot på.

Bilaga A

Utdrag ur Convention on Cybercrime, 23,XI,2001

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c "service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;

d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Bilaga B

Rambeslutet om angrepp mot informationssystem

RÅDETS RAMBESLUT 2005/…/RIF

av den

om angrepp mot informationssystem

EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA RAMBESLUT

med beaktande av Fördraget om Europeiska unionen, särskilt artiklarna 29, 30.1 a, 31.1 e och 34.2 b,

med beaktande av kommissionens förslag

med beaktande av Europaparlamentets yttrande[202], och

av följande skäl:

(1) Syftet med detta rambeslut är att förbättra samarbetet mellan rättsliga och andra behöriga myndigheter, inbegripet polismyndigheter och andra specialiserade brottsbekämpande organ i medlemsstaterna, genom tillnärmning av medlemsstaternas strafflagstiftning på området för angrepp mot informationssystem.

(2) Det har konstaterats att det förekommer angrepp mot informationssystem, särskilt till följd av hotet från den organiserade brottsligheten, och det finns en stigande oro för terroristattacker mot de informationssystem som ingår i medlemsstaternas vitala infrastruktur. Detta utgör ett hot mot skapandet av ett säkrare informationssamhälle och ett område med frihet, säkerhet och rättvisa och kräver därför motåtgärder på EU-nivå.

(3) Ett effektivt svar på dessa hot kräver en samlad syn på nät- och informationssäkerhet, vilket betonas i handlingsplanen eEurope, i kommissionens meddelande "Nät- och informationssäkerhet: förslag till en europeisk strategi" och i rådets resolution av den 6 december 2001 om en gemensam inställning och särskilda åtgärder på området för nät- och informationssäkerhet.[203]

(4) Behovet av att ytterligare öka medvetenheten om problemen som har att göra med informationssäkerhet och ge praktisk hjälp har också betonats i Europaparlamentets resolution av den 5 september 2001.

(5) Stora klyftor och skillnader i medlemsstaternas lagstiftning på detta område kan försvåra kampen mot organiserad brottslighet och terrorism och komplicera ett effektivt polisiärt och rättsligt samarbete när det gäller angrepp mot

[202] Yttrandet avgivet den 22 oktober 2002 (EUT C 300 E, 11.12.2003, s.26)
[203] EGT C 43, 16.2.2002, s.2

informationssystem. De moderna informationssystemens nationsöverskridande och gränslösa karaktär innebär att angrepp mot sådana system ofta är gränsöverskridande, vilket understryker det trängande behovet av ytterligare insatser för att tillnärma strafflagstiftningen på detta område.

(6) Rådets och kommissionens handlingsplan för att på bästa sätt genomföra bestämmelserna i Amsterdamfördraget om upprättande av ett område med frihet, säkerhet och rättvisa[204], Europeiska rådet i Tammerfors den 15–16 oktober 1999, Europeiska rådet i Santa Maria da Feira den 19–20 juni 2000, kommissionen i "resultattavlan" och Europaparlamentet i sin resolution av den 19 maj 2000 anger eller uppmanar till lagstiftningsåtgärder mot högteknologisk brottslighet, inklusive gemensamma definitioner, kriminaliseringar och påföljder.

(7) Det arbete som utförs av internationella organisationer, särskilt Europarådets insatser för tillnärmning av strafflagstiftning och G8:s arbete för gränsöverskridande samarbete på området för högteknologisk brottslighet, måste kompletteras genom att det fastställs en gemensam strategi på detta område inom Europeiska unionen. Detta krav utvecklades ytterligare i kommissionens meddelande till rådet, Europaparlamentet, Ekonomiska och sociala kommittén och Regionkommittén "Ett säkrare informationssamhälle – ökad säkerhet i informationsinfrastrukturen och bekämpning av datorrelaterad brottslighet".

(8) Strafflagstiftningen om angrepp mot informationssystem bör tillnärmas i syfte att få till stånd största möjliga polisiära och rättsliga samarbete när det gäller brott som hänför sig till angrepp mot informationssystem och att bidra till kampen mot organiserad brottslighet och terrorism.

(9) Alla medlemsstater har ratificerat Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter. Personuppgifter som behandlas i samband med genomförandet av detta rambeslut bör skyddas i enlighet med principerna i den nämnda konventionen.

(10) Gemensamma definitioner på detta område, särskilt av informationssystem och datorbehandlingsbara uppgifter, betyder mycket för att säkra att detta rambeslut tillämpas enhetligt i medlemsstaterna.

(11) Det finns ett behov av att fastställa en gemensam inställning i fråga om brottsrekvisit, genom att gemensamt kriminalisera olagligt intrång i informationssystem, olaglig systemstörning och olaglig datastörning.

(12) För att kunna bekämpa IT-relaterad brottslighet bör varje medlemsstat säkerställa effektivt rättsligt samarbete avseende brott vilka bygger på de typer av handlande som avses i artiklarna 2, 3, 4 och 5.

(13) Det finns ett behov av att undvika att kriminaliseringen går för långt, särskilt i fråga om ringa fall, liksom att undvika att kriminalisera rättighetshavare och behöriga personer.

(14) Det finns ett behov av att medlemsstaterna föreskriver påföljder för angrepp mot informationssystem. Dessa påföljder skall vara effektiva, proportionella och avskräckande.

[204] EGT C 19, 23.1.1999, s.1

(15) Det är lämpligt att föreskriva strängare påföljder när ett angrepp mot ett informationssystem sker inom ramen för en sådan kriminell organisation som avses i gemensam åtgärd 98/733/RIF av den 21 december 1998 om att göra deltagande i en kriminell organisation i Europeiska unionens medlemsstater till ett brott[205]. Det är också lämpligt att föreskriva strängare påföljder när ett sådant angrepp har orsakat allvarliga skador eller har påverkat väsentliga intressen.

(16) Åtgärder bör även förutses för samarbete mellan medlemsstaterna, i syfte att säkra effektiva insatser mot angrepp mot informationssystem. Medlemsstaterna bör därför för utbyte av uppgifter använda sig av det befintliga nät med operativa kontaktpunkter som omnämns i rådets rekommendation av den 25 juni 2001 om kontaktpunkter som upprätthåller ett öppethållande dygnet runt för bekämpning av högteknologisk brottslighet[206].

(17) Eftersom målen för detta rambeslut, nämligen att se till att angrepp mot informationssystem i medlemsstaterna blir föremål för effektiva, proportionella och avskräckande straffrättsliga påföljder och att förbättra och uppmuntra rättsligt samarbete genom att undanröja eventuella komplikationer, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna, då bestämmelserna måste vara gemensamma och förenliga med varandra, och de därför bättre kan uppnås på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i EG-fördraget. I enlighet med proportionalitetsprincipen i samma artikel går detta rambeslut inte utöver vad som är nödvändigt för att uppnå dessa mål.

(18) I detta rambeslut respekteras de grundläggande rättigheter och iakttas de principer som erkänns genom artikel 6 i Fördraget om Europeiska unionen och återspeglas i Europeiska unionens stadga om de grundläggande rättigheterna, framför allt i kapitlen II och VI i denna.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Definitioner

I detta rambeslut används följande beteckningar med de betydelser som här anges:

a) informationssystem: en apparat eller en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av datorbehandlingsbara uppgifter, samt datorbehandlingsbara uppgifter som lagras, behandlas, hämtas eller överförs med hjälp av dessa för att de skall kunna drivas, användas, skyddas och underhållas.

b) datorbehandlingsbara uppgifter: framställning av fakta, information eller begrepp i en form som lämpar sig för behandling i ett informationssystem, inklusive program som lämpar sig för att få ett informationssystem att utföra en viss uppgift.

[205] EGT L 351, 29.12.1998, s.1
[206] EGT C 187, 3.7.2001, s.5

c) juridisk person: enhet som har sådan status enligt tillämplig lagstiftning, med undantag av stater eller andra offentliga organ vid utövandet av de befogenheter som de har i egenskap av statsmakter samt internationella offentliga organisationer.

d) orättmätigt: intrång eller störning som sker utan tillstånd från ägaren eller annan rättighetshavare till systemet eller del av detta eller som inte medges i den nationella lagstiftningen.

Artikel 2

Olagligt intrång i informationssystem

1. Varje medlemsstat skall vidta de åtgärder som är nödvändiga för att straffbelägga uppsåtligt orättmätigt intrång i ett informationssystem som helhet eller en del av ett sådant system, åtminstone i fall som inte är ringa.

2. Varje medlemsstat får besluta att det handlande som avses i punkt 1 endast skall kriminaliseras när brottet begås genom intrång i en säkerhetsåtgärd.

Artikel 3

Olaglig systemstörning

Varje medlemsstat skall vidta de åtgärder som är nödvändiga för att se till att det är straffbart att uppsåtligen allvarligt hindra eller avbryta driften av ett informationssystem genom att mata in, överföra, skada, radera, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter, när gärningen utförs orättmätigt, åtminstone i fall som inte är ringa.

Artikel 4

Olaglig datastörning

Varje medlemsstat skall vidta de åtgärder som är nödvändiga för att se till att det är straffbart att uppsåtligen radera, skada, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter i ett informationssystem, när gärningen utförs orättmätigt, åtminstone i fall som inte är ringa.

Artikel 5

Anstiftan, medhjälp och försök

1. Varje medlemsstat skall straffbelägga anstiftan av och medhjälp till brott som avses i artiklarna 2, 3 och 4.

2. Varje medlemsstat skall straffbelägga försök till de brott som avses i artiklarna 2, 3 och 4.

3. Varje medlemsstat får besluta att inte tillämpa punkt 2 för de brott som avses i artikel 2.

Artikel 6

Påföljder

1. Varje medlemsstat skall vidta de åtgärder som är nödvändiga för att se till att de brott som avses i artiklarna 2, 3, 4 och 5 är belagda med effektiva, proportionella och avskräckande straffrättsliga påföljder.

2. Varje medlemsstat skall vidta de åtgärder som är nödvändiga för att se till att de brott som avses i artiklarna 3 och 4 är belagda med straffrättsliga påföljder som innebär ett maximistraff på minst ett till tre års fängelse.

Artikel 7

Försvårande omständigheter

1. Varje medlemsstat skall vidta de åtgärder som är nödvändiga för att se till att det brott som avses i artikel 2.2 och de brott som avses i artiklarna 3 och 4 är belagda med straffrättsliga påföljder som innebär ett maximistraff på minst två till fem års fängelse, när de begås inom ramen för en sådan kriminell organisation som avses i gemensam åtgärd 98/733/RIF, oberoende av den påföljdsnivå som anges i den gemensamma åtgärden.

2. En medlemsstat får även vidta de åtgärder som avses i punkt 1, när brottet har orsakat allvarliga skador eller påverkat väsentliga intressen.

Artikel 8

Juridiska personers ansvar

1. Varje medlemsstat skall vidta de åtgärder som är nödvändiga för att se till att juridiska personer kan ställas till ansvar för brott som avses i artiklarna 2, 3, 4 och 5 och som begås till deras förmån av en person som agerar antingen enskilt eller som en del av den juridiska personens organisation och har en ledande ställning inom den juridiska personen, grundad på

a) befogenhet att företräda den juridiska personen, eller

b) befogenhet att fatta beslut på den juridiska personens vägnar, eller

c) befogenhet att utöva kontroll inom den juridiska personen.

2. Utöver de fall som anges i punkt 1 skall medlemsstaterna se till att en juridisk person kan ställas till ansvar när brister i övervakning eller kontroll som skall utföras av en sådan person som avses i punkt 1 har gjort det möjligt för en person som är underställd den juridiska personen att till förmån för denna juridiska person begå de brott som avses i artiklarna 2, 3, 4 och 5.

3. En juridisk persons ansvar enligt punkterna 1 och 2 skall inte utesluta lagföring av fysiska personer som är gärningsmän vid, anstiftare av eller medhjälpare till de brott som avses i artiklarna 2, 3, 4 och 5.

Artikel 9

Påföljder för juridiska personer

1. Varje medlemsstat skall vidta de åtgärder som är nödvändiga för att se till att en juridisk person som har fällts till ansvar i enlighet med artikel 8.1 kan bli föremål för effektiva, proportionella och avskräckande påföljder, som skall innefatta bötesstraff eller administrativa avgifter och som får innefatta andra påföljder, som

a) fråntagande av rätt till offentliga förmåner eller stöd,

b) tillfälligt eller permanent näringsförbud,

c) rättslig övervakning, eller

d) rättsligt beslut om upplösning av verksamheten.

2. Varje medlemsstat skall vidta de åtgärder som är nödvändiga för att se till att en juridisk person som har fällts till ansvar i enlighet med artikel 8.2 kan bli föremål för effektiva, proportionella och avskräckande påföljder eller åtgärder.

Artikel 10

Behörighet

1. Varje medlemsstat skall fastställa sin behörighet beträffande de brott som avses i artiklarna 2, 3, 4 och 5, när brottet har begåtts

a) helt eller delvis på dess territorium, eller

b) av en av dess medborgare, eller

c) till förmån för en juridisk person som har sitt huvudkontor på medlemsstatens territorium.

2. Varje medlemsstat skall vid fastställandet av sin behörighet enligt punkt 1 a se till att behörigheten innefattar fall där

a) brottslingen är fysiskt närvarande på medlemsstatens territorium när brottet begås, oavsett om brottet riktar sig mot ett informationssystem på denna medlemsstats territorium eller inte, eller

b) brottet riktar sig mot ett informationssystem på medlemsstatens territorium, oavsett om brottslingen är fysiskt närvarande på detta territorium när brottet begås eller inte.

3. En medlemsstat som enligt sin lagstiftning ännu inte utlämnar eller överlämnar sina egna medborgare skall vidta de åtgärder som är nödvändiga för att fastställa sin behörighet i fråga om och, när det är lämpligt, väcka åtal för de brott som avses i artiklarna 2, 3, 4 och 5, när de har begåtts av en av landets medborgare utanför landets territorium.

4. När ett brott faller under fler än en medlemsstats behörighet och vilken som helst av dessa stater kan lagföra brottet på grundval av samma omständigheter, skall de berörda medlemsstaterna samarbeta för att avgöra vilken av dem som skall lagföra brottslingarna, för att, om möjligt, centralisera lagföringen till en enda medlemsstat. I detta syfte kan medlemsstaterna anlita de organ eller mekanismer som inrättats inom Europeiska unionen för att underlätta samarbetet mellan deras rättsliga myndigheter och samordningen av deras verksamhet. Följande omständigheter får beaktas i successiv ordning:

– Medlemsstaten skall vara den inom vars territorium brotten har begåtts enligt punkt 1 a och punkt 2.

– Medlemsstaten skall vara den i vilken gärningsmannen är medborgare.

– Medlemsstaten skall vara den på vars territorium gärningsmannen påträffats.

5. En medlemsstat får besluta att inte eller endast i särskilda fall eller under särskilda omständigheter tillämpa de bestämmelser om behörighet som anges i punkt 1 b och 1 c.

6. Medlemsstaterna skall underrätta rådets generalsekretariat och kommissionen när de beslutar att tillämpa punkt 5, i förekommande fall med uppgift om i vilka särskilda fall eller under vilka särskilda omständigheter beslutet gäller.

Artikel 11

Utbyte av uppgifter

1. För utbyte av uppgifter om de brott som avses i artiklarna 2, 3, 4 och 5 skall medlemsstaterna, med iakttagande av bestämmelser om dataskydd, säkerställa att de använder det befintliga nät med operativa kontaktpunkter som kan nås dygnet runt alla dagar i veckan.

2. Varje medlemsstat skall underrätta rådets generalsekretariat och kommissionen om sin utsedda kontaktpunkt för utbyte av uppgifter om brott som avser angrepp mot informationssystem. Generalsekretariatet skall vidarebefordra dessa uppgifter till de andra medlemsstaterna.

Artikel 12

Genomförande

1. Medlemsstaterna skall vidta de åtgärder som är nödvändiga för att följa bestämmelserna i detta rambeslut senast den ...[*].

2. Senast den…[*] skall medlemsstaterna till rådets generalsekretariat och kommissionen överlämna texten till bestämmelser genom vilka de skyldigheter som ålagts dem enligt detta rambeslut införlivas med deras nationella lagstiftning.

[*] Två år efter det att detta rambeslut har trätt i kraft.
[*] Två år efter det att detta rambeslut har trätt i kraft.
[**] 30 månader efter det att detta rambeslut har trätt i kraft.

Senast den ...** skall rådet, på grundval av en rapport som skall utarbetas utifrån information och en skriftlig rapport från kommissionen, bedöma i vilken utsträckning medlemsstaterna har följt bestämmelserna i detta rambeslut.

Artikel 13

Ikraftträdande

Detta rambeslut träder i kraft samma dag som det offentliggörs i Europeiska unionens officiella tidning.

Utfärdat i Bryssel den

På rådets vägnar
Ordförande

Litteraturförteckning

Offentligt tryck

Lagar

SFS 2003:389	Lag om elektronisk kommunikation
SFS 1998:204	Personuppgiftslag
SFS 1990:409	Lag om skydd av företagshemligheter
SFS 1973:289	Datalag
SFS 1962:700	Brottsbalk

Propositioner

Prop. 2003/04:164	Sveriges antagande av rambeslut om angrepp mot informationssystem
Prop. 1997/98:44	Personuppgiftslag
Prop. 1993/94:130	Ändringar i brottsbalken m.m.
Prop. 1985/86:65	med förslag till ändringar i brottsbalken m.m.

Motioner

2003/04:Ju31	Motion till riksdagen av Rolf Olsson m.fl. (v)
2003/04:Ju32	Motion till riksdagen av Beatrice Ask m.fl. (m)

Remissvar

R-2004/0495	Remissvar från Sveriges Advokatsamfund, 2004-04-28

Offentliga utredningar

SOU 1992:110	*Information och den nya Informationsteknologin – straff- och processrättsliga frågor m.m.,* Datastraffrättsutredningen
SOU 1992:70	*Telelag*, Betänkande av Telelagsutredningen
SOU 1991:107	*Lag om radiokommunikation, m.m.,* Betänkande av Frekvensrättsutredningen
SOU 1983:50	*Översyn av lagstiftningen om förmögenhetsbrott utom gäldenärsbrott*, Förmögenhetsbrottsutredningen
SOU 1972:47	*Data och integritet*, Offentlighets- och sekretesslagstiftningskommittén

Europarådet

Convention on Cybercrime, Budapest, 23.XI.2001
Explanatory report to the convention on Cybercrime, ETS No. 185

Europeiska Unionen

15010/04, 17.1.2005	Rådets rambeslut om angrepp mot informationssystem, CNS 2002/0086
EGT C 19, 23.1.1999	Handlingsplan för att på bästa sätt genomföra bestämmelserna i Amsterdamfördraget om upprättande av ett område med frihet, säkerhet och rättvisa,
EGT C 203 E, 27.8.2002	Förslag till rådets rambeslut om angrepp mot informationssystem, KOM/2002/0173 slutlig CNS 2002/0086
EUT C 300 E, 11.12.2003	Betänkande om förslaget till rådets rambeslut om angrepp mot informationssystem, A5-0328/2002

Litteratur

Holmqvist L, m.fl.	Brottsbalken en kommentar Del I, upplaga 3, studentutgåva, Nordstedts Juridik AB, Göteborg 2002
Holmqvist L, m.fl.	Brottsbalken en kommentar Del II, upplaga 3, studentutgåva, Nordstedts Juridik AB, Göteborg 2002
Jareborg N	Straffrättens gärningslära, Fritzes förlag, Malmö 1995
Jareborg N	Straffrättens ansvarslära, Iustus förlag, Uppsala 1994
National Encyklopedin	Band 4, Bokförlaget Bra Böcker, Höganäs 1990
Silvander J	Dator- och datarelaterade brott, Lund 2004
Silvander J	Dator- och datarelaterade förmögenhetsbrott utom borgenärsbrotten, Lund 1998
SIS	Dataordboken SS 011601 utgåva 4, SIS, Stockholm 1989
Svenska akademien	Svenska akademiens ordlista över svenska språket,
upplaga	12, tryckning 4, Svenska akademien, Stockholm 1999
Övrigt tryck	
BRÅ	Rapport 2000:2 IT-relaterad brottslighet, Brottsförebyggande rådet, Stockholm 2000
Computer Security Institute	CSI/FBI Computer Crime and Security Survey, 2004
Post & Telestyrelsen	Analys av hotbilden för IT-incidenter, Bilaga 4 till rapport ”Förutsättningar för att inrätta en särskild funktion för IT-incidenthantering” Dnr 99-19448, Stockholm 2000
Wranghult H	Datakriminalitet – Hackers, insiders och datorstödd brottslighet, RPS rapport 1988:5, Rikspolisstyrelsen, Stockholm 1988
Riksdagens utredningstjänst	PM Dataintrång, Dnr 2004:2450, 2004-12-20
Artiklar	
Nylén L	”Fragglarna” – knäckte NASA:s koder, Nordisk Kriminalkrönika 2001
Nylén L	Skurkar i cyberspace, Nordisk Kriminalkrönika, 1999
Karlberg L-A	Fördubbling av it-brott på fem år, NyTeknik, 040419
Carlsson T	Tips för e-spanare, NyTeknik, 040130
Carlsson T	Svensk polis klarar inte internationella IT-brott, NyTeknik 030430
Kleja M	Sverige rustar för krig mot hackarna, NyTeknik 030129
Carlsson T	Allt fler brott mot datalagen anmäls till polisen, NyTeknik 991007
Bjurman T	IT brottsbekämpningen halkar efter bovarna, IDG 040623

Internet källor (2005-04-10)

http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=19/10/04&CL=ENG
http://conventions.coe.int/treaty/en/Reports/Html/185.htm
http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm
http://dictionary.reference.com/search?q=hack
http://hacks.mit.edu/Hacks/
http://news.bbc.co.uk/1/hi/sci/tech/1541252.stm
http://www.bra.se/
http://www.cert.org/stats/cert_stats.html
http://www.fbi.gov/pressrel/pressrel00/mafia080700.htm
http://www.securitylex.org/glossary#hacker,%20hacking

Rättsfallsförteckning

Svea hovrätt	B7095-02, 2003-12-16
Svea hovrätt	B10958-02, 2003-09-01
Svea hovrätt	B5413-01, 2002-11-25
Svea hovrätt	B5647-02, 2002-10-07
Eskilstuna tingsrätt	B506-02, 2002-04-16
Gotlands tingsrätt	B114-01, 2001-06-14
Gävle tingsrätt	B12-97, 1998-11-27
Kalmar tingsrätt	B322-04, 2004-03-25
Katrineholms tingsrätt	B61-02, 2002-06-12
Lunds tingsrätt	B1914-97, 1998-02-05
Nacka tingsrätt	B565-02, 2002-04-19
Stockholms tingsrätt	B7618-00, 2002-11-21
Stockholms tingsrätt	B11-7613-95, 1996-05-01
Södertälje tingsrätt	B1260-99, 2000-02-28