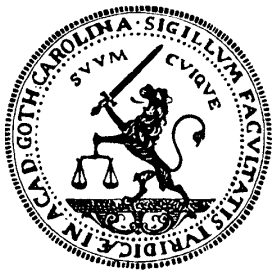

JURIDISKA FAKULTETEN
vid Lunds universitet

Marie-Louise Collin

Dataintrång

- en granskning av den gällande lagstiftningens omfattning och begränsning

Examensarbete
20 poäng

Handledare: Per Ole Träskman

Straffrätt och IT-rätt

HT 2001

Innehåll

Förord

Valet av ämne för ett examensarbete kan ske på flera olika sätt. Vissa har redan tidigt under utbildningens gång bestämt sig för vilket ämne de vill fördjupa sig i under den sista terminen. Andra (författaren inkluderat) väntar in i det sista med att fatta detta avgörande beslut och gör valet närmast av en slump. Detta behöver inte betyda att uppgiften blir mindre intressant. Tvärtom har jag funnit det väldigt stimulerande att skriva detta fördjupande arbete inom ett område som jag tidigare enbart hade berört flyktigt under utbildningens gång. Och framför allt har det inneburit en stor utmaning. Så här i efterhand kan jag konstatera att det hade underlättat om mina datakunskaper varit något mer omfattande. Men varför välja den lättaste vägen.

Under arbetets gång har jag vid ett flertal tillfällen haft frågor och funderingar och jag vill i detta förord passa på att tacka dem som så välvilligt ställt upp med svar. Framför allt vill jag rikta ett stort tack till Lotta Gustavsson på Justitiedepartementet och till kriminalinspektör Markus Küchler på Försvarshögskolan som varit till stor hjälp med både litteraturtips och kommentarer. Jag vill även tacka dem som under arbetets gång läst igenom min uppsats och kommit med frågor och synpunkter. Avslutningsvis vill jag även ge min handledare professor Per-Ole Träskman ett stort tack för att han givit mig vägledning i arbetet.

Lund, december 2001

Marie-Louise Collin

Förkortningar

AD	Arbetsdomstolen
ADB	Automatisk databehandling
BrB	Brottsbalken
BRÅ	Brottsförebyggande rådet
DN	Dagens Nyheter
Ds	Departementsserien
DSU	Datastraffrättsutredningen
EMRK	Europakonventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna
ISO	International Organization for Standardization
IT	Informationsteknologi
JO	Justitieombudsmannen
KTH	Kungliga Tekniska Högskolan
NJA	Nytt Juridiskt Arkiv
OSK	Offentlighets- och sekretesslagstiftningskommittén
Prop.	Proposition
PTS	Post- och telestyrelsen
PuL	Personuppgiftslagen
RFV	Riksförsäkringsverket
RH	Rättsfall från hovrätterna
RRV	Riksrevisionsverket
SAF	Svenska arbetsgivareföreningen

SIS	Standardiseringskommissionen i Sverige
SOU	Statens offentliga utredningar
SU	Stockholms Universitet

1 Inledning

1.1 Bakgrund

Under efterkrigstiden har det skett en snabb utveckling av system för automatisk databehandling (ADB) och dessa s.k. informationssystem har haft stor betydelse för och inverkan på det traditionella informationsutbytet. Det samhälle vi lever i idag präglas till stor del av den nya informationsteknologin och det brukar ibland benämnas IT-samhället. Den tekniska utvecklingen har skapat nya möjligheter för kommunikation mellan människor, men den har även bidragit till nya möjligheter att begå brott. Denna nya grupp av brott vilka har gemensamt att det finns en relation till datorteknik brukar kallas för IT-relaterad brottslighet och kategorin omfattar en rad brott som t.ex. virus, datorbedrägeri och dataintrång. Flertalet av dessa IT-relaterade brott täcks in av redan befintliga teknikneutrala straffbestämmelser, men i den svenska lagstiftningen har även några lagrum införts som specifikt tar sikte på IT-relaterad brottslighet, däribland BrB 4:9c som reglerar dataintrång.

Bestämmelsen om dataintrång infördes som ett komplement till den redan befintliga lagstiftningen som fanns till skydd för informationsintrång. Till följd av den snabba tekniska utvecklingen uppstod nya möjligheter att förvara uppgifter och det uppstod ett behovet av att skydda denna nya typ av information i form av datalagrade uppgifter. Sverige införde redan 1973 som första land en bestämmelse om dataintrång som tar sikte på vissa sorters informationsintrång framför allt hacking.[1] Under de nära trettio år som passerat sedan den första lagregeln om dataintrång infördes i den dåvarande datalagen har bestämmelsen endast genomgått mindre förändringar. Idag återfinns lagregeln i BrB 4:9c och den är i princip identisk med bestämmelsen från 1973. Detta trots att informationsteknologin har utvecklats enormt under motsvarande period och genomgått omfattande förändringar.

På senare tid har en rad kritiska röster höjts mot den befintliga lagstiftningen om dataintrång, och ett flertal utredningar har tillsats för att undersöka huruvida brottsbalkens bestämmelse är i behov av reformering. Frågan har uppstått om IT-utvecklingen har förändrat förutsättningarna för tillämpning av BrB 4:9c och om det finns något behov av att reformera lagstiftningen. Med anledning av antagandet av Europarådets konvention om cyber-brottslighet, vilken är den första internationella traktaten som reglerar IT-relaterad brottslighet, har det återigen blivit intressant att se över hur väl den svenska regleringen är anpassad till det moderna IT-samhället.

[1] SOU 1992:110, s. 61-62. Se vidare i kapitel 2.4 om hacking.

1.2 Syfte

Syftet med denna uppsats är att närmare granska dataintrång. Avsikten är att undersöka omfattningen av den nuvarande lagregleringen av brottet för att avgöra vilka gärningar som täcks in av den gällande lagstiftningen, samt att studera hur paragrafen tillämpas i praxis. Mot denna bakgrund är min intention att bedöma om den nuvarande lagregeln är en effektiv bestämmelse för att bekämpa brottet eller om det finns ett reformbehov, samt att undersöka om andra åtgärder kan vara nödvändiga för att på ett effektivt sätt motverka brottet. Vid avgörandet av om paragrafen är i behov av ändringar kommer särskilt den nyligen antagna Europarådskonventionen att beaktas.

1.3 Frågeställning

Den första frågan som blir relevant för att avgöra om den gällande lagstiftningen är en effektiv reglering av brottet dataintrång är vilka gärningar täcks in av den nuvarande bestämmelsen? Faller några gärningar utanför paragrafens tillämpningsområde och i så fall vilka? För att vidare kunna avgöra om det finns ett reformbehov är det väsentligt att undersöka hur förekomsten av dataintrång ser ut i praktiken. Är de handlingar som täcks in av lagstiftningen också de typer av dataintrång som förekommer i praktiken? Vad säger de statistiska uppgifterna om dataintrång och hur ser praxis på området ut? Vid avgörandet av om den nuvarande regleringen effektivt motverkar dataintrång blir det även nödvändigt att studera om det finns några alternativa åtgärder som kan bli aktuella för att hindra brottsligheten.

1.4 Avgränsning

Vid undersökningen av om den nuvarande svenska regleringen om dataintrång kan tänkas vara i behov av reformering kommer bl.a. att studeras hur BrB 4:9c överensstämmer med Europarådets konvention om cyberbrottslighet. Konventionen kommer att behandlas dels för att undersöka vilka eventuella ändringar som kan bli nödvändiga för att uppfylla Sveriges internationella förpliktelser, dels för att jämföra hur den svenska lagstiftningen förhåller sig till denna internationella standard som konventionen anses representera. Uppsatsen avgränsas till att enbart jämföra innehållet i den svenska lagstiftningen med konventionens bestämmelse och någon utvärdering av huruvida konventionen kommer att bli ett effektivt instrument görs inte.

1.5 Material

Materialet jag använt mig av i arbetet utgörs främst av förarbeten, doktrin och rättsfall. Till största del har jag använt mig av juridisk litteratur, men även datainriktad litteratur har varit till stor nytta. Det finns relativt mycket litteratur om IT-relaterad brottslighet men den är ofta av äldre natur och p.g.a. den snabba utvecklingen inom IT därför också förlegad. Olika institutioner, som t.ex. BRÅ och RRV, samt departement har dock utarbetat rapporter om ämnet och jag har haft stort användning av dessa. Dataintrång har även diskuterats relativt flitigt i svensk press på senare tid, och jag har också i viss utsträckning använt mig av tidningsartiklar.

1.6 Metod och disposition

Metoden i uppsatsen är både av beskrivande och analyserande karaktär. De deskriptiva delarna återfinns framför allt i uppsatsens inledande kapitel där bl.a. den gällande lagstiftning beskrivs. Metoden som använts är traditionell rättsdogmatisk metod. Uppsatsens inledningskapitel följs av en allmän presentation av brottet dataintrång för att ge läsaren en uppfattning om vilka brott som kan tänkas utgöra dataintrång, samt en definition av olika sorters dataintrång, vilka senare används för att kategorisera olika gärningar. Därefter följer en utförlig redogörelse för den gällande lagstiftningen i BrB 4:9c där regelns olika rekvisit behandlas och förklaras. Från kapitel fyra och framåt har uppsatsen en mer analyserande karaktär. I kapitel fyra presenteras statistiska uppgifter om dataintrång, vilka används för att försöka göra en uppskattning av förekomsten av dataintrång hos företag och privatpersoner. Syftet med redogörelsen för och analysen av praxis, som återfinns i kapitel fem, är att undersöka förekomsten olika kategorier av dataintrång samt att se hur lagregeln tillämpas av domstolarna. Kapitlet hjälper också till att belysa hur allvarligt domstolen ser på olika typer av gärningar, och analysen tar bl.a. sikte på om det finns några omständigheter kring dataintrånget som gör att brottet kan ses som mer allvarligt. Med utgångspunkt i den teoretiska redogörelsen för lagstiftningen samt analysen av praxis kommer den nuvarande regleringens problem och brister att presenteras i kapitel sex. I kapitel sju undersöks huruvida bestämmelsen uppfyller de krav som uppställs i den nyligen antagna Europarådskonventionen om cyber-brottslighet för att avgöra om några, och i så fall vilka, ändringar som kan bli aktuella för att uppfylla internationella åtagande. Därefter, i kapitel åtta, presenteras och analyseras några av de ändringsförslag som lämnats av olika utredningar och i kapitlet ges även förslag på övriga åtgärder som bör vidtas för att förhindra brottsligheten. Egen analys presenteras löpande i uppsatsen och i det avslutande kapitlet görs en sammanställning av dessa samt en presentation av slutsatser.

2 Dataintrång

2.1 Inledning

Dataintrång är ett samlingsbegrepp på ett stort antal gärningar, som alla har gemensamt att det sker ett obehörigt intrång i ett datasystem, men vilka kan skilja sig åt både vad gäller tillvägagångssätt och syfte. Den brottsliga gärningen kan t.ex. begås genom användning av en dator eller en terminal ansluten till en dator, eller genom avlyssning av en ledning för datakommunikation, och målet kan bl.a. vara att ta sig in i ett register eller att stjäla information.[2]

Dataintrång kan delas in i två olika kategorier beroende på hur förhållandet mellan personen som gör sig skyldig till dataintrånget och brottsobjektet gestaltar sig. Utgångspunkten är huruvida hotet kan anses komma utifrån eller inifrån den kategori av personer som har tillgång till data, och dessa kategorier brukar följaktligen kallas interna respektive externa dataintrång. Trots att interna och externa dataintrång har många likheter kan det ändå vara betydelsefullt att särskilja dessa båda brottskategorier åt, bl.a. för att det krävs olika åtgärder för att förhindra dem.

Det är även vanligt att det görs en indelning av dataintrång beroende på vilket bakomliggande motiv och tillvägagångssätt gärningsmannen har. Dessa intrångssätt benämns hacking respektive cracking. Även avseende dessa gärningar görs normalt en åtskiljning eftersom gärningar som utgör cracking ibland lagförs enligt en annan paragraf än BrB 4:9c.

I viss litteratur används en gemensam beteckning på samtliga dataintrång medan andra författare gör en strikt uppdelning mellan en mängd olika kategorier. Det senare är framför allt fallet vad avser datainriktad litteratur. I svensk juridisk litteratur förekommer vanligtvis diskussion kring fyra begrepp för att klassificera olika typer av dataintrång; internt dataintrång, externt dataintrång, hacking och cracking. Internt respektive externt dataintrång samt hacking respektive cracking är två olika kategoriseringar som kan tillämpas oberoende av varandra. En gärning kan således bedömas som antingen internt eller externt dataintrång och samtidigt klassificeras som hacking respektive cracking och vice versa. I det följande ska dessa fyra begrepp presenteras eftersom de återkommer i uppsatsen för att kategorisera olika typer av dataintrång.

[2] Almblad & Brorsson, s. 8; Ds 1990:45, s. 25. Se vidare i kapitel 3.4.

2.2 Internt dataintrång

Med internt dataintrång avses de fall av dataintrång som sker på en arbetsplats eller inom ett företag av någon som tillhör de anställda på detta arbetsställe.[3] Signifikant för denna typ av dataintrång är således att den som begår brottet har en viss relation, p.g.a. av anställningskontrakt eller någon annan form av auktorisering, till platsen där brottet begås.[4] Internt dataintrång kan t.ex. ske genom att en arbetstagare överskrider sin befogenhet genom att ta sig in i register eller datasystem som de ej har rätt till. Vanligtvis begås de interna dataintrången just genom att anställda tar fram sekretessbelagda registerupplysningar utan tillstånd, vilket särskiljer dem från de externa.[5] Det rör sig således om personer som inom sin behörighet tar fram uppgifter vilka inte är relevanta för deras tjänste-utövning, och denna typ av brott har framför allt uppmärksammats inom rättsväsendet, postgirot, landstinget och vid försäkringskassorna.[6] Ett annat exempel på internt dataintrång är när anställda går in i sina kollegors datorer eller filer, antingen för att tillgodogöra sig information eller förstöra den. Eftersom det ofta krävs särskilda kunskaper om system och program för att ta sig in i och hantera ett datasystem, vilket inte är nödvändigt vid denna typ av dataintrång, utgörs en stor andel av det totala antalet dataintrång som begås av interna dataintrång.[7]

2.3 Externt dataintrång

Externa dataintrång karaktäriseras av att någon utomstående, d.v.s. någon som inte är anställd eller har auktorisation, bryter sig in i ett datasystem. Att någon är utomstående behöver inte betyda att det inte finns något relation mellan förövaren och brottsplatsen utan gärningsmannen kan t.ex. vara en f.d. anställd, en kund eller en konkurrent.[8] Externa dataintrång har historiskt sett utgjort en liten del av det totala antalet dataintrång, men på senare år har de ökat drastiskt i antal och är idag nästan lika vanliga som interna. I många u-länder anses externa dataintrång utgöra ett stort hot mot utvecklingen av Internet, och problemet är så omfattande att externa dataintrång i vissa länder till och med klassificeras som en nationell säkerhetsrisk.[9] Hur stort problemet med externa dataintrång egentligen är kan dock vara svårt att avgöra eftersom det antas finnas ett stort mörkertal av brott som aldrig anmäls.[10] Undersökningar i Sverige visar att i drygt 80 procent av de fall då ett företag utsätts för dataintrång är gärningsmannen en utomstående.[11] Det

[3] BRÅ, s. 28.
[4] Boni & Kovacich, s. 88
[5] BRÅ, s. 29.
[6] Ds 1990:45, s. 25.
[7] Casey, s. 171.
[8] Boni & Kovacich, s. 74-75.
[9] Casey, s. 171.
[10] Se vidare angående statistik om förekomsten av dataintrång i kapitel 4.
[11] BRÅ, s. 29.

är dock inte ovanligt att gärningsmannen vid externa dataintrång har tillgång till intern säkerhetsinformation, t.ex. lösenord och användaridentiteter, eller har fått insidertips om säkerhetsbuggar på det aktuella datasystemet, vilket avsevärt underlättar intrånget.[12]

2.4 Hacking

En vanlig form av dataintrång är hacking. Vid hacking är syftet med dataintrånget inte att förstöra eller stjäla information, utan vanligtvis är gärningsmannen bara intresserad av att utforska och undersöka datasystemet.[13] Den brottsliga gärningen kan delas in i två olika kategorier beroende på om förövaren enbart tar sig in i ett data- eller kommunikationssystem, ren hacking, eller om han också tillgodogör sig informationen, oren hacking.[14] Oren hacking anses generellt sett som en allvarligare gärning än ren hacking, eftersom det innebär att förövaren på något sätt tar del av informationen, t.ex. genom att läsa eller kopiera den.

2.5 Cracking

Gemensamt för hacking och cracking är att gärningsmannen, hackern respektive crackern, olovligen gör intrång i ett datasystem, men medan hackern nöjer sig med att läsa informationen har crackern ett mer långtgående syfte. Målet vid cracking är att kopiera, ändra eller på något annat sätt förstöra eller skada data som finns lagrade i systemet, och det är i denna kategorin som de största externa hoten för företag finns.[15] Exempel på angreppsobjekt vid cracking är stöld av företagshemlig information och sabotage av strategiska datasystem. En cracker kan även figurera som gärningsman vid interna dataintrång. Inte sällan är crackern en missnöjd anställd som vill ta ut hämnd på sin arbetsgivare genom att störa funktionen hos IT-systemet och på så sätt åstadkomma skada för företaget.[16] Cracking är ofta ett förled till annan brottslighet och i många fall blir den slutliga brottsrubriceringen en annan än dataintrång t.ex. spioneri (BrB 19:5) eller sabotage (BrB 12:1).[17] I de fall cracking ändå bedöms som dataintrång och inte som något annat brott beror det oftast på att gärningsmannen, av en eller annan anledning, hindrats från att fullfölja sitt brott eller att uppsåt till annat brott inte kan bevisas.[18]

[12] Barrett, s. 40-41.
[13] BRÅ, s. 15.
[14] SOU 1992:110, s. 187.
[15] BRÅ, s. 15.
[16] SOU 1992: 110, s. 142.
[17] SOU 1992:110, s. 194-195, 204.
[18] SOU 1992:110, s. 142.

3 Lagstiftning BrB 4:9c

3.1 Inledning

Bestämmelsen om dataintrång återfinns i BrB 4:9c och den infördes där i samband med att den tidigare datalagen (1973:289) ersattes med personuppgiftslagen, PuL, (1998:204).[19] Som nämnts i inledningen är paragrafen nära trettio år gammal och syftet med bestämmelsen var att införa ett skydd för information i form av datalagrade uppgifter. De teknikneutrala bestämmelser som redan fanns till skydd för information ansågs inte vara tillräckliga för att komma åt de nya intrång som den nya tekniken för automatisk databehandling, ADB, gav upphov till, utan en ny bestämmelse om dataintrång infördes. Bestämmelsen har sedan dess enbart genomgått mindre förändringar och den har följande ordalydelse:

BrB 4:9 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).

3.2 Data

Det centrala begreppet i lagstiftningen om dataintrång är ordet ”data” och i normalt språkbruk har detta begrepp en inte entydig innebörd. Begreppet kan sägas ha en viss betydelse i allmänt tal och en annan i informations-teknisk mening, och för att kunna avgöra vilka förfarande som är kriminaliserade som dataintrång är det nödvändigt att definiera vad som innefattas i begreppet i den senare fallet. I dagens reglering av dataintrång finns ingen uttrycklig definition av begreppet data intagen i lagregeln, utan istället får svaret sökas i förarbetena. I det betänkande som avlämnades av Offentlighets- och sekretesslagstiftningskommittén, OSK, 1972 beskrivs data som uppgifter vilka matats in och bevarats i datamaskinens minne eller i medier för ADB, och som inte är visuellt läsbara utan enbart har maskinläsbar form.[20] I förarbetena till brottsbalken från 1992 ges en mer utförlig beskrivning av begreppet data av Datastraffrättsutredningen, DSU. Där anges att data är ”representationen av fakta, begrepp eller instruktioner i en form lämpad för överföring, tolkning eller bearbetning utförd av människor eller av automatiska hjälpmedel”[21]. Vid bestämmandet av den informationstekniska innebörden har således fokus lagts på själva representationen av information. Den huvudsakliga uppgiften för data är att

[19] Bestämmelsen om dataintrång återfanns i 21§ datalagen.
[20] SOU 1972:47, s. 37.
[21] SOU 1992:110, s. 83.

förmedla information vilket sker genom att data tolkas och data kan sägas ha en kvasimateriell karaktär eftersom det visserligen existerar men ändå inte är fysiska föremål.[22] Någon vidareutveckling av vad som ska anses innefattas i begreppet går inte att finna i förarbetena utan i ett senare betänkande förekommer en mer kortfattade definition av data som ”uppgifter som har elektronisk form”[23] vilket inte ger någon närmare vägledning.

3.3 Skyddsobjekt

3.3.1 Upptagningsbegreppet

Skyddsobjektet i regleringen om dataintrång är ”upptagning” för automatisk databehandling, och vad som ska anses innefattas i detta begreppet har varit föremål för livlig debatt. En grundläggande utgångspunkt har varit att försöka täcka in den datarelaterade brottsligheten med redan befintlig lagstiftning, och vid utarbetandet av bestämmelsen om dataintrång har paralleller dragits till redan gällande lagregler. Vid utformningen av upptagningsbegreppet har utgångspunkten varit regleringen om handlingar.[24] Liksom bestämmelserna om handlingar tar upptagningsbegreppet sikte på ett konkret föremål vari uppgifterna fixerats i ett föremål, minne, och inte enbart på själva informationen som sådan.[25] Exempel på sådana föremål där uppgifter kan fixeras är magnetband, skivminne och kärnminne, medan hålkort och hålremsor torde kunna betraktas som både handlingar och upptagningar. Något närmare klargörande av vad som innefattas i kravet på fixering går inte att finna i lagmotiven, men troligtvis får inte data vara lagrade alltför kort tid om fixering ska anses föreligga.[26]

Departementschefen, liksom vissa remissinstanser, var dock av annan mening då de ansåg att fokuseringen på att information ska fixeras vid ett visst objekt innebär att upptagningsbegreppet får ett alltför vidsträckt innehåll, och istället ska med upptagning avses själva informationsinnehållet.[27] Den lagtekniska lösning som valdes av OSK har dock tagit sikte på det förra alternativet, och det innebär att reglernas upptagningsbegrepp liknar det för en traditionell handling, d.v.s. den fokuserar på ett konkret föremål och inte på själva informationen som sådan. Utgångspunkten för särskiljning mellan handling och upptagning har varit huruvida uppgifterna kan läsas med ADB-teknik eller inte, och riktlinjen har varit att uppgifter som är visuellt läsbara inte ska omfattas av definitionen. Dock har någon exakt gränsdragning mellan upptagningar och handlingar inte ansetts vara nödvändig.[28]

[22] Seipel, s. 22.
[23] SOU 1997:39, s. 501.
[24] SOU 1972:47, s. 50.
[25] Prop. 1973:33, s. 23.
[26] SOU 1992:110, s. 109.
[27] Prop. 1973:33, s. 33, 74-75.
[28] Prop. 1973:33, s. 23.

Genom ett tillägg till bestämmelsen 1986 klargjordes att med upptagning ska även avses uppgifter som är under befordran via elektroniskt eller annat jämförligt hjälpmedel för att användas för automatisk databehandling, även om uppgifterna inte är att anse som upptagningar för ADB. Lagändringen vidtogs för att subsidiärt kunna bestraffa de typer av brott som innebär olovlig avlyssning av information under transport, s.k. wire-tapping, som inte föll in under brottsbeskrivningen av brytande av telehemlighet enligt BrB 4:8.[29] Information som förs över från en terminal till en dator för bearbetning via en privat förbindelse är inte fixerad på något datamedium och det är därför tveksamt om den omfattades av den dåvarande ordalydelsen. Vid transport i motsatt riktning, d.v.s. från en dator till en terminal, är dock informationen redan lagrad i ett datamedium och detta förfarande täcks således av lagen. Problemet var alltså att uppgifterna var skyddade vid transport i ena riktningen men inte i den andra. Enligt vissa uttalande i förarbetena skulle upptagningsbegreppet även omfatta uppgifter som matats in på en terminal och sedan sänts till en dator.[30] Huruvida detta är en tolkning som är förenlig med kravet på att uppgifterna ska vara fixerade på ett datamedium är dock tveksamt, och för att undanröja oklarheter utvidgades brottsbeskrivningen av dataintrång till att även omfatta uppgifter under befordran.

3.3.2 Automatisk databehandling

Enligt ordalydelsen i paragrafen ska intrånget avse upptagning för ”automatisk databehandling” och avgörande för att regleringen ska bli tillämplig är således att uppgifterna antingen ingår i eller kan matas in i ett ADB-system.[31] Vad som avses med automatisk databehandling framgår dock inte av lagmotiven. Databehandling i vidsträckt bemärkelse har traditionellt sett ansetts vara all hantering av data i form av siffror, bokstäver och andra tecken, utan några egentliga krav på regler för hur hanteringen ska utföras.[32] I dagligt språkbruk definieras databehandling numera som utförandet av en systematisk serie operationer på givna data.[33] Det har dock varit svårt att hitta en lämplig och hållbar definition av begreppet i juridisk mening, bland annat p.g.a. den snabba utvecklingen av datatekniken. En uppfattning har varit att en sådan definition inte är nödvändig eftersom det ”i de flesta fall gav sig självt” vad som avses med begreppet, eller att en sådan definition i alla fall inte är nödvändig för att på ett effektivt och rättssäkert sätt kunna tillämpa lagstiftningen.[34] Trots detta uttalande har flertalet försök gjorts, både i doktrin och i förarbete, att ange vad som ska anses falla in under begreppet.

[29] Prop. 1985/86:65, s. 31-32.
[30] Se bl.a. SOU 1983:50, s. 185.
[31] Prop. 1973:33, s. 23.
[32] SOU 1992:110, s. 83.
[33] SOU 1992:110, s. 83.
[34] SOU 1990:61, s. 91.

Ett försök att bringa klarhet i begreppet gjordes av SIS som 1977 utarbetade en definition av automatisk databehandling. Enligt deras definition menas med automatisk databehandling ”databehandling som huvudsakligen utförs med dator” och i samma handbok beskrivs dator som ”databehandlings-apparat som utan mänskligt ingripande under körning kan utföra omfattande beräkningar med ett stort antal aritmetiska eller logiska operationer”.[35] Viktigt att ha i åtanke är att SIS avsikt inte var att utarbeta en definition av begreppet som var avsedd att användas i juridisk mening, och vilken betydelse denna definition har haft för den rättsliga regleringen av dataintrång är inte helt klart. Någon uttrycklig hänvisning till definitionen utarbetad av SIS har inte gjorts i de förarbeten som legat till grund för ändringar av bestämmelsen om dataintrång. Istället verkar utgångspunkten vara det uttalande som gavs i prop. 1973:33 eftersom en hänvisning dit har gjorts i de flesta förarbetena rörande dataintrång. Där ges dock som sagt bara knapphändig information om vad som ska anses som automatisk databehandling. Det enda som uttryckligen sägs är att uppgifterna ska ingå i eller kunna matas in i ett sådant system och beskrivningen av automatisk databehandling får således anses som vag och oklar. Det är dessutom tveksamt om ett underlag som inte ska utnyttjas för automatisk databehandling omfattas. Något direkt svar på frågan går inte att hitta i förarbetena, men för att undvika att vissa former av databehandling faller utanför definitionen får det antas att en automatisk behandling sker då sådana upptagningar förs in i en dator oavsett om detta är fallet i realiteten.[36]

3.4 Intrångssätten

3.4.1 Bereder sig tillgång

Enligt ordalydelsen i BrB 4:9c straffbeläggs den som ”olovligen bereder sig tillgång” till upptagning för automatisk databehandling, men någon närmare beskrivning av sätten för att bereda sig tillgång ges dock inte i lagtexten. Vid tillkomsten av lagregleringen om dataintrång i början av 1970-talet ansågs det mest troliga brottsscenariot vara att någon bröt sig in i ett rum där en dator eller ansluten terminal förvarades, och med hjälp av denna utrustning beredde sig tillgång till informationen. [37] Det var också med utgångspunkt i den föreställningen som lagregeln skrevs.

I takt med den tekniska utvecklingen har omfattande utbyggnader av nätverk vidtagits, och det har öppnat nya möjligheter att bereda sig tillgång till ADB-upptagningar. Detta innebär att det numera är möjligt att bereda sig tillgång till sådana upptagningar utan att det nödvändigtvis måste innefatta att fysiskt ta sig in i ett rum. Dataintrång kan t.ex. begås genom att avlyssna

[35] Silvander, s. 54.
[36] Silvander, s. 59.
[37] SOU 1992:110, s. 187.

en ledning för datakommunikation med hjälp av teknisk utrustning som kopplas in direkt på ledningen, genom att avlyssna en dataskärms elektromagnetiska strålning, eller genom att med hjälp av optisk utrustning ta del av information på en dataskärm.[38]

Förmögenhetsbrottsutredningen försökte i samband med översynen av lagstiftningen 1983 att precisera innebörden av begreppet ”bereda sig tillgång” och utredningen delade in gärningstyperna i fyra olika kategorier beroende på angreppsobjektet och sättet att utföra dem.[39] Den första gruppen av gärningar karaktäriseras av att de resulterar i att outputen av en databehandlingsprocess blir felaktig, till följd av att program ändras eller att oriktiga uppgifter inmatas. Denna typ av gärningar kan i sig innebära en förmögenhetsskada, vilket medför att de istället för dataintrång kan bedömas som bedrägeri, trolöshet mot huvudman eller förfalskningsbrott.[40] Den andra gruppen av gärningar har gemensamt att ett skadegörande angrepp på datorns mjukvara företas. Det är inte ovanligt att dessa gärningar bedöms enligt BrB 12:1 som skadegörelse. I den tredje gruppen återfinns de gärningar som innebär att någon obehörigen bereder sig tillgång till program eller data, medan den fjärde gruppen innefattar gärningar som innebär angrepp mot datorn i egenskap av sak, t.ex. stöld och skadegörelse.

Av ordalydelsen i paragrafen följer att gärningsmannen inte behöver ha tillgodogjort sig innehållet i upptagningen för att en brottslig gärning ska anses ha begåtts, utan det är tillräckligt att förövaren berett sig tillgång till uppgifterna.[41] Även då någon bereder sig indirekt tillgång till uppgifter, t.ex. då uppgifterna används för att göra en utskrift anses ett dataintrång föreligga.[42] Det krävs dock att gärningen är uppsåtlig.[43] I de fall då någon oavsiktligt får tillgång till ADB-upptagningar föreligger inte någon brottslig gärning.

3.4.2 Ändrar, utplånar eller i register för in

Förutom förfarande där någon bereder sig tillgång till ADB-uppgifter kriminaliseras gärningar som innebär att sådana uppgifter ändras eller utplånas. Detta innebär att någon som har behörighet att ta del av datalagrade uppgifter kan dömas för dataintrång om han/hon raderar eller på något annat sätt ändrar i uppgifterna. Även denna reglering var tänkt att subsidiärt täcka in de gärningar som inte omfattas av de redan befintliga brottsbeskrivningarna i kapitel fyra i brottsbalken.[44] Trots att det inte direkt framgår av ordalydelsen omfattas såväl kvantitativa som kvalitativa

[38] Almblad & Brorsson, s. 8.
[39] SOU 1983:50, s. 174-175.
[40] Prop. 1985/86: 65, s. 12.
[41] SOU 1992:110, s. 180.
[42] Almblad & Brorsson, s. 26.
[43] BrB 1:2.
[44] Prop. 1973:33, s. 52, 104-105.

ändringar av lagrade data av lagtexten.[45] Som exempel på en kvantitativ ändring av data kan anges förfarandet då någon utplånar vissa delar av lagrade data medan en kvalitativ ändring sker genom att en upptagning eller själva dataprogrammet som styr databehandlingen ändras. Ändringen kan därutöver antigen vara temporär eller konstant, och båda fallen täcks in av lagstiftningen.[46]

Därutöver kriminaliseras gärningar som innebär att någon för in en upptagning för automatisk databehandling i ett register. Detta förfarande lades till i bestämmelsen om dataintrång i samband med att PuL infördes, och det register som åsyftas torde vara ett personuppgiftsregister i enlighet med 5 § PuL.[47]

3.4.3 Olovlighetsrekvisitet

För att en gärning ska kunna klassificeras som dataintrång krävs vidare att den företas utan medgivande. Enligt lagtextens ordalydelse straffbeläggs endast olovliga åtgärder, och detta innebär att om någon med tillåtelse bereder sig tillgång till uppgifter kan denne inte bestraffas i enlighet med paragrafen. Ett samtycke till gärningen, som givits av någon som är behörig att förfoga över intresset, har således straffbefriande verkan.[48] Problem att avgöra huruvida en åtgärd företagits olovligen kan förekomma vid tillhandahållande av elektroniska förmedlingstjänster[49]. Dessa karaktäriseras av att alla användare av tjänsten har tillgång till de elektroniska meddelandena, vilket innebär att den som tillhandahåller tjänsten, p.g.a. denna allmänna åtkomst, har rätt att ta del av de elektroniska meddelandena.[50] Troligtvis torde inte detta förfarande innebära ett ”olovligt” intrång. Motsatsen gäller dock för e-post. Där kan en jämförelse göras med traditionell post, och detta medför att om den som tillhandahåller en elektronisk förmedlingstjänst tar del av innehållet i ett e-post meddelande har han/hon förfarit olovligen.[51]

3.5 Skyddsintresse

BrB 4:9c reglerar tillsammans med BrB 4:8-9b de gärningar som rör informationsintrång. Gemensamt för dessa paragrafer är att de har samma

[45] Silvander, s. 218.
[46] Holmqvist m.fl., s. 246.
[47] Holmqvist m.fl., s. 246.
[48] Prop. 1993/1994:130, s. 39. En djupare diskussion om samtyckes straffbefriande verkan kommer här inte att föras utan den intresserade kan läsa närmare om detta i propositionen s. 38-44.
[49] Med elektroniska förmedlingstjänster avses främst tjänster för förmedling av elektroniska meddelande, t.ex. elektroniska anslagstavlor. För en närmare förklaring se SOU 1996:40, s. 141-147.
[50] SOU 1996:40, s. 207.
[51] SOU 1996:40, s. 207. Se även vidare i kapitel 6.3.

skyddsintresse, d.v.s. att se till att information endast ska vara tillgänglig för förfogande av annan än den som innehar informationen om samtycke föreligger, eller om informationen erhållits på ett icke lagstridigt sätt.[52] Bestämmelsen om dataintrång verkar enligt min mening även ta sikte på att skydda mot ingrepp i den personliga integriteten. Syftet vid bestämmelsens tillkomst var följaktligen att hindra de som var ansvariga för dataregister från att använda den nya tekniken till skada för andra.[53] Bestämmelsen om dataintrång har begränsats till att avse uppgifter som finns lagrade eller överförs med datamedier, men skyddet avser all typ av information oavsett dess innehåll. Även om det ursprungliga syftet var att skydda uppgifter i personregister omfattar regleringen alla typer av datauppgifter, även sådana som inte innehåller någon personinformation. Det spelar således ingen roll om dataintrånget medför ett otillbörligt integritetsintrång eller ej.[54]

3.6 Regelkonkurrens

Såsom uttryckligen stadgas i lagtexten är bestämmelsen om dataintrång tänkt att användas subsidiärt i förhållande till de övriga reglerna om informationsintrång som finns angivna i BrB 4:8 samt BrB 4:9-9b. Regeln kan liknas vid en paraplybestämmelse som har till uppgift att täcka in de brottsliga förfarande som inte faller in under någon av de andra bestämmelserna som skyddar information, såsom brytande av post- och telehemligheter (BrB 4:8), intrång i förvar (BrB 4:9) eller olovlig avlyssning (BrB 4:9a). I takt med digitalteknikens utbredning har antalet konkurrenssituationer ökat, vilket medför att det ibland kan vara svårt att avgöra huruvida en gärning ska bedömas som ett brott enligt bestämmelsen om dataintrång eller enligt någon annan reglering. I förarbetena och praxis har tidigare uttalats att i de fall konkurrenssituationer uppstår p.g.a. att flera brottsbeskrivningar kan anses vara tillämpliga ska bestämmelsen om dataintrång anses vara subsidiär även i förhållande till andra brottsbalksbestämmelser än de som numera uttryckligen anges i lagtexten, som t.ex. skadegörelse, tjänstefel eller trolöshet mot huvudman.[55] I och med att bestämmelsen flyttats över från datalagen till brottsbalken har dock angivits att lagkonkurrens mellan dataintrång och övriga brottsbalksbrott får avgöras enligt traditionella principer för bedömning av lagkonkurrens.[56] Straffskalan för dataintrång sträcker sig från böter till fängelse i högst två år.

[52] SOU 1992: 110, s. 181.
[53] SOU 1972:47, s. 95.
[54] Freese, s. 163.
[55] Prop. 1973:33, s. 145; prop. 1985/86:64, s. 12-13; RH 1996:133, s. 341.
[56] Prop. 1997/98:44, s. 149.

3.7 Försök och förberedelse

I BrB 4:10 stadgas att försök och förberedelse till dataintrång är straffbart förutsatt att brottet, om det fullbordas, inte skulle ha varit att anse som ringa. Denna bestämmelse lades till i brottsbalken samtidigt som regeln om dataintrång flyttades dit från datalagen. Tidigare återfanns bestämmelsen i datalagens 21 § andra stycket och den kom till efter påpekande i ett remissvar från den juridiska fakulteten i Stockholm angående de stora värden i form av information som finns att skydda på IT-området.[57] I propositionen till lagändringen ges ingen utförligare förklaring till hur bestämmelsen om försök och förberedelse ska tolkas, utan där anges enbart att dessa gärningar kan vara straffbara och i övrigt hänvisas till utredningarna gjorda av Datalagskommittén (SOU 1997:39) och DSU (SOU 1992:110).[58]

I DSU:s betänkande diskuteras relativt ingående hur förberedelse och försök till dataintrång ska bestraffas.[59] Angående straffbart försök görs en hänvisning till BrB 23:1 och vid avgörandet av om fara för brottets fullbordan förelegat, eller om den uteslutits enbart p.g.a. tillfälliga omständigheter ska särskild hänsyn tas till IT-miljön. Förberedelse till brott är kriminaliserat enligt BrB 23:2 och sedan den 1 juli 2001 har bestämmelsen en ny ordalydelse. Tidigare angavs i paragrafen som straffbart beteende att motta pengar, vederlag eller förlag samt att anskaffa, förvara, lämna o.d. gift, sprängämne, vapen, dyrk, förfalskningsverktyg eller annat sådant hjälpmedel. Uppräkningen av hjälpmedel inkluderade dock inte de särskilda IT-objekt som kan bli aktuella vid förberedelse till dataintrång, och denna brist har påpekats ett flertal gånger både i förarbete och doktrin. Genom ändringen har hänsyn tagits till den utveckling som skett inom teknikens område, och i den reformerade paragrafen återfinns numera en mer generell bestämmelse. Den normerande uppräkning av hjälpmedel som paragrafen tidigare innehöll har ersatts med ordalydelsen ”något som är särskilt ägnat åt att användas som hjälpmedel vid ett brott” och i förarbetena anges som exempel på sådana hjälpmedel datorprogram och annan mjukvara.[60] Även samlingar av information såsom en sammanställning av koder kan utgöra hjälpmedel i enlighet med paragrafen, men då krävs att informationen nedtecknats eller lagrats på något annat sätt, eftersom ren kunskap inte kan anses utgöra ett hjälpmedel i paragrafens bemärkelse.[61]

[57] SOU 1992:110, s. 199, se även prop. 1973:33, s. 68.
[58] Prop. 1997/98:44, s. 112-113.
[59] SOU 1992:110, s. 198-201.
[60] Prop. 2000/2001:85, s. 50.
[61] Prop. 2000/2001:85, s. 50-51.

3.8 Kommentar

Något som verkar vara karaktäristiskt för lagregleringen om dataintrång är att det är svårt att bilda sig en uppfattning om vad som egentligen avses med de olika begrepp som paragrafen innehåller. Lagregeln innehåller ingen klar och tydlig definition av vad som ska avses med de uppräknade rekvisiten och även om viss ledning kan sökas i förarbetena är känns definitionerna vaga och oklara.

Detta gäller t.ex. definitionen av data. OSK anger att data är uppgifter som matas in i ett ADB-medium och som enbart kan läsas maskinellt medan DSU anser att begreppet data är vidare och även omfattar uppgifter som bearbetas av människor. Det föreligger således en klar divergens mellan de två definitionerna eftersom ett av OSK:s rekvisit är att uppgifterna ska bearbetas maskinellt. I det följande kommer dock visas att denna tvetydighet inte har någon större betydelse för tillämpningen av BrB 4:9c eftersom paragrafen uttryckligen begränsats till att reglera intrång i uppgifter för automatisk databehandling, vilket torde utesluta data enligt DSU:s definition.

Inte heller upptagnings-begreppet är klart och tydligt definierat i paragrafen utan även här får ledning sökas i förarbetena. Utgångspunkten vid formuleringen av upptagningsbegreppet har varit att utarbeta ett begrepp som så långt möjligt liknar det traditionella handlingsbegreppet och följden har blivit att fokuseringen har lagts på ett konkret föremål. Något som kan antas ge upphov till problem är att ingen klar gränsdragning har gjorts mellan handlingar och upptagningar. Eftersom paragrafens tillämpnings-område inskränkts till upptagningar för automatisk databehandling har dock problemet delvis löst. Dessutom är BrB 4:9c subsidiär i förhållande till andra bestämmelser och därmed ska den tillämpas enbart i de fall ingen annan paragraf blir tillämplig.

Något som däremot kan ge upphov till problem är att ADB inte är klart och tydligt definierat i varken lagstiftningen eller förarbetena. Att kunna utröna vad som innefattas i begreppet måste anses som väsentligt eftersom det utgör en central del i lagstiftningen. Enbart upptagningar för automatisk databehandling omfattas av paragrafens ordalydelse och därför är det avgörande att det går att bestämma vad som avses med ADB. Kanske är det så att ”det i de flesta fall ger sig självt” och att det i dagsläget inte finns något uttalat behov av en sådan definition. Dock anser jag att det inte omöjligt att avsaknaden av en klar och tydlig definition kan ge upphov till problem i en framtid där analoga och digitala medier kan komma att sammanverka.

Paragrafen om dataintrång träffar gärningar som innebär att någon bereder sig tillgång till information, eller ändrar, utplånar eller i register för in och genom valet av ordalydelse kriminaliseras en mängd gärningar. Vid en

första anblick kan bestämmelsen tyckas träffa ett stort antal gärningar men genom olovlighetsrekvisitet begränsas tillämpningsområdet. Enligt min uppfattning har lagstiftarna valt att straffbelägga gärningarna i ett så tidigt stadium som möjligt. Det finns således inget krav på att gärningsmannen ska ha tagit del av uppgifterna, och anledningen är troligen att det skulle uppstå stora bevissvårigheter om ett sådant rekvisit skulle föras in i bestämmelsen. Det verkar som om lagstiftarna har föredragit att ett stort antal gärningar träffas av paragrafen och att antalet brottsliga gärningar avgränsas genom ett resonemang kring olovlighets- och uppsåtsrekvisitet istället för varit att ha en lagregeln där de straffbelagda intrångssätten mer precist räknas upp.

4 Statistik

4.1 Inledning

På senare år har det gjorts ett flertal försök att kartlägga den IT-relaterade brottsligheten i Sverige för att om möjligt kunna konstatera ifall incidenterna är så omfattande och allvarliga som de ofta framställs. En av de senaste utredningarna genomfördes av BRÅ under 1999 och den visar att de IT-relaterade brotten och incidenterna har ökat med 55 procent hos företag och offentliga institutioner sedan mitten av 1990-talet.[62] Som jämförelse användes statistik framtagen av RRV vilken byggde på en omfattande undersökning av datarelaterade brott under åren 1995-1996. Även tidigare har försök gjorts att kartlägga förekomsten av databrott. Rikspolisstyrelsen publicerade 1984, 1991 och 1994 enkätundersökningar baserade på uppgifter från landets polismyndigheter, men sedan dess har det inte funnits medel till fler liknande undersökningar. BRÅ och RRV har också använt sig av enkäter i sina undersökningar då det varit svårt att på något annat sätt skapa sig en bild av förekomsten av databrottslighet, eftersom databrott inte redovisas separat i brottsstatistiken p.g.a. att de inte utgör någon homogen brottskategori.[63]

4.1.1 Företag

De undersökningar avseende förekomsten av IT-relaterad brottslighet hos företag som gjorts av RRV och BRÅ bygger på förfrågningar gjorda hos företag, statliga myndigheter och bolag, kommunala förvaltnings-myndigheter och bolag, samt landsting med minst 50 anställda, i forstättnigen kallade företag. I båda fallen skickades brevenkäter ut till ca 1600[64] av landets 4500 företag som uppfyllde normen, och svarsfrekvensen var relativt hög. Erfarenheter från andra länder visar att ca 20-50 procent av de tillfrågade brukar inkomma med svar men vid undersökningen utförd av RRV var svarsfrekvensen 77 procent medan den var något lägre vid enkäten av BRÅ.[65]

Undersökningarna visade att dataintrång utgör 14 procent av den totala IT-relaterade brottsligheten i Sverige, och det är det näst vanligaste databrottet efter datavirus.[66] Av antalet tillfrågade företag uppgav 173 (BRÅ) respektive 117 (RRV) företag att de drabbats av dataintrång, vilket är att jämföra med

[62] BRÅ, s. 7.
[63] RRV, s. 20; BRÅ, s. 11.
[64] 1693 företag i RRV:s undersökning respektive 1564 företag i BRÅ:s.
[65] Svarsfrekvensen vid BRÅ:s undersökning var 67 procent. I BRÅ:s rapport anges att svarsfrekvensen vid liknande studier har legat på mellan 20-40 procent medan RRV anger siffrorna 20-50 procent, se BRÅ, s. 11 resp. RRV, s. 22.
[66] BRÅ, s. 22; RRV, s. 28.

778 respektive 530 som drabbats av virus. Antalet dataintrång har ökat konstant de senaste åren, något som särskilt visade sig i RRV:s undersökning. Där angavs att 87 procent av de rapporterade dataintrången under 1995-1996 inträffade under det andra året och det ansågs ha sin förklaring i den stora anslutning till Internet som skedde under denna period.[67] En ökning av användandet av Internet är troligtvis också förklaringen till att antalet dataintrång har ökat med 48 procent under de senaste fem åren.[68]

Vid undersökningen har de tillfrågade delats upp i olika branschgrupper för att få ett så heltäckande statistiskt resultat som möjligt. De har bl.a. delats upp i en offentlig och en privat sektor där såväl statliga och kommunala bolag, som privata företag finns representerade. Av undersökningen framgår att den privata sektorn är hårdast drabbad, och mest utsatta är företag inom industrin. Nära 70 procent av alla dataintrång begås inom den privata sektorn och detta är en ökning av antalet dataintrång inom den sektorn med 78 procent jämfört med 1996.[69] Inom den offentliga sektorn är kommunal förvaltning värst utsatt med 13 procent av det totala antalet dataintrång eller 43 procent av samtliga dataintrång inom den offentliga sektorn.[70] Där är ökningen av brottsligheten betydligt mindre än vad gäller den privata sektorn.

Ett av de vanligaste angreppsobjekten vid dataintrång är företags och myndigheters e-post. Anställda använder sig ofta av e-post då de kommunicerar med sina kunder eller medarbetare, och det är inte ovanligt att hemlig affärsinformation förmedlas på detta sätt. Nära en tredjedel av alla dataintrång riktas mot myndigheters och företags e-post, något som företag som jobbar med IT-säkerhet anser vara oroande.[71]

Det har även gjorts försök att bestämma de ekonomiska skadorna av dataintrång. Eftersom kostnaderna för de rapporterade incidenterna endast uppgivits i 25 procent av fallen bygger uppgifterna på en uppskattning av kostnaderna baserade på de rapporterade fallen. De totala ekonomiska skadorna för dataintrång under åren 1997-1998 uppskattas till någonstans mellan 17 och 60 miljoner kronor, och medelkostnaden per brott till mellan 98 700 och 346 100 kronor.[72] Orsakerna till den stora spännvidden är att det i minimifallet antagits att de 75 procent som ej angivit någon kostnad inte heller drabbats av någon ekonomisk förlust, medan det i maxfallet antagits att de drabbats lika hårt som de som angivit en kostnad. Vilken av uppgifterna som skulle kunna tänkas ligga närmast sanningen har BRÅ inte

[67] RRV, s. 30.
[68] BRÅ, s. 7.
[69] BRÅ, s. 31.
[70] BRÅ, s. 31.
[71] Byttner, Computer Sweden, nr 18 2000.
[72] BRÅ, s. 24.

närmare spekulerat i, utan de har nöjt sig med att konstatera att maxfallet troligtvis är en överskattning av kostnaderna.[73]

4.1.2 Privatpersoner

Som nämnts i det föregående har ett stort antal utredningar av den IT-relaterade brottsligheten företagits. Flertalet av dessa har dock varit inriktade på att undersöka hur utbredd databrottsligheten är hos företag och myndigheter, och de har således inte omfattat privatpersoner. Under 1999 genomförde BRÅ en undersökning av den IT-relaterade brottsligheten hos privatpersoner, och den baserades på information insamlad genom telefonintervjuer med 1000 privatpersoner med Internetabonnemang.[74] Någon liknande undersökning företogs dock inte av RRV vid deras kartläggning av databrottsligheten, och därför är det inte helt lätt att försöka fastställa hur utvecklingen inom det här området ser ut. Redovisning av resultatet är dessutom inte lika utförligt som den avseende företags-undersökningen, vilket ytterligare bidrar till att det svårt att skapa sig en bild av situationen.

Av de 1000 tillfrågade uppgav 21 stycken d.v.s. två procent att de blivit utsatta för dataintrång.[75] Detta kan jämföras med företagsundersökningen där 11 procent av företagen uppgav att de utsatts för dataintrång. Även i privatpersonundersökningen var datavirus det vanligaste brottet, medan dataintrång hamnade längre ner på listan än i företagsundersökningen. Någon uppskattning av de ekonomiska skadorna för dataintrång liknande den hos företag har inte gjorts.

Enligt en nyligen genomförd undersökning i Norden utsätts åtta av tio Internetanvändare i hemmet för försök till dataintrång.[76] Detta är en markant ökning jämfört med de uppgifter som presenterats av BRÅ där enbart två procent uppgav att de blivit utsatta för dataintrång. En bidragande faktor till denna drastiska ökning är tillväxten av bredband, vilket har bidragit till att allt fler datorer har kopplats upp mot Internet. Visserligen redovisar den nordiska undersökningen antal försök till dataintrång och inte det faktiska antalet fullbordade dataintrång, men det torde vara troligt att anta att åtminstone en del av de försök som görs resulterar i ett fullbordat brott.

4.1.3 Polisanmäld brottslighet

Det har visat sig att den som utsätts för ett databrott är obenägen att göra en polisanmälan. Ett fåtal länder har infört en särskild anmälningsplikt för dylika brott för få en bättre kontroll över den IT-relaterade brottslighet, men

[73] BRÅ, s. 24.
[74] BRÅ, s. 11.
[75] BRÅ, s. 24.
[76] TT, Sydsvenskan 2001-11-09.

än så länge finns ingen sådan skyldighet enligt svensk lag.[77] Det finns ett flertal orsaker till att de som utsatts för dataintrång underlåter att polisanmäla brottet. En av förklaringarna till att de drabbade undviker att ge sig till känna är p.g.a. att de rädda för att få dåligt rykte. Detta gäller framför allt företag eftersom bristande IT-säkerhet anses vara något mycket känsligt.[78] Dessutom har det visat sig att många företag underlåter att göra en polisanmälan eftersom de har en bristande tilltro till polisens förmåga att klara upp brottet.[79] De tror helt enkelt inte att det lönar sig att rapportera till polisen utan att det enbart innebär merarbete. En annan orsak till att antalet databrott är underanmälda kan vara att den som utsätts för brottsligheten helt enkelt inte märker att ett brott har begåtts. Särskilt vid hacking då ingen skadegörelse eller stöld av data sker kan det vara svårt att upptäcka att ett dataintrång har skett. Dessutom visar undersökningar att upp till hälften av alla mindre företag inte har några rutiner för att upptäcka den typen av databrottslighet.[80]

Vid den senaste undersökningen av BRÅ gjordes även en kartläggning av samtliga polisanmälda databrott under åren 1997-1998. Det totala antalet databrott under den här perioden var 608 stycken och av dessa utgjorde 239 dataintrång.[81] Majoriteten av de polisanmälda dataintrången, 60 procent, klassificerades som externa eftersom de var gjorda av någon utomstående. Resterande fall utgjordes av interna dataintrång, och uppgifter lämnade i polisanmälningarna visade att de ekonomiska skadorna är betydligt större vid interna än externa dataintrång.[82]

Trots att det har ansetts vara känsligt för företag att blotta sina svaga sidor har det visat sig att företag har en större benägenhet att anmäla dataintrång än privatpersoner. Endast 15 procent av polisanmälningarna hade gjorts av privatpersoner medan 78 procent av anmälningarna var gjorda av företag. Det är dock vanligt att företag istället för att göra en polisanmälan väljer att försöka komma åt problemet med dataintrång genom interna utredningar, eftersom nyttan av dessa anses vara större än av en polisutredning.[83]

4.2 Analys

Trots att det finns nyligen gjorda undersökningar om förekomsten av dataintrång är det inte lätt att försöka bilda sig en uppfattning om hur vanligt brottet är. Den enda säkra slutsatsen jag vågar mig på att dra är att brottet troligtvis är vanligare än vad siffrorna i BRÅ:s och RRV:s undersökningar visar. Detta grundar jag på uppgifterna som givits i enkäterna om att de

[77] SOU 1992:110, s. 158.
[78] Lindstedt, Sydsvenskan 2000-11-05.
[79] Söderman, s. 8-9.
[80] RRV, s. 41.
[81] BRÅ, s. 25.
[82] BRÅ, s. 32.
[83] Söderman, s. 9.

drabbade ofta inte upptäcker att brottet begåtts eller att de ändå väljer att inte göra någon anmälan. Den nyligen publicerade nordiska undersökningen ger också stöd för mitt antagande. Enligt undersökningen skulle så många som 80 procent av alla privatpersoner som är uppkopplade till Internet i hemmet utsättas för dataintrångsförsök. Dessutom bör det påpekas att i de undersökningar som utförts av BRÅ och RRV avses med dataintrång endast hacking, och det får till följd att gärningar som i och för sig skulle kunna anses utgöra dataintrång, men som klassificeras som cracking inte finns redovisade i statistiken.

Att försöka fastställa vilka ekonomiska kostnader dataintrång medför är inte heller en helt enkel uppgift. Som visats ovan i statistiken är företag dels ovilliga att över huvud taget anmäla att de utsatts för dataintrång och än mindre intresserade av att avslöja vilka ekonomiska konsekvenser de får. Att dataintrång kan medföra enorma kostnader finns det dock ett flertal exempel på. Ett fall, som i och för sig inte är svenskt men som ändå kan nämnas för att belysa vilka oerhörda skador som kan uppstå, är det s.k. ”Mafiaboy-fallet” där en kanadensisk tonåring gjorde sig skyldig till 56 åtal rörande dataintrång vilka orsakade skador för cirka 15 miljarder kronor.[84] Troligtvis får inte alla dataintrång lika omfattande ekonomiska konsekvenser, men exemplet ger i alla fall en indikation om att summorna det rör sig om inte är obetydliga. Detta medför att åtalen om dataintrång ofta kombineras med kraftiga skadeståndsanspråk.

[84] TT, Sydsvenskan 2001-01-26.

5 Praxis

5.1 Inledning

Erfarenheter visar att generellt sett få fall av dataintrång anmäls. Detta i kombination med bevissvårigheter resulterar i att det relativt sällan förekommer fällande domar avseende brottet dataintrång. Trots det finns ändå viss rättspraxis inom området och i det följande ska några av de mer uppmärksammade rättsfallen presenteras. Rättsfallen används för att belysa hur BrB 4:9c tillämpas i praktiken i syfte att försöka avgöra hur olika sorters dataintrång bedöms av domstolarna. Domstolsavgörandena har i det följande delats in i två kategorier; interna och externa dataintrång.

5.2 Internt dataintrång

Interna dataintrång karaktäriseras av att det finns ett anställningsförhållande eller någon annan form av auktorisering mellan gärningsmannen och brottsplatsen. Denna typ av brottslighet sker således på en arbetsplats t.ex. på ett företag eller en myndighet. En undersökning av praxis visar att interna dataintrång är en vanlig företeelse inom myndigheter, och under de senaste åren har flera fällande domar avkunnats. Framför allt inom landstinget, rättsväsendet och försäkringskassorna är det vanligt att personal olovligen tar del av registerinformation som inte är relevant för deras yrkesutövning. Svenska Polisförbundet har klargjort att dataintrång är ett vanligt förekommande brott inom polisen och enligt deras mening är inget annat brott lika frekvent inom yrkeskåren som detta.[85] Vid samma tillfälle konstaterades att det fanns ett 15-tal domar där poliser fällts för brottet dataintrång av varierande slag och omfattning. Även försäkringskassan har haft problem med hantering av skyddade personuppgifter, och i en rapport av Datainspektionen anmärktes på att en stor del av personalen hade tillgång till skyddade personuppgifter.[86] Sjukvårdens hantering av journaluppgifter har också varit föremål för kontroll av Datainspektionen vid ett flertal tillfällen, och problemet aktualiserades återigen i samband med rättsfallet om den s.k. *Blomberg-journalen*[87]. Nedan kommer ett par rättsfall att presenteras för att belysa problemet med interna dataintrång.

5.2.1 Polisfall 1

I mars 1995 avkunnade Svea hovrätt dom i ett mål[88] om dataintrång och tjänstefel. Den tilltalade, som var polisman, hade under lång tid och i relativt

[85] AD 1996 nr 23, s. 203.
[86] Datainspektionen, Direkt nr 4/2000, s. 9. Se även Datainspektionen, rapport 1999:3.
[87] Se vidare i kapitel 5.2.5.
[88] B 296/95

stor omfattning gjort slagningar, 10-15 stycken, i polisens dataregister varav vissa innehöll sekretessbelagda uppgifter. Syftet med merparten av registersökningarna var att kolla upp vissa personer som polismannen planerade att rapportera till SÄPO, medan avsikten vid ett tillfälle istället var att kontrollera en person som han ville rekommendera till Polishögskolan. Polismannen erkände de ifrågavarande gärningarna, men invände att han skulle vara fri från ansvar med hänvisning till nöd eftersom gärningarna syftade till att undanröja fara.

Tingsrätten ansåg att denna invändning inte var underbyggd, och då polismannens erkännande hade stöd av utredningen i övrigt kunde han inte undgå ansvar för gärningarna. Vad avsåg påföljdsfrågan konstaterade tingsrätten att straffvärdet för brottet är högt eftersom det anses vara av stor vikt att förtroendet för polisens tjänsteåtgärder upprätthålls.[89] Tingsrätten lade dock stor vikt vid ett uttalande från rikspolisstyrelsens personalansvarsnämnd om att polismannen vid en fällande dom skulle komma att skiljas från sin anställning. Detta ansågs vara ett sådant stort ingripande i sig att påföljden, trots brottets allvarlighet, borde bestämmas till villkorlig dom.[90] Med hänsyn till samma skäl dömdes inga böter ut i förening med den villkorliga domen.

Hovrätten gjorde ingen bedömning i ansvarsfrågan utan prövade enbart tingsrättens utdömda påföljd. Domstolen ansåg att det inte fanns några omständigheter som kunde föranleda en annan bedömning än den tingsrätten gjort, och påföljden fastställdes till villkorlig dom.

5.2.1.1 Kommentar

Både tingsrätten och hovrätten verkar vara av uppfattningen att dataintrång som begås av en polisman är att anse som ett allvarligt brott. Vid utdömandet av påföljd säger tingsrätten uttryckligen i domskälen att omständigheten att polismannen kommer att sägas upp från sin anställning gör att påföljden bör bestämmas till villkorlig dom, något som kan tolkas som att ett strängare straff hade utdömts om inte omständigheten hade förelegat. Vilken påföljd som hade varit aktuell i det fallet diskuteras inte närmare. Hovrätten konstaterar enbart att de omständigheter som framkommit i hovrätten inte föranleder någon annan bedömning, och de godtar således tingsrättens resonemang. Intressant att notera är dock att uppsägningen av polismannen ogiltigförklarades av arbetsdomstolen eftersom det ifrågavarande brottet inte ansågs utgöra saklig grund för uppsägning.[91] Med hänsyn till tingsrättens uttalande anser jag att det får förutsättas att en strängare påföljd hade valts om detta hade kunnat förutsägas.

[89] B 296/95, s. 7.
[90] B 296/95, s. 7.
[91] AD 1996 nr 23, s. 209.

5.2.2 Polisfall 2

I ett annat mål[92] som nyligen avgjordes av hovrätten dömdes en polisman för dataintrång sedan han gjort minst sju sökningar, som inte var nödvändiga för fullgörandet av hans arbetsuppgifter i polisens register. Polismannen, som varit anställd inom polisen i tio år, hade i och för sig behörighet att söka i ovan nämnda register, men de sökningar åtalet avsåg var gjorda för privat bruk. Enligt tingsrättens bedömning var gärningen att anse som tjänstefel i enlighet med BrB 20:1, men hovrätten undanröjde tingsrättens dom och utdömde istället ansvar för dataintrång. Motiveringen var att register-sökningarna saknat samband med de ärenden som handlagts av polismannen och därför inte innebar myndighetsutövning, något som är ett av rekvisiten för att tjänstefel ska föreligga. Hovrätten diskuterade även kring de bevissvårigheter som föreligger då det gäller att avgöra vilken information den som berett sig tillgång till register verkligen erhållit. Enligt hovrättens bedömning ska ett påstående om att en sökning inte gett tillgång till information enbart godtas om detta påstående stöds av andra uppgifter, och då inga sådana omständigheter lagts fram skulle den tilltalades påstående lämnas utan avseende.[93] Avslutningsvis konstaterades att eftersom det rört sig om registeruppgifter som var sekretesskyddade kunde brottet inte bedömas som ringa, och påföljden bestämdes till 60 dagsböter.[94]

5.2.2.1 Kommentar

I förevarande dom konstateras att den tilltalade gjort minst sju sökningar som är att klassificera som dataintrång, och enligt hovrättens bedömning ska det faktum att uppgifterna varit sekretesskyddade medföra att brottet inte är att bedöma som ringa. Huruvida detta innebär att brottet ska anses vara av normalgraden eller ett allvarligt brott kan dock inte avgöras av detta uttalande, utan den enda slutsatsen som kan dras är att det inte är ett lindrigt fall.

Vid avgörandet av ansvarsfrågan diskuterar hovrätten kring de bevissvårigheter som uppkommer då det ska fastställas vilken information den tilltalade berett sig tillgång till. Domstolens uttalande måste tolkas som att det föreligger en presumtion för att den som söker i register också erhåller den information som registerna innehåller, och den som hävdar motsatsen har bevisbördan. Denna omvända bevisbörda torde vara rimlig eftersom det annars skulle vara i princip omöjligt att i efterhand säkra bevis angående vilken information den tilltalade berett sig tillgång till.

[92] RH 2000:90.
[93] RH 2000:90, s. 275.
[94] RH 2000:90, s. 273, 275.

5.2.3 Larmoperatören

Ett annat fall[95] som är högst aktuellt avser en kvinna som varit anställd som larmoperatör vid polisens kommunikationscentral i Dalarna. Åtal väcktes vid Falu tingsrätt, och målet avsåg dataintrång och brott mot tystnadsplikten. Kvinnan hade tagit ut uppgifter ur polisens allmänna spaningsregister, och hon hade sedan sålt dessa för 500 kronor styck till en manlig bekant, som sedan vidarebefordrat dem till mc-klubben Bandidos. Åtalet avsåg sammanlagt fem olovliga sökningar som inte var nödvändiga för att kvinnan skulle kunna fullgöra sina arbetsuppgifter.

Kvinnan erkände gärningarna som lagts henne till last, och då erkännandet vann stöd av utredningen i övrigt fann tingsrätten att kvinnan var skyldig i enlighet med åtalet. I domskälen diskuterades ingående kring om påföljden skulle stanna vid böter eller om fängelse skulle utdömas. Tingsrätten ansåg att dataintrång har likheter med s.k. artbrott som mened och övergrepp i rättssak, eftersom det riktar sig mot en av samhällets centrala funktioner och därmed framstår som särskilt angelägen att förhindra. Dessutom innebär brottet ett missbruk av förtroendeställning som är relativt svårt att upptäcka, och därför ansåg tingsrätten att det förelåg en presumtion för fängelse. Straffvärdet för brottet bedömdes vara 3 månaders fängelse men p.g.a. kvinnans personliga förhållande, hon hade vårdnaden om fyra minderåriga barn och levde under socialt ordnade förhållande, dömdes hon till villkorlig dom med samhällstjänst i 100 timmar.

5.2.3.1 Kommentar

Kvinnan i fallet har berett sig tillgång till sekretessbelagda uppgifter i polisens register och sedan vidarebefordrat dessa till en bekant. Enligt tingsrättens bedömning är denna typ av brottslighet mycket allvarlig, dels eftersom den riktar sig mot en av samhällets centrala funktioner, dels p.g.a. att den innebär ett missbruk av förtroendeställning som är svårt att upptäcka. Domstolen drar paralleller till mened och övergrepp i rättssak och konstaterar att brottsligheten har likheter med artbrott vilket innebär att fängelsestraff bör utdömas. Vad är det då som gör att tingsrätten ser så allvarligt på dataintrånget i det aktuella fallet? Det är långt ifrån det första rättsfallet där någon står åtalad för olovliga intrång i polisregister. Det finns åtskilliga exempel på fällande domar där poliser stått åtalade för liknande brott, men inte i något tidigare fall har jag sett att domstolen dragit paralleller till artbrott. Inte heller i de övriga domar som redogjorts för i uppsatsen har domstolen fört ett lika långtgående resonemang. I *Polisfall 1* där en polisman dömdes i hovrätten för att ha utfört 10-15 olovliga slagningar i polisregister konstaterade domstolen att de såg allvarligt på den ifrågavarande brottsligheten men de diskuterade inte kring artbrott. Påföljden bestämdes i det fallet till villkorlig dom, eftersom domstolen tog i beaktande att polismannen troligen skulle skiljas från sin tjänst. Om detta inte varit fallet är det således rimligt att anta att ett fängelsestraff hade dömts

[95] Mål nr B 793-01.

ut. Denna utgång kan jämföras med domen i senare rättsfall som hovrätten avgjort. I *Polisfall 2* stod en polisman åtalad för att har utfört åtminstone sju olovliga sökningar i sekretessbelagda polisregisterm, och där konstaterar domstolen att denna typ av brottslighet inte är att anse som ringa. Domstolen påstår å andra sidan inte att brottsligheten är av allvarligt slag och inte heller förs något resonemang kring artbrott. Påföljden i det aktuella fallet bestäms till 60 dagsböter vilket skiljer sig ganska markant från *Polisfall 1* och *Larmoperatören*.

Finns det några särskilda omständigheter i det aktuella fallet som motiverar det höga straffvärdet, eller ska domen ses som att domstolarna intagit en hårdare syn på dataintrång begångna av anställda hos polisen? Utvecklingstendensen är enligt min mening inte helt klar. Visserligen konstaterade domstolen både i *Polisfall 1* och *Larmoperatören* att olovliga slagningar i polisregister är ett allvarligt brott och att en sträng påföljd ska utdömas. Däremellan kommer dock *Polisfall 2* där domstolen enbart konstaterar att olovliga slagningar i polisregister inte är att anse som ett ringa fall av dataintrång. Frågan är om skillnaden i domstolens fastställande av brottets allvarlighet kan förklaras av antalet slagningar som gjorts i de olika fallen? I målen där poliser stod åtalade genomfördes 10-15 respektive sju stycken olovliga slagningar och i fallet med larmoperatören fem stycken. Det strängaste straffet utdömdes dock i det fallet där det minsta antalet olovliga slagningar företagits nämligen i *Larmoperatören*, vilket innebär att inte enbart antalet kan ha haft någon avgörande betydelse för bedömningen av brottets allvarlighet.

Har omständigheterna kring brottet i övrigt tagits i beaktande vid bestämmandet av brottets straffvärde? Det finns inga uttalande i de respektive domarna som talar för detta. Varken i *Polisfall 1*, *Polisfall 2* eller i *Larmoperatören* har domstolen angivit i domskälen att de har fäst någon vikt vid vad de erhållna uppgifterna ska användas till. Det är kanske ändå inte helt omöjligt att domstolen har tagit i beaktande att larmoperatören sålt de sekretessbelagda uppgifterna vidare. Till skillnad från de båda polismännen har hon inte enbart berett sig tillgång till uppgifterna för att använda dem för egen del, utan hon har även spridit de känsliga uppgifterna hon tagit del av vidare. Ett spridande av de sekretessbelagda uppgifterna innebär troligtvis att skadan blir större, och eventuellt kan detta ha tagits med vid bedömningen av brottets straffvärde. Domstolen resonerar dock inte uttryckligen kring detta i domen, men de konstaterar att brottet är av sådan art att presumtion för fängelse föreligger. Enligt min uppfattning är detta den troligaste förklaringen till den skillnad som kan konstateras i synen på brottets straffvärde i de redovisade rättsfallen.

5.2.4 Försäkringskassan

I ett aktuellt fall där åtal väckts men dom ännu inte meddelats står en kvinnlig handläggare vid försäkringskassan i Västra Götaland åtalad för

dataintrång och brott mot tystnadsplikten.[96] Handläggaren misstänks för att ha gjort utdrag ur försäkringskassans datasystem vilka hon sedan vidarebefordrat till sin son, som har medverkat i ett nazistiskt nätverk där bl.a. den morddömde Hampus Hellekant ingår. Utdragen har innehållit information om namn, adress, personnummer och i vissa fall inkomst och antal barn, och fyra av de personer som förekommer i utdragen har skyddad identitet.[97] Bland de 40-tal personer som kvinnan gjort utdrag på finns det journalistpar som utsattes för en bilbomb i juni 1999.[98] Kvinnan har erkänt att hon tagit ut samtliga registerutdrag, men hon säger sig vara omedveten om att hon har begått ett brott. Till sitt försvar har hon anfört att avseende det stora flertalet utdrag har hon inte gjort sig skyldig till någon brottslig gärning eftersom uppgifterna är offentliga och kan begäras ut hos skattemyndigheten.[99]

5.2.4.1 Kommentar

I skrivande stund har dom i det aktuella målet ännu inte avkunnats, men eftersom kvinnan erkänt gärningen och erkännandet verkar stödjas av utredningen i övrigt är det troligt att en fällande dom är att vänta. En intressant fråga är huruvida kvinnans invändning om att uppgifterna är offentliga och kan erhållas hos Skattemyndigheten bör resultera i att gärningen inte bedöms som straffbar. Troligtvis beror det på omständigheterna kring hur uppgifterna erhölls som t.ex. var de ifrågavarande uppgifterna fanns tillgängliga etc. Har kvinnan t.ex. fått tag på uppgifterna i en akt eller ett registerutdrag där det finns andra, icke-offentliga uppgifter är det troligt att kvinnans invändning bör lämnas utan avseende.[100] Med beaktande av tidigare rättspraxis där omständigheterna varit likartade, t.ex. *Larmoperatören*, finns det anledning att tro att tingsrätten kommer att se allvarligt på brottet. Kvinnan har gjort ett stort antal slagningar på ca 40 personer, varav vissa har haft skyddad identitet. Dessutom har hon vidarebefordrat uppgifterna till medlemmar i ett nazistiskt nätverk, vilket medför att tingsrätten torde kunna föra ett liknande resonemang om artbrott som gjordes i *Larmoperatören*. Min bedömning är att tingsrätten kommer att anse att det föreligger en presumtion för fängelse och att straffvärdet kommer att bestämmas till ett par månaders fängelse. Jag har inga vidare uppgifter om kvinnans personliga förhållande men eventuellt kan de bidra till att villkorlig dom istället utdöms.

5.2.5 Blomberg-journalen

Även inom sjukvården finns exempel på fällande domar, och ett fall som för närvarande är föremål för prövning i Hovrätten för Västra Sverige är målet

[96] Mål nr B 8608-00. Huvudförhandling är utsatt till 9 november 2001.
[97] Sandberg, DN 2001-11-08.
[98] Gilså, Computer Sweden 2001-06-20; Harne, Aftonbladet 2001-11-09.
[99] Johansson, DN 2001-11-09.
[100] För vidare diskussion se kapitel 6.3.

om den s.k. *Blomberg-journalen*. Målet[101] har avgjorts av Göteborgs tingsrätt och det avser en sjuksköterska som åtalats för dataintrång sedan hon olovligen inhämtat information från en patientjournal. Sjuksköterskan var inte delaktig i vården av patienten utan hon uppgav att hon gick in i journalen dels i utbildningssyfte, dels p.g.a. att hon var nyfiken. Enligt gällande praxis på arbetsplatsen är det vanligt förekommande att personalen som hjälp i arbetet tittade i patientjournaler avseende patienter, som de inte deltar i vården av. Med hänsyn till detta hävdade sjuksköterskan att hon inte visste om att hennes förfarande var olovligt.

Tingsrätten ansåg det vara utrett att kvinnan gick in i den aktuella journalen dels i utbildningssyfte, dels p.g.a. nyfikenhet.[102] För att ett intrång ska vara straffbelagt krävs dock att det skett olovligen, och vad avser patientjournaler ska föreskrifterna i Patientjournallagen och Socialstyrelsens föreskrifter och allmänna råd tillämpas. Där stadgas att endast en begränsad del av personalen vid en klinik behöver ha tillgång till patientens journal, och att läsning p.g.a. ren nyfikenhet aldrig kan godtas. Med beaktande av detta ansågs sjuksköterskans dataslagning vara olovlig.[103]

Vidare diskuterades huruvida sjuksköterskans påstående att hon inte visste om att förfarandet var olovligt skulle beaktas. Tingsrätten konstaterade att hennes påstående inte motsades av utredningen, och att det inte fanns någon anledning att anta att hon handlat på samma sätt om hon vetat om att agerandet var olovligt.[104] Det ursprungliga syftet med kriminalisering av dataintrång var att skydda den enskilde mot otillbörliga intrång i den personliga integriteten, och för att upprätthålla datalagstiftningens effektivitet ansåg tingsrätten att ansvar kunde utdömas även om förövaren inte själv klassificerat sitt handlande som olovligt.[105] Även om sjuksköterskan till viss del kunde anses ursäktad i sitt beteende ansågs hon dock ha gjort sig skyldig till dataintrång, och påföljden bestämdes till 30 dagsböter. Tingsrättens dom har överklagats till hovrätten men dom i målet har ännu inte meddelats.

5.2.5.1 Kommentar

Tingsrättens dom i målet får ses som ett pilotfall. Den aktuella sjuksköterskan var inte ensam om att ha berett sig tillgång till patientjournalen, utan ytterligare 25 anställda vid samma sjukhus hade varit inne och tittat i journalen trots att de inte var delaktiga i vården av patienten. Att ”smygtittande” i patientjournaler är ett vanligt förekommande fenomen på sjukhus bekräftas både av de anställda och av utomstående granskningar av rutinerna. Problemet är ingen ny företeelse utan det uppmärksammades redan 1999 då Carl Bildt vårdades på sjukhus efter en kollaps. Även då

[101] Mål nr B 11913-99.
[102] B 11913-99, s. 4.
[103] B 11913-99, s. 5.
[104] B 11913-99, s. 5.
[105] B 11913-99, s. 6-7.

kunde konstateras att patientjournaler hade lästs av personal som inte var delaktiga i hans vård, men i detta fall väcktes inga åtal.

Om hovrätten gör samma bedömning som tingsrätten kommer domen att vara ett viktigt riktmärke vid avgörande av liknande fall. Enligt sjuksköterskornas uttalande har det rått oklarhet om huruvida beteendet är tillåtet eller inte, och majoriteten verkar vara av uppfattningen att det tillhör den vardagliga rutinen att titta i patientjournaler för att däri söka ledning. Oavsett hur hovrätten bedömer gärningen så kommer domen att spela en viktig roll för att skapa klarhet i det gällande rättsläget, och blir domen liksom i tingsrätten fällande kommer den troligtvis att ha en preventiv effekt. Om det slås fast att förfarandet är olagligt får det antas att det stora flertalet sjuksköterskor i fortsättningen undviker att smygläsa journaler, särskilt med tanke på att det med hjälp av användaridentiteter går att avgöra vem som bereder sig tillgång till vilken journal.

5.3 Externt dataintrång

Karaktäristiskt för externa dataintrång är att förövaren av dataintrånget kan klassificeras som ”utomstående” i förhållande till angreppsobjektet. Gärningsmannen har således inte tillgång till angreppsobjektet p.g.a. anställningskontrakt eller dylikt utan han agerar från utsidan. Enligt de undersökningar som presenterats ovan utsätts privatpersoner ofta för externa dataintrång. Jag har dock inte lyckats hitta några rättsfall för att belysa problematiken. Statistiska uppgifter visar även att företag är ett vanligt offer för externa dataintrång och i det följande redogörs får några av de mer uppmärksammade fallen.

5.3.1 Spray

I ett uppmärksammat mål[106] som avgjorts av Gävle tingsrätt stod en 17-årig man åtalad för dataintrång och utpressning sedan han bl.a. tagit sig in i företaget Sprays dataserver, och därefter begärt ersättning med 10 000 för att berätta hur han lyckats ta sig in i datasystemet. 17-åringen hade via Internet fått kontakt med en av de anställda vid Spray, och under ett av deras samtal avslöjat att han tagit sig in i företagets dataserver. De hade därefter stämt möte på företagets kontor och där upprättat ett kontrakt enligt vilket den tilltalade gavs i uppdrag att mot en ersättning på 10 000 kronor utföra säkerhetskonsultationer för Sprays nätverk. 17-åringen bestred ansvar för de ifrågavarande gärningarna med hänvisning till att tillträdet till dataservern inte skett olovligen, och till att han hade haft en uppgörelse med företaget att göra en översyn av datasäkerheten.

Tingsrätten ansåg det vara utrett att 17-åringen tagit sig in på företagets dataservrar, och det fanns inga uppgifter som gav stöd för påståendet att han

[106] B 12-97.

skulle haft tillstånd till detta.[107] Åtalet för dataintrång ansågs följaktligen styrkt. Angående åtalet för utpressning ansågs det vara utrett att ett skriftligt avtal upprättats mellan den tilltalade och företaget, och trots att det förekommit en del hotfulla uttalande från den tilltalades sida var tingsrätten av uppfattningen att han ansett att det fanns en överenskommelse med företaget.[108] Med hänsyn till den tilltalades uppfattning att han faktiskt fått ett uppdrag, och även med beaktande av hans unga ålder ansåg tingsrätten att uttalandet inte kunde anses som ett utpressningsförsök, utan åtalet på denna punkt ogillades.[109] Vid bestämmandet av påföljden tog tingsrätten hänsyn till den tilltalades ålder samt det faktum att han tidigare var ostraffad och levde under ordnade förhållande, och påföljden bestämdes till kännbara böter, 60 dagsböter.

5.3.1.1 Kommentar

Den tilltalade dömdes för två fall av dataintrång och tingsrättens bedömning var att detta skulle resultera i kännbara böter. Påföljden bestämdes till 60 dagsböter. Tingsrätten för inget vidare resonemang om huruvida brottet ska anses vara av allvarlig art eller inte. Jämförelser kan göras med liknande brott där unga män dömts för dataintrång. I ett fall, *Studentfallet*, stod två studenter åtalade för dataintrång sedan de gjort dataintrång i KTH:s datasystem och med hjälp av stulna lösenord och användaridentiteter hämtat hem olovliga programvarukopior, som de sedan spred olagligt. Värdet på programvaran uppskattades till miljontals kronor, och tingsrätten såg allvarligt på studenternas brottslighet, men de ansåg att det var tillräckligt att ge dem kraftiga böter och påföljden fastställdes till 80 dagsböter.[110] I ett annat fall, *Nasa-hackers,* dömdes två ungdomar till villkorlig dom sedan de brutit sig in i det amerikanska försvarets, flygvapnets och den amerikanska marinens datasystem.[111] Straffet i *Spray-målet* är således inte lika strängt som i de andra fallen. Gemensamt för alla dessa domar är att domstolen vid bestämmande av påföljd har tagit hänsyn till gärningsmännens ålder. Det kan tolkas som att domstolen mycket väl kunnat utdöma ett fängelsestraff i ett liknande fall där förövaren är äldre.

5.3.2 Aftonbladet

Ett annat mycket omskrivet mål[112] avgjordes av Lunds tingsrätt, och där stod en ung man åtalad för att ha gjort sig skyldig till dataintrång på bl.a. Aftonbladets hemsida. Den tilltalade hade via Internet fått tag på lösenordet till Aftonbladets hemsida, och genom att gå in i deras webbserver hade han lyckats byta ut denna mot en felaktig hemsida på vilken det skrivits att Aftonbladet och deras stora konkurrent Expressen skulle gå ihop. Han stod

[107] B 12-97, s. 5.
[108] B 12-97, s. 5.
[109] B 12-97, s. 6.
[110] Jansson, Aftonbladet 2001-09-17.
[111] Svidén, Computer Sweden 2000-02-29.
[112] B 1914-97.

också åtalad för dataintrång hos ett Vetlanda-företag eftersom han berett sig tillträde till företagets e-post och raderat kataloger i namn- och mailservern.

Eftersom den tilltalade erkände gärningarna och erkännandet fann stöd i utredningen i övrigt krävdes ingen längre diskussion kring ansvarsfrågan, utan istället koncentrerade sig domstolen på bedömningen av påföljden. Tingsrätten var av uppfattningen att den typ av brottslighet som den tilltalade gjort sig skyldig till var av så allvarligt slag att påföljden inte kunde stanna vid böter. Med hänsyn till att den tilltalade tidigare var ostraffad och att han levde under ordnande sociala förhållande ansåg dock tingsrätten, ”efter viss tvekan”, att påföljden kunde stanna vid villkorlig dom i kombination med höga dagsböter; 100 st.[113]

5.3.2.1 Kommentar

Tingsrätten ansåg att den ifrågavarande brottsligheten var av allvarligt slag, och deras tveksamhet vid valet av påföljd understödjer även detta påstående. Den tilltalade hade inte enbart berett sig tillgång till Aftonbladets hemsida respektive företagets servrar, utan han hade dessutom ändrat och raderat i den information som erhållits. Att den tilltalade inte tidigare begått några brott samt att han levde under välordnade förhållande bidrog dock till att inte en strängare påföljd utdömdes. Tingsrättens uttalande ”efter viss tvekan” torde väl knappast kunna tolkas på något annat sätt än att ett fängelsestraff mycket väl hade kunnat utdömas för brottet.

5.3.3 KTH och SU

P.g.a. de stora ekonomiska skador som ofta följer av dataintrång är det vanligt att åtalen kombineras med ett skadeståndsanspråk. I ett mål[114] som prövades av Stockholms tingsrätt yrkade Kungliga Tekniska Högskolan, KTH, och Stockholms Universitet, SU, ersättning på cirka 350 000 respektive 100 000 kr från svaranden. Skadeståndsanspråket grundades på de skador som orsakats av de dataintrång hos KTH och SU, som svaranden gjort sig skyldig till. Svaranden hade tidigare blivit dömd för brotten till dagsböter efter att han vid ett stort antal tillfällen berett sig tillträde till upptagningar för automatisk databehandling i KTH:s och SU:s datorer. Genom användning av vissa program lyckades han knäcka de personliga lösenorden, och på så sätt få tillgång till alla, inklusive privata, filer i systemet.[115] Kostnaderna som KTH och SU yrkade ersättning för avsåg utgifter för spårning av dataintrången och telefonsamtal, samt utgifter för byte av lösenord. Svaranden invände mot skadeståndsanspråken och anförde att dessa skulle jämkas med hänvisning till tre grunder; att han inte varit ensam om att göra intrång, att datasystemen hade ett i princip obefintligt skydd mot intrång och att han inte utnyttjat eller spridit informationen han

[113] B 1914-97, s. 3.
[114] T 8-624-96.
[115] T 8-624-96, s. 4.

kom åt.[116] Tingsrätten ansåg dock att de åberopade omständigheterna inte kunde utgöra grund för jämkning av skadeståndet och biföll kärandens yrkanden.

5.3.3.1 Kommentar

Domen belyser de stora ekonomiska konsekvenser som ett dataintrång kan få, och domstolen gjorde bedömningen att ett intrång kan vara kostsamt även om informationen som den tilltalade berett sig tillgång till inte spridits eller utnyttjats på något annat sätt. Att dataintrång kan vara förenat med stora kostnader för den som utsatts för gärningen har studien av statistik visat och dessa uppgifter får nu även stöd av uttalande i praxis. Förhoppningen med ett erkännande av stora skadeståndsanspråk vid dataintrång är att hackers ska avskräckas från att begå liknande brott.[117] Denna förklaring verkar till viss del vara rimlig. Det kan tänkas att den ekonomiskt rationella brottslingen avstår från att göra ett dataintrång om han är medveten om att ett högt skadestånd kan utdömas. Ett exempel på brottslighet som skulle kunna förhindras på detta sätt är sådana dataintrång som begås i syfte att sälja uppgifterna vidare liknande det i *Larmoperatören*. Om den tilltalade i det aktuella rättsfallet riskerat att få betala kraftiga skadestånd kan det kanske tänkas att hon låtit bli att begå brottet. Med liknande motivering skulle ”nyfikenhetsbrott” som det i *Blomberg-journalen* eller olovliga sökningar i polisregister kunna förhindras. Å andra sidan är det tveksamt om den ekonomiska skadan i likartade fall blir så omfattande som i *KTH och SU*. Enligt de statistiska uppgifterna är de ekonomiska skadorna betydligt större vid interna dataintrång än vid externa. De ekonomiska skador som anges vid interna dataintrång har dock framför allt avsett skador som orsakats av att företagshemlig information åtkommits etc.

De situationer där troligtvis de största skadorna åsamkas är de mer omfattande intrången i företags och myndigheters datasystem, som begås av någon utomstående, och enligt statistiken är upptäcktsrisken vid dessa brott i princip obefintlig. Dessutom visar statistiken att dessa brott sällan polisanmäls. I jämförbara fall anser jag det vara föga troligt att höga skadestånd skulle ha någon avskräckande effekt på presumtiva gärningsmän. Vad som vidare bör påpekas är att i straffskalan för dataintrång ingår redan en allvarlig påföljd, två års fängelse, och det kan diskuteras om den som inte avskräcks av en sådan kraftig sanktion kommer att avstå från att begå en brottslig gärning p.g.a. att en ekonomisk sanktion riskerar att utdömas.

5.4 Analys

Dataintrång är ett samlingsbegrepp för ett stort antal olika gärningar, vilka alla har gemensamt att det sker ett intrång i en upptagning för ADB, men som framgår av redovisad praxis är sättet på vilket dataintrånget begås

[116] T 8-624-96, s. 7-8.
[117] Andersson, s. 19.

väldigt skiftande. I vissa fall består den brottsliga gärningen av att någon ”smygtittar” på information som de har tillgång till men inte någon befogenhet att ta del av. I andra fall är intrånget mer avancerat och består t.ex. av att gärningsmannen tar sig in i ett datasystem, som han inte har behörighet till.

Liksom gärningarna kan vara av olika slag varierar också skadan som gärningen orsakar från fall till fall. Vid vissa dataintrång, som i *Aftonbladet,* är det direkta syftet med gärningen att ändra i den information som erhålls, och vid denna typ av brottslighet är det en ganska naturlig följd att skadan kan bli relativt omfattande. Rättsfallet utgör ett typexempel på cracking. I studien av rättspraxis har jag kunnat konstatera att även andra sorters dataintrång kan orsaka stora skador och då framför allt gärningar som kan klassificeras som oren hacking. Dataintrång som innefattar att gärningsmannen tillgodogör sig företagskänslig information, eller information som innehåller sekretessbelagda uppgifter kan resultera i stora skador för den drabbade. Detta har bl.a. slagits fast i *KTH och SU*. Ett annat fall där det kan tänkas att domstolen skulle göra samma bedömning om en skadeståndsprocess skulle drivas är *Försäkringskassan* och *Larmoperatören*. I dessa fall resulterade dataintrånget i att sekretessbelagda uppgifter såldes vidare till Bandidos-medlemmar respektive nynazister, och skadan av gärningarna kan antas vara relativt omfattande.

Det är kanske inte möjligt att tala om gärningar som inte orsakar någon som helst skada, men i vissa fall kan ändå den skada som uppkommer vid vissa dataintrång anses som relativt liten. Så kan t.ex. vara fallet vid vissa former av ren hacking där gärningen enbart består av att bereda sig tillgång till vissa datasystem utan att tillgodogöra sig informationen ifråga. Den typen av dataintrång kan trots den relativt lindriga skadan ändå bli mycket kostsam för offret, t.ex. om stora insatser läggs ner på att försöka spåra och identifiera gärningen. Detta framkommer framför allt vid en studie av statistiken inom området där det har gjorts försök att uppskatta kostnaderna av dataintrång och där de konstateras att de är långt ifrån obefintliga. Av denna anledning är det motiverat att inte utgå från något skaderekvisit vid avgörandet av om ett dataintrång har begåtts. Lagstiftaren verkar även ha haft detta i åtanke eftersom något skaderekvisit inte tagits med i paragrafens ordalydelse.

Inte heller vid bedömande av brottets allvarlighet verkar domstolen ha tagit hänsyn till vilken skada som åsamkats. Domstolen verkar se allvarligt på i huvudsak två typer av dataintrång, dels externa dataintrång, dels interna dataintrång där sekretessbelagda uppgifter spridits vidare. I samtliga genomgångna rättsfall avseende externa dataintrång har domstolen uttalat att de ser allvarligt på den ifrågavarande brottsligheten. I såväl *Nasa-hackers* som *Aftonbladet* dömdes de tilltalade till villkorlig dom och i *Studentfallet* utdömdes kraftiga böter, men i samtliga fall har domstolen resonerat kring fängelsestraff. Enda anledningen till att en strängare påföljd inte utdömts verkar vara att gärningsmännen i de ifrågavarande rättsfallen varit unga och

levt under ordnade förhållande. Ett lika konsekvent strängt förhållningssätt till brottsligheten som domstolen intagit till externa dataintrång går inte att finna avseende interna dataintrång. Om domstolen i princip har diskuterat kring fängelse i samtliga fall av externa dataintrång har det bara skett i ett fall av internt dataintrång, *Larmoperatören*. Signifikant för fallet är att registeruppgifterna som erhållits vid dataintrånget spridits vidare och domstolen anser att vid ett så allvarligt brott föreligger en presumtion för fängelse. Om mina antagande är riktiga borde domstolen föra ett liknande resonemang om fängelse i *Försäkringskassan.*

6 Problem och brister

6.1 Inledning

Mot bakgrund av den granskning av lagregeln och den presentation av praxis och statistik som gjorts i föregående avsnitt är det intressant att försöka fastställa om den befintliga lagstiftningen kan tänkas ha några problem eller brister. I följande avsnitt kommer att undersökas dels om den gällande lagstiftningen kan tänkas ha några luckor eller om den kan ses som en heltäckande och effektiv reglering, dels vilka övriga svårigheter som t.ex. gränsdragnings- och identifieringsproblem som kan uppkomma vid tillämpning av paragrafen.

6.2 Luckor i lagen

Trots att paragrafen om dataintrång till viss del ändrats för att fylla i de luckor i lagstiftningen som uppstått till följd av den tekniska utvecklingen är bestämmelsen inte en heltäckande reglering. Huvudsyftet med lagregeln har varit att täcka in de brottsliga gärningar som faller utanför de övriga regleringar som redan fanns på området, men det har visat sig att vissa gärningar i alla fall inte omfattas av bestämmelsen.

Medan det i vissa fall har varit svårt att avgöra huruvida ett visst förfarande ska falla in under bestämmelsen eller inte har det i andra fall varit lättare att konstatera att en viss gärning helt klart faller utanför paragrafens tillämpningsområde. Som exempel på en sådan gärning kan anges det förfarande som innebär att gärningsmannen endast undanhåller en upptagning utan att det går att klassificera gärningen som intrång i upptagningen.[118] Ett annat förfarande som inte heller omfattas av lagstiftningen är om s.k. logiska verktyg används för att skada en upptagning.[119]

Andra potentiella luckor i lagstiftningen har varit mer omdiskuterade än de som nämnts i det föregående, och som exempel kan anges s.k. röjande signaler. Röjande signaler alstras då teknisk utrustning utför informationsbehandling och de utgörs av akustiska, elektriska och elektromagnetiska signaler.[120] Vanligtvis utgörs röjande signaler av strålning från bildskärmar, men begreppet innefattar även strålning från hårddiskar och kablar.[121] Röjande signaler har inget egentligt kommunikationssyfte, men om de avlyssnas kan de ge tillgång till information. Till exempel är det

[118] Silvander, s. 221.
[119] Silvander, s. 221.
[120] Almblad & Brorsson, s. 12.
[121] Gustavsson, s. 3.

möjligt att på upp till ett par hundra meters avstånd avlyssna den elektromagnetiska strålning som alstras av en bildskärm till en dator, och på så sätt uppfatta skärmbilden.[122] Dessa signaler anses inte vara radiokommunikation i Radio- och TV-lagens bemärkelse eftersom de *oavsiktligt* har kommit ut i etern, och de kan inte heller betraktas som upptagning för automatisk databehandling då signalerna inte tillkommit i ett sådant syfte.[123] Konsekvensen blir att en olovlig avlyssning eller upptagning av sådana signaler faller utanför de båda regleringarnas tillämpningsområde. Detta verkar vara den dominerande uppfattningen vilken bl.a. DSU och IT-utredningen ställt sig bakom. Andra har dock varit av annan åsikt och ansett att någon ändring av reglerna i detta avseende inte varit nödvändig, eftersom förfarandet redan täcks upp av den befintliga lagstiftningen.[124]

6.3 Tveksamma fall

Förutom de förfarande som faller utanför lagens tillämpningsområde finns handlingar som ger upphov till gränsdragningsproblem när det gäller att avgöra det straffbara området. Studien av rättsfall visar att det finns aktuella fall inom vården där det råder tveksamhet om vilka handlingar som ska anses utgöra dataintrång. Enligt praxis inom sjukvården är det vanligt att titta i journaler avseende patienter som man inte deltar i vården av förutsatt att det sker i utbildningssyfte. Det är dock tveksamt i vilken omfattning detta är tillåtet. Aktuella föreskrifter på området ger ingen vidare vägledning utan de stadgar enbart att endast en begränsad del av personalen vid en klinik behöver ha tillgång till patienters journal. Det finns således ett behov av att ytterligare klargöra i vilken omfattning det är tillåtet att ta del av patienters journaler, för att kunna avgöra vilka handlingar som ska anses som straffbara dataintrång, och vilka som är i enlighet med föreskrifterna inom området.

Ett ytterligare område där det enligt studien av rättsfall kan råda tveksamhet om en gärning ska klassificeras som ett internt dataintrång är när en anställd bereder sig tillgång till uppgifter som visserligen är offentliga, men som inte är nödvändiga för fullgörande av arbetsuppgifterna. Frågan har framför allt aktualiserats i samband med *Försäkringskassan* men även tidigare har domstolarna diskuterat kring om det faktum uppgifterna som tagits fram är offentliga och finns att tillgå vid någon annan myndighet ska läggas till grund vid avgörande av om gärningen ska anses som brottslig eller inte. I RH 2000:90 konstaterade tingsrätten att vissa uppgifter som polismannen tagit fram visserligen funnits tillgängliga i ett registerutdrag vid tingsrätten, men eftersom polisens register även innehåller andra uppgifter ansågs förfarandet vara olovligt. Dessutom påpekade domstolen att den tilltalade inte haft något fog för sina sökningar. Tingsrättens uttalande om att inte alla uppgifter i utdraget var offentliga kan tolkas som att i det fall samtliga

[122] SOU 1992:110, s. 190.
[123] SOU 1992:110, s. 190-191.
[124] Se bl.a. Almblad & Brorsson, s. 41-42.

upplysningar varit offentliga hade gärningen inte varit brottslig. Frågan är om det är riktigt att dra denna slutsats? Jag anser det dock vara viktigt att rättsläget på denna punkt klargörs för att de som handskas med offentliga uppgifter får besked om vad som utgör en straffbar handling.

Ett ämne som varit föremål för het debatt är huruvida en arbetsgivare ska anses ha rätt att ta del av sina anställdas e-post, eller om ett sådant förfarande faller in under bestämmelsen om dataintrång. Frågeställningen är långt ifrån ny, men problemet har uppmärksammats framför allt på senare tid. Som nämnts i kapitel 3.4.3 jämställs e-post vanligtvis med vanliga brev, och frågan är vem som ska anses ha behörighet att lovligen ta del av sådan e-post som finns lagrad i teknisk utrustning på en arbetsplats. Problemet har berörts på ett flertal ställe i förarbetena till bestämmelsen om dataintrång, men trots det går det inte att hitta något direkt svar på frågan. IT-utredningen uttalade i sitt betänkande att det var av stor vikt att myndigheter genom interna föreskrifter meddelade sin personal om vad som gäller i olika hänseende.[125] Enligt allmänna bestämmelser är gärningen fri från straffansvar om ett samtycke föreligger, men det har ännu inte prövats rättsligt om en myndighet kan anses förfoga över olovlighetsrekvisitet genom att meddela ett förbud mot privat användning av e-post med följd att privata meddelande skickade till en e-post adress får läsas utan samtycke.

DSU begränsade inte sin diskussion till myndigheter utan de uttalade allmänt att en arbetsgivare har rätt att bereda sig tillgång till data i de datautrymmen han tillhandahållit, förutsatt att han först meddelat arbetstagaren att informationsbehandling inte får ske för privat bruk. Denna åsikt delas bl.a. av det IT-rättsliga observatoriet, Jusek och SAF (numera Svenskt Näringsliv).[126] Även domstolspraxis ger stöd för denna uppfattning eftersom ingen fällande dom har avkunnats i de flertal fall där arbetsgivarens rätt att undersöka anställdas e-post har prövats av arbetsdomstolen.[127] Enligt DSU ska detta dock inte gälla om arbetsgivaren givit den anställde tillstånd att använda utrustningen utanför arbetet, och råder det tveksamheter om vad som tillåtits ska en restriktiv hållning intas.[128] Har inget förbud för privat användning meddelats ska utgångspunkten vara att e-post är avsedd för arbetsändamål, men hänsyn ska även tas till den sedvänja avseende privat användning av e-post som finns på arbetsplatsen.[129] En arbetsgivare som vill undvika risken att göra sig skyldig till dataintrång bör alltså för att slippa oklarheter tydligt informera sina anställda om vad som gäller.

Rättsläget inom detta område är dock inte helt klart och genom direktiv 1999:73 har Integritetsutredning tillsatts som bl.a. har fått i uppdrag att se

[125] SOU 1996:40, s. 253.
[126] IT-rättsliga observatoriet, PM 5:1999; SOU 1992:110, s. 560; Byttner, Computer Sweden nr 121 1999.
[127] Byttner, Computer Sweden nr 99 2000.
[128] SOU 1992:110, s. 560-561.
[129] IT-rättsliga observatoriet, PM 5:1999.

över skyddet av personlig integritet i samband med användning av e-post i arbetet. Utredningens arbete förväntas vara färdigt vid årsskiftet 2001/2002.

6.4 Tolkningsproblem

Viss kritik har även riktats mot paragrafens nuvarande skyddsobjekt; upptagning för automatisk databehandling, och då framför allt mot fokuseringen på data eftersom det anses kunna ge upphov till tolkningsproblem. Begreppet data anses vara ett alltför vidsträckt begrepp som innefattar både uppgifter för automatisk databehandling och traditionella representationsformer som skriftliga handlingar, och detta stämmer inte överens med regelns tillämpningsområde.[130] Visserligen har en avgränsning av vilken data som avses i lagregeln gjorts genom ordvalet ”upptagning för automatisk databehandling”, men denna lösning anses ändå inte vara ändamålsenlig. Dessutom kritiseras att tonvikten lagts vid ett materiellt begrepp, d.v.s. vid representationen av information och inte vid informationen som sådan eftersom data vanligtvis anses vara immateriell.[131]

Ett av de mer omfattande förslagen till ändrad lagstiftning presenterades av DSU och enligt deras betänkande[132] ska data som fysiskt fenomen vara det nya skyddsobjektet i en reformerad lagstiftning. Enligt den nya ordalydelsen ska olovliga intrång i ”data för automatisk informationsbehandling” kriminaliseras. Detta innebär att data inte ska anses vara information utan istället ska med ”data” avses fysiska fenomen som bär information. [133] Det avgörande rekvisitet är att informationen uttrycks i en för datorn omedelbart bearbetbar representationsform.[134]

Förslaget har dock mött kraftig kritik bl.a. från det IT-rättsliga observatoriet. Enligt deras uppfattning kommer användande av begreppet ”information” i stället för data i ett straffrättsligt sammanhang att medföra problem, eftersom begreppet är väldigt mångtydigt och i allmänt språkbruk anses som en samlingsbeteckning för olika fenomen.[135]

6.5 Identifierings- och bevisproblem

Även om det kan konstateras att en gärning täcks in av brottsbeskrivningen i BrB 4:9c och att ett dataintrång således har begåtts visar studien av statistik att det kan vara svårt att finna förövaren av brottet. Problemet med att spåra och identifiera gärningsmannen varierar bl.a. beroende på om dataintrånget kan klassificeras som internt eller externt.

---

[130] SOU 1992:110, s. 83, 176-180.
[131] Almblad & Brorsson, s. 31.
[132] SOU 1992:110.
[133] Almblad & Brorsson, s. 31.
[134] SOU 1992:110, s. 114.
[135] IT-rättsliga observatoriet, PM 3:1999, s. 2.

Vid interna dataintrång är det relativt lätt att spåra förövaren förutsatt att det finns ett väl fungerande system med behörigheter och användaridentiteter på arbetsplatsen. På företag och myndigheter där ett stort antal personer vanligtvis har tillgång till datasystemen används sådana system som regel, men det finns fortfarande en rad arbetsplatser där rutinerna är bristfälliga eller helt saknas.

Ett område där problemet särskilt har uppmärksammats är inom vården, och i Datainspektionens årsredovisning för år 2000 påpekades ett flertal brister som bidrar till att underlätta dataintrång och försvåra igenkännandet av förövaren.[136] En av de stora säkerhetsbristerna inom vården avsåg användningen av behörigheter och användaridentiteter. Kritik riktades framför allt mot att behörigheterna inte är begränsade till ett så litet antal personer som möjligt, utan de är tillgängliga för en stor del av de anställda. Vidare påpekades att fungerande rutiner för tilldelning av behörigheter saknas, och det resulterar bl.a. i att gamla behörigheter för personer som slutat inte tas bort. Följden av detta blir att ett stort antal personer lätt kan bereda sig tillgång till information som de egentligen inte har behörighet att ta del av. Ett ytterligare problem är att de användaridentiteter som användes vid sökning i register inte är personliga, utan de används av ett stort antal personer. Detta resulterar i stora svårigheter när det gäller att spåra gärningsmannen till dataintrånget. För att underlätta spårningen av vem som har haft åtkomst till personuppgifterna ska en maskinell logg finnas, men vid inspektionen konstaterades att logg antingen saknas, eller att det inte finns några rutiner för att kontrollera den. Samtliga brister i systemet med behörigheter och användarrutiner bidrar till att interna dataintrång kan vara svåra att spåra inom vården.

Om det är relativt enkelt att vidta åtgärder för att effektivt kunna spåra gärningsmannen vid interna dataintrång är det desto svårare att hitta förövaren vid externa. Vid dataintrång som sker genom användning av teleförbindelser går det ofta att spåra förövaren via s.k. logg-filer på samma sätt som vid interna dataintrång. I loggfilerna återfinns IP-adressen för avsändaren, och denna adress är individuell och obligatorisk för varje Internet-ansluten dator.[137] Adressen innehåller uppgifter om teleadressen som meddelandet skickats till eller från, och det kan vara ett abonnemang, en enskild anknytning, en kod eller en adress för elektronisk post.[138] Med hjälp av brottsoffrets teleoperatör är det sedan möjligt att spåra abonnemangsuppgiften bakom teleadressen, förutsatt att gärningsmannen har samma operatör som sitt offer.[139] I de fall förövaren och angreppsobjektet har olika teleoperatörer är det betydligt svårare att spåra gärningsmannen, och därför är det vanligt att förövaren involverar flera olika teleoperatörer för att försvåra identifiering. Därutöver tillkommer

[136] Datainspektionen 2000, s. 14.
[137] Küchler, s. 9.
[138] Prop. 1994/95:227, s. 31.
[139] Küchler, s. 52.

problemet med att binda en viss person till den aktuella abonnemangsuppgiften, särskilt i miljöer där flera personer har tillträde till det aktuella abonnemanget. Att försöka spåra gärningsmannen vid ett externt dataintrång är alltså en inte helt enkel uppgift.

6.6 Straffvärdesproblematik

Studien av rättsfall visar även att det råder tveksamhet om vilka gärningar som ska anses utgöra allvarliga fall av dataintrång. Det går inte att utläsa några klara riktlinjer för hur olika gärningar ska bedömas även om det går att skönja vissa tendenser. Jag har inte lyckats hitta några uttalande i förarbetena som ger vägledning om vilket straffvärde olika gärningar ska föranleda och domskälen jag studerat ger inte heller någon klar bild. I kapitel 5 har jag undersökt om det är möjligt att klargöra hur allvarligt domstolen ser på olika sorters dataintrång och även om vissa slutsatser dragits har jag påpekat att det finns undantag där domstolarna inte verkar anse att liknande brott har liknande straffvärde. Det har framför allt uppmärksammats vid de interna dataintrång som rört slagningar i polisregister. Det är möjligt att dessa divergenser i straffvärde kan förklaras av andra omständigheter men detta framgår inte uttryckligen av domskälen och jag anser det vara angeläget att det skapas klarhet på denna punkt.

7 Ändringar till följd av Europarådskonventionen

7.1 Inledning

Europarådet har arbetat i mer än 10 år med att försöka åstadkomma en gemensam internationell lösning på problemet med IT-relaterad brottslighet, och den 11 november 2001 antogs slutligen en konvention om cyberbrottslighet[140]. Konventionen kommer att öppnas för signering den 23 november 2001, och som medlem i Europarådet planerar Sverige att underteckna konventionen inom det snaraste.[141] Problemet med IT-relaterad brottslighet anses av världssamfundet som ett viktigt och angeläget ämne, och flera stater som inte är medlemmar i Europarådet som USA, Kanada, Japan och Syd-Afrika har deltagit i utarbetandet av konventionen. Konventionen anses som ett viktigt instrument för att motverka den IT-relaterade brottsligheten, och den förväntas få stor betydelse som riktmärke för lagstiftningen inom det här området.

Nedan kommer att undersökas hur den svenska lagstiftningen förhåller sig till konventionens bestämmelser, i syfte att avgöra om några ändringar av den svenska regleringen av dataintrång blir nödvändig för att uppfylla förpliktelserna enligt traktaten. Någon officiell översättning av konventions-texten till svenska har ännu inte utarbetats och nedan anges min egen tolkning av den engelska texten. I bilaga A finns de relevanta bestämmelserna i konventionen återgivna i sin ursprungliga lydelse.

7.2 Data

I utkastet till konventionen har definitioner av vissa begrepp medtagits för att skapa klarhet och enighet om räckvidden av regleringen. I artikel 1(b) beskrivs data som ”varje representation av fakta, information eller begrepp som förekommer i en form anpassad för behandling i ett datasystem, inklusive ett program som är avsett att få ett datasystem att utföra en funktion”. Enligt ordalydelsen ska data vara ”anpassad för behandling”, vilket innebär att den ska ha en sådan form att den direkt kan behandlas av ett datasystem. Dessutom används i den engelska ursprungstexten uttrycket ”computer data” för att klargöra att regleringen avser data i informationsteknisk mening, d.v.s. data som är avsedd att bearbetas elektronisk eller på något liknande sätt.[142]

---

[140] Convention on Cybercrime, Budapest, 23.XI.2001.
[141] http://www.coe.int/T/E/Communication_and_Research/Press/Themes_Files/Cybercrime, 2001-11-09.
[142] Explanatory Report, artikel 1(b).

7.2.1 Kommentar

Huruvida denna definition kommer att leda till några tolkningsproblem är än så länge svårt att uttalas sig om. Definitionen utgår dock från den definition av data som är utarbetade av ISO vilken många länder redan använder sig av, och detta torde underlätta harmonisering av staternas lagstiftning. Den definition som använts i konventionens bestämmelse är, om än inte identisk, i alla fall mycket snarlik den definition av data som angivits i de svenska förarbetena. I båda definitionerna har tonvikten lagts vid representationen av information, och som centralt har angivits att data ska ha maskinläsbar form. I nuläget finns det inget som tyder på att den svenska definitionen av data inte skulle stämma överens med definitionen i konventionen, och någon lagändring på denna punkt torde följaktligen inte vara aktuell.

7.3 Skyddsobjekt

I definitionen av data anges som ett rekvisit för att en uppgift ska anses vara data i informationsteknisk mening att den har en sådan form att den kan behandlas i ett datasystem. Vad som avses med ett datasystem definieras närmare i artikel 1(a) i utkastet till konventionen. Där anges att med ett datasystem avses en anordning eller apparat, eller en grupp av sammankopplade sådana, där en eller flera av anordningarna med hjälp av ett program utför automatisk behandling av data. Enligt konventionens definition består ett datasystem av hårdvara och mjukvara avsett för automatisk behandling av digital data.[143] Att behandlingen ska ske automatiskt innebär att det inte behövs någon mänsklig medverkan för att detta ska ske. Med datasystem ska även avses telekomsystem och radioförbindelser, eftersom dessa system också innefattar automatisk databehandling.[144]

7.3.1 Kommentar

Skyddsobjektet i den svenska lagstiftningen är ”upptagning för automatisk databehandling”. I konventionen kriminaliseras åtgärder som innebär intrång ”i data som kan behandlas i ett datasystem” och detta torde överensstämma med den svenska lagstiftningen. Det är inte troligt att någon lagstiftningsåtgärd behöver vidtas i detta avseende, eftersom skyddsobjekten är de samma.

7.4 Brott mot åtkomsten m.m. till datasystem

I den nya konventionen återfinns bestämmelserna om intrång i datasystem i ett särskilt avsnitt kallat brott mot sekretessen, integriteten och åtkomsten

[143] Explanatory Report, artikel 1(a).
[144] Draft Convention, artikel 1(a), not 2.

till data och datasystem. Brottet kallat dataintrång regleras i en särskild bestämmelse, men det finns även förfarande i andra artiklar som täcks in av gärningsbeskrivningen i BrB 4:9c. Nedan kommer att redogöras för de artiklar i avsnittet som faller in under brottsbalkens bestämmelse om dataintrång.

7.4.1 Art 2 – Olovligt tillträde

Enligt denna artikel åläggs staterna att kriminalisera de förfarande som innebär att någon olovligen bereder sig tillgång till hela, eller en del av ett datasystem. Huvudsyftet med bestämmelsen är att täcka in de mest vanligt förekommande angreppen mot data och datasystem d.v.s. hacking och cracking. Artikeln ger staterna möjlighet att välja att enbart kriminalisera intrång som sker med ett visst syfte, t.ex. att få tillgång till viss data, eller som innebär att säkerhetsåtgärder passerats eller satts ur spel. Enligt bestämmelsen är enbart uppsåtliga gärningar straffbara. Vad som ska anses vara uppsåt bestäms enligt de nationella lagstiftningarna, dock ska eventuellt uppsåt räcka i de fall det existerar i det nationella rättssystemet.[145]

7.4.1.1 Kommentar

Regeln i konventionen motsvaras i stort av den svenska regleringen om dataintrång, BrB 4:9c. Liksom i den svenska regleringen är det tillräckligt att gärningsmannen ”berett sig tillgång” till data för att förfarandet ska anses vara olagligt. Han behöver således inte ha tillgodogjort sig innehållet för att gärningen ska vara straffbar. Bestämmelsen kriminaliserar dock enbart de gärningar som innebär att någon bereder sig tillgång till hela eller en del av ett datasystem, och den täcker inte e-post eller filer som skickas till datasystemet. Denna typ av uppgifter omfattas dock av konventionens artikel 3. Även i svensk rätt finns ett krav på uppsåt och för att en gärning ska anses straffbar räcker att ett eventuellt uppsåt föreligger. Det förfarande som anges i konventionens artikel är redan kriminaliserat enligt BrB 4:9c, och någon ytterligare reglering eller ändring av den befintliga lagstiftningen torde således inte vara aktuell.

7.4.2 Art 3 – Olovlig avlyssning

Konventionens bestämmelse ålägger staterna att införa bestämmelser som straffbelägger olovlig avlyssning av icke-offentliga överföringar av data till, från eller inom ett datasystem. Avlyssningen måste utföras med tekniska hjälpmedel, t.ex. med hjälp av elektronisk avlyssningsapparatur eller direkt via datasystemet för att förfarandet ska vara kriminaliserat. Bestämmelsen kriminaliserar också avlyssning av så kallade elektriska emissioner eller röjande signaler. Syftet är att skapa ett integritetsskydd vid

[145] Draft Convention, artikel 2 not 4.

datakommunikation som ska komplettera det skydd för den personliga integriteten som återfinns i EMRK.[146]

7.4.2.1 Kommentar

Olovlig avlyssning av data är kriminaliserat i den svenska lagen genom bestämmelserna om brytande av post- och telehemlighet, BrB 4:8 och dataintrång, BrB 4:9c. Vad avser det första ledet i artikeln täcks denna redan in av den svenska lagstiftningen och inga ändringar är nödvändiga i det avseendet. Som redan diskuterats i det föregående råder det däremot tveksamhet om huruvida röjande signaler täcks in av den befintliga lagstiftningen, och för närvarande pågår diskussioner inom Justitie-departementet för att avgöra ifall några ändringar av den svenska bestämmelsen är aktuella för att den ska stå i överensstämmelse med konventionen. Med tanke på den relativt omfattande kritik som riktats mot den svenska lagstiftningen på denna punkten anser jag att det är troligt att paragrafen kommer att ändras i detta avseende.

7.4.3 Art 4 – Dataintrång

Artikeln ålägger staterna att införa bestämmelser som gör det olagligt att skada, ändra och förstöra o.d. data. I den engelska originaltexten kriminaliseras ett flertal förfarande för att på så sätt ge ett heltäckande skydd mot olovliga intrång i data. Uttrycken ”förändra” och ”förstöra” syftar till att skydda data från alla förändringar av informationsinnehållet.[147] Gärningar som innebär att någon hindras från att ta del av data p.g.a. att den är raderad och således inte längre existerar fysiskt, eller p.g.a. att den gjorts oåtkomlig trots att gärningsmannen själv kan ta del av den är också straffbara. [148]

7.4.3.1 Kommentar

Enligt Justitiedepartementets preliminära bedömning är de förfaranden som regleras i konventionens bestämmelse om dataintrång redan straffbelagda i svensk rätt. Skadegörelse av data är förbjudet enligt BrB 12:1 och ändringar av data av såväl kvantitativ som kvalitativ karaktär är olagliga i enlighet med BrB 4:9c första meningen. [149] Som påpekats i kapitel 6.2 är det dock tveksamt om sådana förfarande som innebär att en upptagning undanhålls utan att gärningen kan betraktas som dataintrång är straffbara. Ett sådant olovligt undanhållande torde således inte omfattas av bestämmelsen.

7.4.4 Art 5 – Systemintrång

Enligt artikel 5 ska staterna kriminalisera gärningar som innebär att funktionerna hos ett datasystem hindras t.ex. genom inmatning, överföring,

[146] Explanatory Report, section 51.
[147] Explanatory Report, section 61.
[148] Draft Convention, not 11.
[149] Gustavson, s. 3-4.

förstöring eller ändring av data. Artikeln motsvarar bestämmelsen om datasabotage som återfinns i Europarådets rekommendation Nr (89) 9, och syftet är att förbjuda gärningar som hindrar ett lagenligt användande av datasystem. I den förklarande rapporten anges vidare att hindrandet måste vara allvarligt för att förfarandet ska anses vara olagligt, men det är upp till staterna själva att bestämma vad som ska krävas för att gärningen ska bedömas som ”allvarlig”. Ett exempel på sådant förfarande är massutskick av oombedd e-post, s.k. ”spamming” vilket kan leda till att kommunikationen hindras.[150] Även ”denial of sevice attacks”, vilka innebär bombardemang av information till en e-post adress, kriminaliseras enligt artikeln.[151]

7.4.4.1 Kommentar

Datasabotage anses som en straffbelagd gärning i enlighet med den svenska regleringen av skadegörelse, BrB 12:1. Vidare täcks även artikeln delvis in av bestämmelsen om dataintrång i BrB 4:9. Vad som kan vålla problem är dock de situationer som innebär att endast en funktion hindras.[152] Det är för närvarande inte kriminaliserat genom BrB 4:9, och det torde heller inte vara olagligt enligt någon annan svensk lagregel. På vilket sätt kriminalisering ska ske, eller vilken omfattning en sådan reglering ska ha lämnas dock till Sverige att bestämma.[153] Enligt den svenska bestämmelsen om dataintrång är dessutom bara införande (inputting) av upptagning i register olaglig. Övrig inputting av data är inte kriminaliserat enligt de nuvarande bestämmelserna, och en ändring av den svenska regleringen i detta avseende är således aktuell.

7.4.5 Art 6 – Illegal användning av hjälpmedel

I artikel 6 återfinns bestämmelserna om förberedelse till dataintrång och regleringen är relativt utförlig. Artikeln kriminaliserar produktion, försäljning, anskaffande, import, distribution eller annat förvärvande av ett föremål, t.ex. ett dataprogram eller ett datalösenord, i syfte att begå något brott enligt artikel 2-5. Likaså straffbeläggs innehav av sådana föremål. I artikeln tydliggörs dock att ovan nämnda förfarande inte är olagliga i de fall de sker utan något syfte att begå brott, och som exempel anges åtgärder för auktoriserad testning eller skydd av datasystem. Vid utformandet av bestämmelsen diskuterades huruvida alla föremål som kunde användas för dataintrång skulle omfattas, eller om bara de föremål som skapats exklusivt för att begå brott skulle avses.[154] I den slutliga konventionstexten valdes

[150] Explanatory Report, section 69.
[151] Explanatory Report, section 67.
[152] Gustavson, s. 4.
[153] ”The text leaves it to the Parties to determine the extent to which the functioning of the system should be hindered – partially or totally, temporarily or permanently” Explanatory Report, section 69.
[154] Explanatory Report, section 73.

ingen av de två föreslagna alternativen utan istället lades den avgörande betydelsen vid *syftet* med anskaffandet, produktionen etc.

7.4.5.1 Kommentar

I Sverige är försök och förberedelse till dataintrång kriminaliserat genom BrB 4:10 och BrB 23:2 och enligt den preliminära bedömning som Justitiedepartementet gjorde täcker den svenska bestämmelsen endast delvis in de förfarande som anges i artikel 6.[155] Kritiken riktades främst mot att den svenska uppräkningen av hjälpmedel inte omfattade sådana IT-objekt som dataprogram eller lösenord som anges i ordalydelsen i konventionen. Efter att denna bedömning gjordes har dock den svenska regleringen ändrats bl.a. i detta avseende och den svenska paragrafens nya ordalydelse torde inte stå i konflikt med konventionens artikel.

7.5 Analys

En genomgång av konventionens artiklar visar att vissa ändringar av den svenska lagstiftningen kommer att behöva vidtas. Några av de punkter där det råder inkongruens mellan BrB 4:9c och konventionen rör sådana brister eller tveksamheter i den svenska lagregeln som redan påpekats i kapitel 6. Som exempel kan nämnas röjande signaler. Detta fenomen har diskuterats relativt flitigt i förarbeten och doktrin och det finns omfattande utredningar och förslag på hur detta ska åtgärdas. Andra problem som t.ex. införande av data på andra ställen än i register har tidigare inte uppmärksammats av kritikerna utan ett nytt diskussionsområde har öppnats. För närvarande arbetar Justitiedepartementet med att undersöka vilka ändringar som kan bli aktuella och hur de i så fall ska ske. Min personliga åsikt är att den svenska lagstiftningen bör ändras på de punkter där brister påpekats ovan.

[155] Se Gustavson, s. 4.

8 Åtgärdsförslag

8.1 Inledning

Den nuvarande regleringen av dataintrång har sitt ursprung i början av 70-talet och bestämmelsen är således nära 30 år gammal. Under denna tidsperiod har den tekniska utvecklingen tagit fart och användningen av Internet och datorer har ökat explosionsartat. I takt med denna tekniska utveckling har även nya möjligheter till att begå brott öppnat sig, och medan tekniken förfinats och anpassat sig är lagbestämmelsen om dataintrång i princip sig lik. Den undersökning av lagregelns utsträckning och omfattning, samt studien av praxis och statistik som jag företagit visar dock att den nuvarande regleringen av dataintrång inte är helt utan brister. Det finns en rad förfarande som helt faller utanför paragrafens tillämpningsområde, och andra gärningar där det råder tveksamhet om huruvida de ska anses omfattas av bestämmelsen. Dessutom tillkommer svårigheter med att spåra och identifiera gärningsmännen samt att fastställa gärningarnas straffvärde. I det följande kommer jag att redogöra för de lagändringar och övriga åtgärder som jag anser vara nödvändiga för att på ett mer effektiv sätt förhindra och motverka problemet med dataintrång.

8.2 Ändring av lagstiftningen

Den gällande lagstiftningen om dataintrång har trots den allmänt hållna formuleringen vissa luckor, och enligt min mening kan den inte anses vara ett helt effektivt verktyg för att motverka och förhindra dataintrång. Det jag anser vara den största bristen är att s.k. röjande signaler faller utanför lagens tillämpningsområde och detta bör åtgärdas. Enligt min uppfattning verkar det inte råda någon oenighet om huruvida intrång i röjande signaler ska anses som en straffbar gärning eller inte. Istället tycks det vara tveksamt ifall en ändring av lagen verkligen är nödvändig, eller om röjande signaler redan omfattas. Detta verkar vara ett reellt och överhängande problem som uppmärksammats från flera håll, och med anledning av detta anser jag att lagstiftningen bör anpassas så att även dessa omfattas för att undanröja oklarheter. Dessutom är det en av de punkter där den svenska bestämmelsen inte är harmoniserad med Europarådets konvention om cyberbrottslighet, utan där det som påpekats i det föregående är nödvändigt med en lagändring. Genom ett tillägg bör således införas ansvar för ”den som olovligen med tekniska hjälpmedel tar del av eller upptar uppgifter i form av signaler som oavsiktligt spridits på trådlös väg”[156].

Därutöver är det, som jag påpekat i kapitel 7, troligt att vissa ytterligare ändringar är nödvändiga för att den svenska regleringen ska uppfylla kraven

[156] SOU 1992:110, s. 191.

i Europarådets konvention om cyberbrottslighet. Detta gäller t.ex. förfarande som innebär att en upptagning undanhålls utan att gärningen kan betraktas som dataintrång, men också situationer där endast en funktion hindras. En annan gärning som troligen heller inte omfattas och där en lagändring således torde vara aktuell är inputting av data på något annat ställer än i ett register. Några förslag på hur en kriminalisering av dessa förfarande skulle se ut har jag dock inte lyckats hitta och kan därför inte presentera något utkast till hur en ändring skulle formuleras.

Dessutom har diskussioner förts om huruvida skyddssubjektet bör ändras och det mest konkreta förslag, vilket presenterades av DSU, har redovisats i det föregående. Kritik har riktats mot fokuseringen på begreppet data eftersom det anses vara ett alltför vidsträckt begrepp och istället ska det centrala begreppet vara information. Min åsikt är dock att även det senare begreppet är väldigt omfattande och kan ge upphov till tvetydigheter. Information anses utgöra innebörden av data och information måste således ha en mening. Att använda sig av det nya begreppet kan eventuellt tänkas ge upphov till nya problem i fall den som bereder sig tillgång till uppgifter inte förstår innehållet, eftersom det då kan ifrågasättas om han verkligen lyckats bereda sig tillgång till informationen. Motiveringen för att byta ut ordet data har just varit att ett nytt begrepp skulle skapa klarhet, men enligt min mening kan ordet information ge upphov till minst lika mycket tolkningsproblem som det nuvarande begreppet. Därför anser jag att en lagändring på denna punkt inte bör vidtas.

8.3 Avgränsning av det straffbara området

Ett annat stort problem som jag uppmärksammat under min studie av den gällande lagstiftningen är att det i vissa fall uppstår gränsdragningsproblem. Det har visat sig att det avseende vissa gärningar kan vara svårt att avgöra huruvida de utgör straffbara dataintrång eller inte, och jag anser det vara angeläget att det klargörs hur långt det straffbara området sträcker sig. Detta gäller framför allt vid interna dataintrång inom sjukvården och förhoppningsvis kommer hovrättens avgörande av *Blomberg-journalen* att ge viss vägledning till hur detta problem ska bedömas. Även domstolens avgörande i *Försäkringskassan* kan tänkas bringa klarhet i tveksamma frågor kring detta gränsdragningsproblem. Dessutom beräknas Integritets-utredningen att redovisa sin utredning om skyddet av personlig integritet vid användning av e-post i arbetet vid årsskiftet 2001/2002, och troligtvis kommer deras betänkande att ytterligare förtydliga hur långt det straffbara området sträcker sig.

8.4 Preventiva åtgärder

Enligt min mening är det troligt att vissa andra åtgärder kan behöva vidtas för att problemet med dataintrång ska kunna bekämpas på ett mer effektivt

sätt. I BRÅ:s enkätsvar framkom att det som upplevs som ett av de största problemen vid bekämpningen av dataintrång är rättsväsendets bristande förmåga att utreda och lagföra IT-relaterad brottslighet. Framför allt företrädarna för näringslivet är av åsikten att andra åtgärder än en reformering av BrB 4:9c är nödvändig för att komma till rätta med problemet.

De insatser som kan bli aktuella är av varierande slag, och användare av datorer kan själva försöka att så långt möjligt försvåra dataintrång genom att vidta vissa åtgärder. Externa dataintrång kan förhindras, eller i vart fall försvåras genom att användaren installerar en s.k. brandvägg. Dessutom kan risken för dataintrång reduceras genom att begränsa installation och öppnande av program och tjänster till sådana som verkligen är nödvändiga. För att ytterliggare minimera riskerna är det angeläget att se till att programvaror och tjänster endast köps i originalskick och av välrenommerade återförsäljare. En annan åtgärd som kan vidtas för att förhindra såväl interna som externa dataintrång är att införa system med behörigheter och lösenord. För att öka effekten av dessa bör rutiner inrättas för att skydda dem, t.ex. genom kryptering, och för att byta ut dem frekvent. Skadegörande dataintrång, cracking, kan förhindras genom motåtgärder som väl installerade operativsystem och serverprogram.[157]

8.5 Åtgärder för att spåra och identifiera gärningsmannen

Även om preventiva åtgärder vidtas kvarstår problemet med att spåra och lagföra gärningsmännen om ett dataintrång trots allt lyckas genomföras. System med behörigheter och användaridentiteter kommer inte enbart att ha en preventiv effekt, utan de kommer även att spela en betydelsefull roll för att underlätta identifieringen av gärningsmän. Stora brister i hantering av behörigheter och användaridentiteter har framför allt uppmärksammats inom vården, och då studien av statistik och praxis har visat att dataintrång är ett vanligt förekommande fenomen där är det angeläget att rutinerna omedelbart ändras. Datainspektionen gav i sin årsredovisning för år 2000 exempel på vilka regler som bör gälla vid hantering av personuppgifter.[158] Visserligen gäller Datainspektionens förslag på åtgärder enbart hanteringen av personuppgifter skyddade i PuL, men dessa regler torde kunna vara till vägledning även vid upprättande av rutiner för hantering av andra datauppgifter. Såväl myndigheter som företag kan genom att vidta liknande åtgärder underlätta upptäckten och identifieringen av gärningsmannen vid dataintrång.

Som förslag på åtgärder som bör vidtas anges att behörigheten till datasystem bör begränsas till de personer som verkligen behöver ta del av

[157] PTS, bilaga 4, s. 12.
[158] Datainspektionen 2000, s. 14.

uppgifterna för att utföra sitt arbete. Dessutom ska ett system för behörighetskontroll installeras vid de situationer där datorn används av mer än en person. Användaridentiteter bör göras personliga och det ska inte vara tillåtet att överlåta dem till någon annan. Ytterligare åtgärder, som bör vidtas för att underlätta spårningen av gärningsmannen om datorn används av mer än en person, är installation av ett loggsystem. Med hjälp av en maskinell logg kan åtkomsten av viss information spåras, och det går bl.a. att se vem som har haft åtkomst, vilka uppgifter åtkomsten har avsett, och när den har skett. Trots att det kan tänkas vara möjligt att inrättande av liknande regler inte helt och hållet kan förhindra dataintrång skulle det troligtvis bli svårare både att bereda sig tillgång till uppgifterna och att undgå upptäckt.

En ytterligare åtgärd som kan vidtas är att inrätta en särskild enhet för hantering av IT-incidenter. I november 1999 gav regeringen i uppdrag åt PTS att utreda förutsättningarna för att inrätta en särskild funktion för IT-incidenthantering och rapporten avlämnades i december 2000.[159]

I rapporten framkom att en särskild funktion för IT-incidenthantering bör inrättas. Huvuduppgiften ska vara att motverka angrepp på informations- och kommunikationstekniska system och infrastrukturer inom den statliga sektorn, men den ska även kunna samverka med enskilda organisationer.[160] Detta mål ska bl.a. uppnås genom att förmedla varningar, råd och annan information till myndigheter, företag, privatpersoner och organisationer runt om i Sverige. Dessutom ska funktionen anordna utbildningar i IT-incidenthantering och svara för hotbilds- och riskanalys, och dataintrång anges som en av de kategorier av incidenter som särskilt bör beaktas. För att underlätta sammanställningen av hotbilds- och riskanalysen ska myndigheterna skicka in rapporter om incidenterna till funktionen. Det är ännu inte bestämt om myndigheterna ska åläggas en rapporteringsplikt, eller om det ska ske på en frivillig basis. Vidare betonas vikten av att ett bra samarbete mellan polisen och funktionen, respektive myndigheterna upprättas.[161] PTS anser att polisen bör medverka i funktionen och det bör även undersökas om polisiära uppgifter och befogenheter bör tilldelas funktionen.

8.6 En grov brottsrubricering

Som nämnts i föregående avsnitt har kritik riktats mot den befintliga lagstiftningen om dataintrång och denna har framför allt avsett bestämmelsens ordalydelse, men även riktat sig mot bestämmelsens straffsats. Vissa kritiker har ansett att den befintliga lagstiftningen inte är tillräcklig för att bestraffa vissa typer av dataintrång, och därför har ett krav på en grov brottsrubricering framförts. Ett förslag är att införa en bestämmelse om grovt dataintrång som tar sikte på tillvägagångssättet, och

[159] PTS, s. 5.
[160] PTS, s. 87.
[161] PTS, s. 88.

som avgörande rekvisitet har angivits att intrånget kan anses vara kvalificerat, systematiskt och samordnat.[162] En ytterligare försvårande omständighet som kan tas i beaktande vid avgörandet av om brottet ska anses som grovt är om dataintrånget har inneburit en kränkning av den personliga integriteten. Någon uppgift om vilken straffsats som bestämmelsen bör innehålla har inte lämnats, men med tanke på det resonemang som domstolen förde i t.ex. *Larmoperatören* är det troligt att anta att det föreligger en presumtion om fängelse vid dylika brott. Ett ytterligare problem med den befintliga lagstiftningen är att tvångsmedlet hemlig teleövervakning (RB 27:19) inte är tillåtet p.g.a. brottets straffskala, och användning av institutet husrannsakan (RB 28:1) hos tele- och Internetoperatörer har kritiserats av JO.[163] Om en grov brottsrubricering med en strängare straffskala införs skulle detta tvångsmedel kunna användas i större utsträckning.

[162] Küchler, SvD 2001-08-10.
[163] PTS, s. 90.

9 Avslutande analys

Utgångspunkten vid kriminalisering av olagliga förfarande som uppkommer till följd av utvecklingen på IT-området har varit att så långt möjligt täcka in dessa gärningar med redan befintlig lagstiftning. I de fall som detta inte har varit möjligt har nya lagregler stiftats för att täcka in dessa luckor, och för att åstadkomma en enhetlig reglering har paralleller dragits till redan befintlig reglering då nya paragrafer har utformats. Den svenska lagregeln om dataintrång var från början tänkt att subsidiärt täcka in de brottsliga förfarande som inte föll in under någon av de övriga bestämmelserna som återfanns i brottsbalken. Detta kan förklara bestämmelsens ganska allmänt hållna formulering. Lagregeln kriminaliserar gärningar som innebär att någon bereder sig tillgång till uppgifter och relativt många handlingar faller in under denna bestämmelse. Den typ av gärningar som lagstiftningen främst var avsedd att skydda var troligtvis sådana som innebar interna intrång i dataregister liknande de som återfinns i *Blomberg-journalen*, *Larmoperatören, Polisfall 1* och *Polisfall 2*. Andra troliga brottssituationer som lagstiftaren hade i åtanke var externa dataintrång bestående av att någon utomstående bröt sig in i på en arbetsplats och där tog sig in i register de ej hade behörighet till. Exempel på sådana förfarande har jag dock inte hittat i rättspraxis.

I takt med den tekniska utvecklingen har dock nya förfaranden dykt upp som också de innebär ett olovligt intrång i datauppgifter. De brottsliga gärningarna i *Nasa-hackers*, *Spray-målet* och *Aftonbladet* var troligtvis inte vad lagstiftaren hade i åtanke då den befintliga lagstiftningen utarbetades, men likväl faller dessa gärningar in under bestämmelsens tillämpningsområde. Detta beror säkert delvis på den allmänt hållna formuleringen samt det vida skyddsområdet. Om bestämmelsen hade begränsats till att enbart skydda integritetskänsliga uppgifter hade antagligen många av de gärningar som idag är föremål för åtal fallit utanför den befintliga regleringen.

Såväl studien av statistik som praxis visar att dataintrång är ett stort och högst aktuellt problem för såväl privatpersoner som företag och myndigheter. Ingen går fri från angreppsrisk utan all information som finns lagrad i dataform utgör ett potentiella angreppsobjekt. Enligt min åsikt är lagstiftningen i det stora hela ett effektivt verktyg i bekämpningen av dataintrång. Visserligen kommer en del ändringar troligen att bli nödvändiga för att uppfylla de internationella åtagandena med anledning av Europarådets konvention om cyberbrottslighet. Min undersökning visar också att den befintliga lagstiftningen har vissa luckor t.ex. röjande signaler. Huruvida detta utgör ett stort problem och vanligt förekommande fenomen i praktiken har jag dock inte lyckats bringa klarhet i. Därför är det svårt att avgöra om en ändring av lagstiftningen för att inkludera denna typ av brottslighet skulle få någon märkbar effekt.

Bland de övriga problem kring lagstiftningen som farmhållits anges bl.a. gränsdragningsproblem för när en gärning ska anses som dataintrång. Ett sådant tveksamt fall har avser arbetsgivares rätt att ta del av anställdas e-post, och även om inget liknande fall har blivit föremål för domstolsprövning är problemet omdiskuterat i litteraturen. Att det finns ett behov för klarare och tydligare instruktioner om vilka gärningar som ska anses som dataintrång är även *Blomberg-journalen* ett bra exempel på. Både uttalande i rättsfallet och i andra sammanhang visar att det råder osäkerhet om vilka gärningar som ska klassificeras som dataintrång, och detta problemet figurerar främst inom vården även om det förekommer på andra arbetsplatser som t.ex. försäkringskassan och polisen. Denna gränsdragningsproblematik verkar således enbart förekomma vid interna dataintrång, men problemet återfinns både inom den offentliga och privata sektorn.

Även om det således finns ett behov av att klargöra det straffbar området verkar det problem som finns i dagsläget med att ett stort antal dataintrång inte straffbeläggs inte bero på att gärningarna faller utanför den befintliga lagstiftningen, utan snarare på att brotten aldrig upptäcks eller anmäls. Därtill kommer svårigheten med att identifiera förövaren och bevisa vem som utfört gärningen. Min åsikt är således att det är här som de övriga resurserna bör sättas in.

En möjlig åtgärd är att inrätta en särskild funktion för att hantera IT-incidenter såsom PTS föreslagit. Genom att tilldela en särskild enhet huvudansvaret för IT-relaterad brottslighet samlas information och kunskap om denna typ av brott på ett och samma ställe. Ett av de främsta argumenten som företagen presenterat för att motivera underlåtenheten att anmäla dataintrång har just varit att polisen saknar kompetens att utreda den ifrågavarande brottsligheten. Detta argument borde förlora sin bärkraftighet om en särskild funktion med den specifika kunskapen ges befogenhet att utreda brottsligheten. En ytterligare fördel uppnås genom att funktionen som således tillsänds rapporter om incidenter också görs huvudansvarig för information om denna typ av brottslighet. Visserligen ska funktionen enbart ta emot rapporter från statliga sektorn, men information och råd ska även spridas till företag och privatpersoner.

Dessutom anser jag att resurserna bör inriktas på att vidta effektiva åtgärder för att preventivt förhindra dataintrång. Min studie av praxis och statistik har bl.a. visat att interna dataintrång är ett vanligt förekommande problem inom den offentliga sektorn, och ett sätt att preventivt förhindra dylika brott är genom att förbättra rutinerna för behörighet och användaridentiteter. Diskussionen kring behörighetssystem har framför allt koncentrerats till sjukhus och andra offentligrättsliga arbeten, men rutinerna torde även har relevans för andra arbetsplatser. Med hjälp av liknande system kan antalet personer som har behörighet att ta del av upptagningar drastiskt begränsas.

Dessutom förenklas spårningen och identifieringen av gärningsmannen avsevärt.

Preventiva åtgärder kommer troligtvis att få mindre effekt vid bekämpningen av externa dataintrång. Visserligen kan s.k. brandväggar erbjuda ett visst skydd, men för en duktig hacker eller cracker utgör de inget större hot. Självklart bör de preventiva åtgärder som står till buds vidtas, men vid externa dataintrång kommer troligtvis rutiner för att spåra och identifiera gärningsmannen att bli allt mer viktiga i kampen mot dataintrång. Här är det dock nödvändigt att göra en avvägning mellan intresset för att kunna döma och lagföra brottslingar mot skyddet för den personliga integriteten. Att behörighetskontroller och andra rutiner för identifiering inrättas på arbetsplatser anser jag inte innebära något större ingrepp i den personliga integriteten. En anställd är bunden att följa arbetsgivarens instruktioner, och att ta hjälp av liknande rutiner för att se till att dessa åtföljs anser jag inte vara oproportionerligt. En diskussion kan dock föras kring i vilken omfattning det ska vara möjligt att spåra privatpersoners förehavande på Internet.

Ett ytterligare problem med den nuvarande lagregeln verkar enligt min mening vara att det råder en osäkerhet om vilket straff som ska utdömas för olika sorters dataintrång. Vissa trender går att utröna, men studien av praxis ger ingen klar vägledning och för att bringa klarhet bör en grov brottsrubricering införas. Genom att ange uttryckligen i lagstiftningen vilka faktorer som bör tas med i bedömningen av om ett brott skall anses vara grovt skapas en större rättssäkerhet. Dessutom får domstolarna klarare direktiv om hur olika typer av dataintrång skall bedömas, vilket underlättar vid fastställandet av brottets straffvärde. En studie av den rättspraxis som redovisats i det föregående visar på att sådana riktlinjer skulle vara betydelsefulla för att skapa klarhet i hur olika typer av dataintrång ska bedömas. Kränkning av den personliga integriteten är en av de omständigheter som har angivits som försvårande, och detta verkar till viss del ligga i linje med domstolens bedömning, t.ex. i *Larmoperatören*. Det verkar dock inte som att domstolarna har sett allvarligt på brottet i samtliga fall där en sådan kränkning har skett, som t.ex. *Blomberg-journalen,* och därför är det extra viktigt att klarhet skapas.

En ytterligare effekt av att ett dataintrång kan klassificeras som ett grovt brott är att det kan resultera i ett strängare straff än vad som kan utdömas enligt BrB 4:9c och detta kommer troligtvis ha en preventiv effekt genom avskräckning. Flertalet s.k. ”nyfikenhetsbrott”, vilka ofta resulterar i en kränkning av den personliga integriteten skulle troligtvis förhindras om gärningsmännen riskerade fängelsestraff. Denna typ av brott förekommer framför allt inom vården och polisen, och antalet interna dataintrång liknande *Polisfall 1, Polisfall 2* och *Blomberg-journalen* skulle antagligen reduceras. Kränkning av den personliga integriteten är inte lika vanligt förekommande vid externa dataintrång, och den brottshämmande effekten av en grov brottsrubricering torde antagligen bli mindre. Som nämnts ovan

är det föga troligt att en skärpning av straffskalan skulle ha en avskräckande effekt på de unga gärningsmän som enligt praxis och statistik begår den typen av dataintrång. Tonvikten vid bekämpningen av den typen av brottslighet kommer troligtvis att i framtiden få läggas på andra preventiva åtgärder.

Avslutningsvis kan konstaterat att problemet med dataintrång är väldigt komplext och det verkar inte finnas någon enkel lösning för att motverka brottsligheten. Trenden pekar mot att antalet brottsliga gärningar stadigt ökar, och i takt med den tekniska utvecklingen förfinas och anpassas också gärningarna. Ökningen kan anses ha sin förklaring i en kombination av dålig säkerhet och skickliga aktörer, och med tanke på den ständigt eskalerande användningen av datorer och Internet är det angeläget att nödvändiga åtgärder vidtas. Att komma åt de skickliga aktörerna får närmast anses åligga lagstiftarna medan bristerna i säkerheten är ett problem som företagen får ta itu med. Min undersökning har således visat att den nuvarande regleringen är i behov av vissa ändringar samt att den bör kompletteras med vissa ytterligare åtgärder för att problemet med dataintrång ska kunna bekämpas på ett mer effektivt sätt. Den tekniska utvecklingen verkar hela tiden ligga steget före lagstiftningen och i samma stund som ytterligare gärningar kriminaliseras konstrueras nya brottsliga handlingar som faller utanför.

Bilaga A

Convention on Cybercrime

Chapter I – Use of terms

Article 1 – Definitions
For the purposes of this Convention:

a. "computer system" means any device or a group of inter-connected 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;

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 Article 2 – 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 - 5; and

   b. the possession of an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 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) (2).

Brottsbalk (1962:700)

4 kap. Om brott mot frihet och frid

10 § För försök, förberedelse eller stämpling till människorov, 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 (1998:206).

Litteraturförteckning

Offentligt tryck

Direktiv

Direktiv 1999:73 *Den personliga integriteten i arbetslivet*

Lagar

SFS 1973:289 Datalag

SFS 1985:562 Patientjournallag

SFS 1996:844 Radio- och TV-lag

SFS 1998:204 Personuppgiftslag

Propositioner

Prop. 1973:33 *Förslag till ändring i tryckfrihetsförordningen m.m.*

Prop. 1985/86:65 *med förslag till ändringar i brottsbalken m.m. (vissa frågor om datorrelaterade brott och ocker)*

Prop. 1993/94:130 *Ändringar i brottsbalken m.m.*

Prop. 1994/95:227 *Hemlig teleavlyssning och hemlig teleövervakning*

Prop. 1997/98:44 *Personuppgiftslag*

Prop. 2000/2001:85 *Förberedelse till brott m.m.*

Offentliga utredningar

SOU 1972:47 *Data och integritet*, Offentlighets- och sekretesslagstiftningskommittén

SOU 1983:50 *Översyn av lagstiftningen om förmögenhetsbrott utom gäldenärsbrott*, Förmögenhetsbrottsutredningen

SOU 1990:61 *Skärpt tillsyn – huvuddrag i en reformerad datalag*, Datalagsutredningen

SOU 1992:110 *Information och den nya InformationsTeknologin – straff- och processrättsliga frågor m m*, Datastraffrättsutredningen

SOU 1996:40 *Elektronisk dokumenthantering*, IT-utredningen

SOU 1997:39 *Integritet Offentlighet Informationsteknik*, Datalagskommittén

DS 1990:45 *ADB och samhällets säkerhet på 90-talet*, Civildepartementet

Europarrådet
Europarrådets rekommendation (Nr. R (89) 9)

Convention on Cyber-Crime (ETS no. 185), Budapest, 23.XI.2001. [cit. Convention on Cyber-crime]

Draft Convention on Cyber-crime (Draft N° 25 REV.5). [cit. Draft Convention]

The Explanatory Report (adopted on 8 November 2001)

Litteratur

Barrett, Neil *Digital crime*, London 1997.

Boni, William
Kovacich, Gerald *I-way robbery*, Oxford 1999.

Casey, Eoghan *Digital evidence and computer crime*, San Diego, Calif 2000.

Freese, Jan *Kommentar till datalagen*, Stockholm 1983.

Holmqvist, Lena m.fl. *Brottsbalken – en kommentar* (Del 1), 2:a upplagan Studentutgåva, Stockholm 2000.

Küchler, Markus *Dataintrång – Om personlig integritet och bevisfrågor*, Stockholm 2000. [cit. Küchler]

Seipel, Peter *Juristen och datorn*, Fritze, Stockholm 1994.

Silvander, Jan *Dator- datarelaterade förmögenhetsbrott utom borgenärsbrott*, Lund 1998.

Övrigt tryck

Almblad, Jörgen *Straffrätt och informationsteknik – en*

Brorsson, Joel — *grundläggande inventering av lagstiftningsbehovet*, PM 1998-03-17, Justitiedepartementet.

BRÅ — *IT-relaterad brottslighet 2000:2*, Stockholm, 2000.

Datainspektionen — *Skyddade uppgifter i folkbokföringen*, rapport 1999:3. [cit. Datainspektionen, rapport 1999:3]

Datainspektionen — *Årsredovisning 2000*. [cit. Datainspektionen 2000]

Gustavson, Lena — *Europarådskonventionen om Crime in Cyberspace*, Arbetspapper 2001-05-30, Justitiedepartementet.

IT-rättsliga observatoriet — *E-post på arbetsplatsen*, PM 5:1999. [cit. IT-rättsliga observatoriet, PM 5:1999]

IT-rättsliga observatoriet — *Observatoriets syn på vissa straff- och processrättsliga lagstiftningsfrågor*, PM 3:1999. [cit. IT-rättsliga observatoriet, PM 3:1999]

PTS — *Förutsättningar för att inrätta en särskild funktion för IT-incidenthantering*, Diarienummer 99-19448.

RRV — *Datorrelaterade missbruk och brott – en kartläggning gjord av Effektivitetsrevisionen*. RRV 1997:33.

Artiklar

Andersson, Helena — *Fyra domar angående brottet dataintrång*, Lov & Data nr 57 1999.

Byttner, Karl-Johan — *CF och Saf oeniga om e-postkontroll*, Computer Sweden nr 121 1999, (publicerat på Internet 1999-12-13). [cit. Byttner, Computer Sweden nr 121 1999]

Byttner, Karl-Johan — *E-post hett mål vid dataintrång*, Computer Sweden nr 18 2000, (publicerat på Internet 2000-02-18). [cit. Byttner, Computer Sweden nr 18 2000]

Byttner, Karl-Johan	*LO-rapport ifrågasätter företags rätt till e-postkoll*, Computer Sweden nr 99 2000, (publicerat på Internet 2000-10-19). [cit. Byttner, Computer Sweden nr 99 2000]
Datainspektionen	*Tjänstemän läckte uppgifter till nazister*, Direkt nr 4/2000. [cit. Datainspektionen, Direkt nr 4/2000]
Gilså, Tomas	*Två kvinnor åtalas för dataintrång*, IDG 2001-06-20.
Harne, Andreas	*Nazister kartlade kända svenskar*, Aftonbladet 2001-11-09.
Jansson, Torsten	*Studenter får böta för dataintrång*, Aftonbladet 2001-11-17.
Johansson, Lars	*Åtalade kvinnan förnekar brott*, DN 2001-11-09.
Küchler, Markus	*Samordna Säpo och Rikskrim*, SvD 2001-08-10. [cit. Küchler, SvD 2001-08-10]
Lindstedt, Tommy	*Dataintrång har blivit en affärsidé*, Sydsvenskan 2000-11-05.
Sandberg, Peter	*Kända nazister beställare*, DN 2001-11-08.
Svidén, Henrik	*Svenska Nasahackare fick villkorligt*, Computer Sweden, (publicerat på Internet 2000-02-29).
Söderman, Krister	*Mer spaning på nätet*, Svensk polis nr 2/2000.
TT	*Hemdatorer utsätts för dataintrång*, Sydsvenskan, 2001-11-09.
TT	*Microsoft erkänner angrepp på hackare*, Sydsvenskan 2001-01-26.

Elektroniska källor

http://www.coe.int/T/E/Communication_and_Research/Press/Themes_Files/Cybercrime, 2001-11-09.

Rättsfallsförteckning

Arbetsdomstolen
AD 1996 nr 23.

Hovrätten
RH 1996:133.
RH 2000:90.
Svea hovrätt, B 296/95

Tingsrätten
Falu tingsrätt; B 793-01.
Gävle tingsrätt; B 12-97.
Göteborgs tingsrätt; B 11913-99.
Göteborgs tingsrätt; B 8608-00.
Lunds tingsrätt; B 1914-97.
Stockholms tingsrätt; T 8-624-96.