Juridiska institutionen
LUNDS UNIVERSITET

Vt - 1998

Internetrelaterade missbruk och brott

Examensarbete i straffrätt 20 poäng

Handledare

Prof. Per- Ole Träskman

Författare

Johan Kern

Innehållsförteckning

1 Inledning

Informationsteknologin i Sverige håller på att skapa ett genomdatoriserat samhälle. Detta får i högsta grad konsekvenser också när det gäller brott och brottsbekämpning. Ekonomiska transanktioner och informationshantering i övrigt sker i allt större utsträckning via datorer, genom nätverk, elektroniska betalningsmedel, datoriserad bokföring, e- post och kommersiella transanktioner.

Den nya IT tekniken har skapat förutsättningar för allt snabbare och effektivare transaktioner och kommunikationer av olika slag. Men med den snabba IT utvecklingen skapas också helt nya sätt att i brottsligt syfte ta del av konfidentiell information, manipulera penningtransaktioner och förändra eller förstöra lagrad information. Datatekniken kan även användas som hjälpmedel vid brott och möjliggör snabba, globala och framförallt anonyma kommunikationer. Den nya tekniken ställer också i viss mån lagstiftningen på huvudet och Datalagen är numera långt ifrån heltäckande. Trots detta kan Sverige ses som något av pionjärer på området eftersom den svenska Datalagen var en av de första i sitt slag i världen.

Traditionella rättsliga begrepp och regler passar inte alltid in i den nya IT miljön och kan ibland leda till osäkerhet ifråga om reglernas tillämpning. I många fall är den tekniska kompetensen hos näringsidkare, poliser och andra inblandade helt otillräcklig för att klara av situationen. Sverige ligger mycket långt fram när det gäller att anpassa samhället efter informationsteknologin och användningen av persondatorer i hemmen är hög.

Hitintills har vi i Sverige varit relativt förskonade från IT och databrottslighet men utvecklingen hänger nära samman med hur långt datoriseringen i samhället i övrigt har gått. Med bakgrund av detta kan man

förvänta sig att IT brottsligheten och databrottsligheten i framtiden kommer att bli ett allt större problem för näringsliv, polis och rättsväsende.

1.1 Syfte

Mitt syfte med detta arbete är att ge en heltäckande bild av de frågeställningar och problem som i framtiden kommer att bli allt vanligare vad gäller Internet och IT relaterad brottslighet.

1.2 Internet

1969 grundade det amerikanska försvarsdepartementet ett nätverk ARPANET.[1] Syftet med detta var att försvarets datorer skulle sammankopplas så att de kunde kommunicera med varandra oberoende av sin geografiska placering. Om en enskild datacentral slogs ut i ett eventuellt krig eller vid ett sabotage skulle informationen inte gå förlorad och de övriga datorerna skulle trots detta fortfarande kunna utbyta information via nätet. ARPANET utvecklades och utvidgades under 1970-talet och bytte 1983 namn till Internet, då nätet delades upp i två administrativa delar. Den militära delen kallades MILNET och den delen av Internet som användes av akademiker behöll namnet ARPANET fram till 1990 då namnet ändrades till NSFNET.[2]

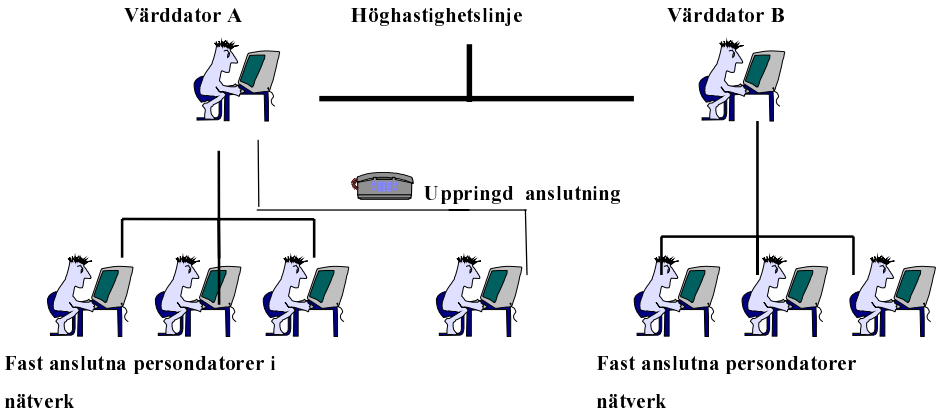
Internet består av ett otal större och mindre lokala nätverk som sammankopplats över nationsgränserna. Dessa lokala nätverk som är anslutna till Internet består av en värddator samt ett visst antal persondatorer. För att få ett nätverk anslutet till Internet krävs dels en fysisk anslutning och dels en användaridentitet. De datorer som är anslutna till nätverket kommunicerar med varandra genom TCP/IP som är

[1] Advanced Research Agency NETwork
[2] Mats Dämvik, IRI rapport 1993:2, s. 18.

kommunikationsstandard.[3] Anslutning till Internet kan ske på två olika sätt antingen genom en uppringd eller genom en fast anslutning. Med en uppringd anslutning menas att man kommunicerar med värddatorn via det allmänna telefon nätet med hjälp av ett modem. Med fast anslutning menas att man alltid är uppkopplad mot sin värddator och således också mot Internet.[4] Internet är uppdelat i domäner som består av ett eller flera nätverk. För att kunna ta emot och skicka data till domäner måste man känna till domänens speciella adress. De vanligaste adresserna är de s k URL och e-post adresserna.[5] E- post adresserna används för att skicka och ta emot e-post meddelanden. Varje person som skall koppla upp sig gentemot Internet får ett Internetkonto av den nätverksadministratör som tillhandahåller anslutningen till Internet. Kontot innefattar en användaridentitet och ett lösenord samt vanligtvis en e- post adress. Det går att ansluta sig till Internet utan att ha ett Internetkonto men man blir då tvungen att logga in som anonym användare eller som gäst vilket medför att man endast får tillgång till en begränsad del av Internet.

[3] TCP/IP (Transmission Control Protocol/Internet Protocol) är namnet på det språk som används för kommunikation på Internet. TCP/IP är det gemensamma namnet för ett flertal skilda men samarbetande protokoll som används för kommunikationen på Internet.
[4] Juridicum är uppkopplat med en fast anslutning mot Internet
[5] URL – adresser används för att kunna koppla upp sig gentemot en värddator i en annan domän.

1.3 En möjlig domän på Internet[6]



World Wide Web eller WWW är den snabbast växande delen av Internet och man beräknar att det idag finns ca 100 miljoner webbdokument över hela världen. WWW utvecklades ursprungligen i syfte att skapa ett sammanlänkat och enhetligt nätverk för hypertextbaserad information.[7] WWW dokumenten skapas och skrivs i programmeringsspråket HTML.[8] En hemsida består av HTML dokument som finns lagrade på en värddator och för överföring av information via WWW används ett program som kallas HTTP.[9] Idag når Internet ett stort antal länder och datorer över hela världen och man räknar med att det finns ca 17 miljoner värddatorer i sammanlagt ca 900 000 nätverk. Antalet värddatorer är relativt enkelt att uppskatta eftersom varje dator motsvarar en s k IP - adress.[10] I Sverige beräknar man att det finns ca 250 000 registrerade värddatorer. Mycket svårare än att

[6] Skissen är hämtad från en artikel av Jonas Ledendal i tidsskriften ”Dissidenten”, mars 1995, s. 12 Tidsskriften utges av Juridiska Föreningen i Lund.
[7] World Wide Webb är en samlingsbetäckning på resurser (datorer, program och dokument) på Internet som använder protokollet HTTP.
[8] HTML (HyperText Markup Languages) är ett sidbeskrivningsspråk som används för att skapa WWW- dokument.
[9] HTTP (HyperText Transfer Protocol) är ett kommunikations protokoll som används för överföring av WWW- dokument.
[10] En IP- adress (Internet Protocol- adress) är ett nummer i fyra grupper t ex 123.123.123.123 som unikt identifierar en viss uppkopplad dator ungefär som ett

uppskatta antalet värddatorer är att försöka ge en korrekt bild av hur många som använder sig av Internet regelbundet. Enligt FSI använder ca 15% av svenskarna i åldern 16-65 år, d v s ungefär en miljon, Internet någon eller några gånger i veckan och antalet användare dubbleras varje år.[11]

telefonnummer, inklusive lands- och riktnummer, identifierar en viss telefon i det globala telenätet.

[11] Forskningsgruppen för Samhälls- och forskningsinformation (FSI) är en fristående institution, som sedan början av 70- talet bedrivit utredningsarbete och sociologisk

forskning med särskild inriktning på masskommunikation- och informationsstudier. FSI grundar sina beräkningar på intervjuer.

2 Datakriminalitet

Det är svårt att ge en entydig och korrekt beskrivning av vad som avses med begreppet databrott. Någon allmänt accepterad definition finns inte utan istället används flera olika termer t ex datorrelaterade brott, datamissbruk, och datorbrott. Gemensamt för alla begreppen är att det rör sig om kriminella handlingar som på ett eller annat sätt har anknytning till datorer, IT och datateknik. Datatekniken som används i den brottsliga verksamheten kan antingen utgöra ett objekt för kriminella handlingar eller användas som medel för att underlätta eller utföra brott.

Datorbrott kan omfatta all sorts brottslighet så länge brottet är kopplat till användande av eller kunskap om datorer. Det är svårt att skapa nya brottsrubriceringar för databrottslighet och lagstiftaren väljer ofta att skriva om redan befintliga paragrafer så att ett brott som involverar datorer kan passas in under traditionella brottsrubriceringar. De flesta datorbrotten finns i brottsbalken och i Datalagens 21 § finns bestämmelsen om dataintrång. I kapitel 7 redogörs även för det nya lagförslaget om ansvar för elektroniska anslagstavlor. Riksrevisionsverket har i en rapport från 1997 försökt ge en bild av hur omfattande de datorrelaterade missbruken och brotten är i svenska organisationer.

Datorrelaterade missbruk och brott har vissa utmärkande egenskaper:[12]

- De kan utföras mycket snabbt och är mycket svåra att upptäcka.
- De avser normalt mycket stora mängder information.
- De riktas inte mot någon enskild person.
- De genomförs med dator och IT-tekniken.
- De kan vara svåra att bevisa eftersom felet eller incidenten kan bero på tekniskt fel eller genom en mänsklig oavsiktlig felhantering.

[12] RRV 1997:33 s. 15

En stor del av de datorrelaterade missbruken och brotten utgörs av ekonomiska brott. Hit räknas databedrägeri, sabotage, dataintrång, traditionell ekonomisk brottslighet relaterad till datorer och stöld av mjukvara och tjänster. De ekonomiska brotten som utförs med ADB- teknik skiljer sig ifrån den traditionella ekonomiska brottsligheten då objekten ofta är abstrakta och vanliga moraliska värderingar lättare åsidosätts vilket ”underlättar” eller t o m möjliggör brottets genomförande.

2.1 Datorbrott enligt brottsbalken

Sveriges Brottsbalk trädde i kraft 1965 efter straffrättskommitténs långa arbete med att omarbeta 1864 års Brottsbalk. Sedan datoriseringen av samhället inleddes har många nya brott och brottsliga förfaringssätt uppkommit. En del av de gamla traditionella brottsbeskrivningarna har utan problem kunnat tillämpas direkt på de nya datorrelaterade brotten. Stöld av en dator behandlas på samma sätt som stöld av vilket föremål som helst och ett vilseledande med hjälp av upptagning för ADB är bedrägeri precis som om vilseledandet hade skett med hjälp av konkreta handlingar. Under senare år har lagstiftarna varit tvungna att ändra och lägga till i lagtexten för att komma åt vissa specifika problem som informationsteknologin och den datorrelaterad brottsligheten fört med sig.

2.2 Skilda typer av brott

De skilda brottstyper som kan förekomma i ett datornätverk utgör ingen enhetlig grupp utan det kan röra sig om allt från upphovsrättsbrott till försäljning av narkotika via Internet. Vad som är gemensamt för brotten är att de innefattar överföring av information. Den svenska straffrätten är relativt väl utformad för att täcka de brott som kan bli aktuella på Internet och i nätverk. Problemet med att beivra brottslighet via Internet ligger till stor del i svårigheten att identifiera gärningsmannen. Användarnas anonymitet är ett problem när det gäller att förhindra och reglera brott som sker via Internet. Den ökade IT användningen i förening med den nya IT

kulturen som växt fram bland användarna av BBS:er och andra elektroniska förmedlingstjänster har gjort det svårt att fastställa varifrån ett datorprogram eller ett uttalande härrör.[13]

De brottsbalksbrott som aktualiseras kan grovt indelas i brott mot allmän ordning, brott mot den personliga integriteten, brott med ekonomiska syften samt brott mot informationen på Internet.

2.3 Allmänt om de aktuella brottsbalksbrotten

2.3.1 Ekonomisk brottslighet

Flertalet av bedrägeribrotten i 9 kap. BrB kan utföras med hjälp av meddelanden över Internet. I 9 kap.1 § första stycket behandlas det egentliga bedrägeribrottet och utmärkande för brottet är att någon genom vilseledande förmår annan till en disposition som antingen kan innebära en handling eller ett underlåtande. Vilseledandet kan vara skriftligt, muntligt, ske genom faktiskt handlande eller bestå i ett förstärkande av en felaktig föreställning. Vilseledandet skall medföra vinning för gärningsmannen och skada för offret. Begreppet vilseledande medförde tidigare problem eftersom datorer i många fall ersatt människor vad gäller olika former av transaktioner. I många situationer var det datorer som vilseleddes istället för människor och detta skapade problem eftersom rekvisitet om vilseledande i det egentliga bedrägeribrottet ofta inte uppfylldes.

Numera krävs inte något vilseledande för datorbedrägeribedrägeri åtal utan det går lika bra att visa att någon manipulerat med data i vinningssyfte.[14] Manipulation kan ske genom att en person avger en ofullständig eller felaktig uppgift som blir föremål för databehandling eller genom att ändra i programmet som används i datorn t ex genom att byta ut hela programmet eller att flytta över det till ett annat bearbetningsställe. Oriktigt resultat kan

[13] BBS (Bulletin Board System) eller elektronisk anslagstavla är en dator eller server dit allmänheten kan sända in meddelanden och ta del av vad andra sänt in.
[14] Brinck, Ohlson, Thornell s. 188

också uppnås genom att ändra i lagrad data som ligger till grund för den automatiska databehandlingen.

2.4 Brott mot information på Internet

2.4.1 21 § Datalagen

21 § Datalagen kriminaliserar vad som brukar kallas för hacking d v s obehörig tillträde till ett datasystem. För att kunna dömas för dataintrång räcker det med att ta sig förbi lösenord eller andra hinder t ex brandväggar som satts upp för att förhindra intrång.[15] Enligt 21 § Datalagen föreligger dataintrång om någon olovligen bereder sig tillgång till datainformation eller olovligen ändrar, utplånar eller tillför sådan information. Brott föreligger både om angreppet sker mot informationen då den är lagrad, och om det sker då den är under befordran. Paragrafen innehåller inte något subjektivt rekvisit och man har istället överlåtit åt rättsskipningen att avgöra om dataintrång kräver uppsåt eller om man kan ställas till ansvar för vårdslöst dataintrång. Datalagens bestämmelser skall inte tillämpas om förfarandet i det enskilda fallet är straffbart enligt bestämmelserna i Brottsbalken eller Lagen om skydd för företagshemligheter.[16] Datalagens 21 § är ett stadgande som är ägnat att vara ett reservstadgande till bestämmelserna i Brottsbalken och används i flertalet fall av hacking och spridande av datavirus men skall bara användas om inget allvarligare brott föreligger.[17]

Förberedelse och försök till dataintrång är straffbart om det fullbordade brottet inte är att anse som ringa. Många dataintrång utgör endast förbrott till brottsbalksbrott och dataintrånget konsumeras då av det grövre brottet och det framgår inte heller av brottsrubriceringen att ett dataintrång varit för handen.

[15] En brandvägg eller firewall innebär att en dator eller ett nätverk skyddas mot obehörig tillträde genom lösenord eller annat säkerhetssystem.
[16] 1990:409
[17] Datalagen (1973:289)

2.5 Brott mot person och integritet

2.5.1 Förtal via Internet

Under våren 1997 avgjorde HovR för nedre Norrland ett mål om förtal över Internet. Bakgrunden var att en kvinna A brutit ett förhållande med mannen L. Efter uppbrottet lät L införa en kontaktannons i A:s namn på en amerikansk Online-site ”ClubLove”. Förutom personuppgifterna, inklusive telefonnummer och e- post adress, angav L under *description*: ”I love to suck and fuck…no limit” och under *seeking*: ”someone to turn me on… call me” Under de tio dagar annonsen var införd fick A 16 e- post brev och ca 15 telefonsamtal med för henne kränkande innehåll. A fick ägna en hel del tid och möda åt att få bort annonsen från siten. L erkände att det var han som skickat in annonsen. Kontaktannonserna var endast åtkomliga av dom som hade abonnemang med tillhörande behörighetskod. I detta fall rörde det sig enligt TR om ”tusentals personer” eller i vart fall ”en inte begränsad krets” (HovR). Både TR och HovR ansåg att tillräcklig spridning skett och att uppgifterna i annonsen var ägnade att utsätta A för missaktning. L dömdes för grovt förtal till 80 dagsböter på sammanlagt 8800 kr samt att utge 15000 kr i skadestånd till A.

I HovR fördes ett resonemang angående spridningens omfattning. En ledamot ansåg att den totala spridningen saknade avgörande betydelse för utgången av målet och menade att förtalet inte borde rubriceras som grovt med hänsyn till att spridningen i kretsar som A var eller kunde tänkas komma i kontakt med måste antagits ha varit begränsad.

2.5.2 Brott mot allmän ordning

De brott som kan komma ifråga är hets mot folkgrupp BrB16 kap. 8 § för den som uttalar missaktning för folkgrupp på grund av ras, hudfärg, etniskt ursprung eller dylikt. Rasistiska meddelanden och budskap som sprids via Internet innefattar ofta uppmaningar till andra att vidta straffbara åtgärder och sådana uppmaningar kan innebära uppvigling enligt BrB16 kap. 5 §.

Barnpornografibrott, BrB 16 kap. 10 a §, föreligger om någon skildrar barn i pornografisk bild eller sprider sådan bild. Olaga våldsskildring BrB 16 kap.10 b § avser bilder med sexuellt våld eller tvång eller annat grovt våld. Att sprida bilder bland barn och ungdom som kan ”verka förråande eller vara skadligt för de ungas sedliga fostran” kan vara brottsligt som förledande av ungdom enligt BrB 16 kap. 12 §. De tre sistnämnda brotten är rena spridningsbrott och varje befattning med en bild i syfte att den skall spridas vidare på t ex Internet är i sig brottsligt. Här torde det vara tillräckligt med ett eventuellt uppsåt hos gärningsmannen.

2.6 Identifiering av gärningsman

Straffrättsligt är frågan vem som kan anses vara ansvarig i enlighet med de aktuella straffbestämmelserna men även vilka administrativa och tekniska åtgärder som kan vidtas för att den som använder en BBS skall kunna identifieras. Exempel för identifiering av användarna är avancerad lösenordshantering, dekryptering av kodade meddelanden och via skriftligt undertecknade handlingar innan en ny användare får tillträde till ett informationssystem eller en BBS.[18]

Problemet att finna en gärningsman ligger i att data utan särskilda kontroller tillförs elektroniska förmedlingstjänster via nätverk. En person som misstänks för brott med anknytning till en BBS eller liknande förmedlingstjänst gör vanligtvis gällande att han inte känner till att det aktuella meddelandet finns i basen eller vem som har sänt in meddelandet.

Tekniskt sett kan brottslig information som sprids via Internet och databaser till skillnad från muntlig kommunikation lämna vissa elektroniska spår som i vissa fall kan leda fram till gärningsmannen. Informationen som finns i databaser och elektroniska diskussionsgrupper lagras och finns kvar även efter det att informationen raderats. Även om oriktiga uppgifter om t ex avsändare har använts så finns det relativt goda möjligheter att på teknisk

[18] SOU 1996:40 s. 150

väg spåra den ursprungliga källan genom att följa kedjan bakåt i näten.[19] Svårare är det att få rättsliga förutsättningar för sådana åtgärder och spaning som avser elektroniska förmedlingstjänster tangerar tvångsmedel som husrannsakan, beslag av datorer, och hemlig teleavlyssning. I den utsträckning som en åtgärd är att bedöma som teleavlyssning eller teleövervakning är användningsområdet med hänsyn till skyddet för den enskildes personliga integritet enligt 2 kap. 6 § RF, begränsat till den grova brottsligheten som oftast inte blir aktuell i dessa fall.

2.7 Brottslingens profil

IT - kriminalitet begås av brottslingar med helt olika profil. I en del fall är det hackers som inte är kriminella i annat avseende än att de begår databrott av visst slag, men bilden av en hacker som en relativt ung person som i grunden är hederlig stämmer långtifrån alltid. Hackers som begår omfattande och kvalificerad databrottslighet är i många fall socialt särpräglade personer som uppvisar missbruk och andra sociala störningar.[20]

Rikspolisstyrelsens databrottsgrupp menar att anmälningarna om dataintrång ökar kraftigt när det är skollov och det skulle tyda på att det fortfarande är mest ungdomar som sysslar med databrotten. Kontokortsbedrägerier begås till stor del av yrkeskriminella som ett led i organiserad brottslighet med ursprung i länder i Asien och Afrika.[21] I vissa fall begås IT brotten av personer anställda inom de företag som drabbas. Insiderbrotten sker för egen räkning eller av externa kriminella som behöver hjälp med att genomföra brottsplanen. Personer som begår insiderbrott känner till datasystemet och kan genom sin position skaffa sig tillfälle att manipulera systemen på ett sätt som är svårt för en utomstående. I en rapport från Riksrevisionsverket anges att i 35% av de uppgivna incidenterna var gärningsmannen en anställd och i 6% av fallen var gärningsmannen en utomstående tillsammans med en

[19] SOU 1996:40 s. 151
[20] Ds 1997:51 s. 83

anställd. Insiderbrotten är svårupptäckta och beror oftast på tillfälligheter samtidigt som dessa brott utgör den svagaste länken i datasäkerheten.[22]

[21] Ds 1997:51 s. 83
[22] RRV 1997:33 s. 32

3 Kryptoteknik

3.1 Allmänt om bakgrunden

Kryptografi har använts i Sverige under lång tid framförallt inom försvaret och i utrikesförvaltningen.[23] Kryptografi används även i bankomatsystem och GSM telefoner. Denna typ av kryptografi är av ett slag som en enskild användare inte kan påverka eller ha någon insyn i. Under den senaste tioårsperioden har myndigheter och företag allt mer börjat att kryptera den interna kommunikation och annan känslig data som lagras på datorns skivminne.[24] Kryptografi är ett ämnesområde som innefattar olika principer och metoder för att omvandla data från läsbart och begripligt till icke begripligt och omvänt. Kryptografi används i huvudsak till att säkerställa identiteten hos mottagare och avsändare av elektroniska dokument och meddelanden, men även för att skydda data och meddelanden mot förvanskning. Eftersom datanäten som t ex Internet är osäkra är kryptering en bra metod för att skydda användarna i sådana situationer då informationen hamnar på avvägar beroende på tekniska brister och fel. Kryptering är en viktig del av näringslivets egna åtgärder för att skydda sig mot kvalificerad ekobrottslighet. Kryptering utgör ett viktigt skydd för känslig datahantering men kan också användas av kriminella för att undandra sig avlyssning i samband med t ex en brottsutredning. Debatten om krypteringen har behandlat frågan om det skall vara fritt att kryptera datakommunikation eller om det skall finnas en skyldighet att bereda myndigheter tillgång till informationen t ex genom att deponera en krypteringsnyckel för användning i samband med brottsutredning.[25]

[23] Kryptering innebär att man omvandlar data genom att använda kryptografi för att framställa icke begripliga data i avsikt att säkerställa dess konfidentialitet.
[24] Rapport från Regeringskansliets referensgrupp för krypteringsfrågor, oktober 1997, s. 7
[25] Regeringskansliets referensgrupp för krypteringsfrågor, s. 8

3.2 Berörd lagstiftning i Sverige

3.2.1 Rätten att ta del av allmänna handlingar

I 2 kap. tryckfrihetsförordningen framgår att varje svensk medborgare har rätt att ta del av offentliga uppgifter som är dokumenterade i vad som innefattas i begreppet allmän handling. Grundläggande förutsättning för att en handling skall anses som allmän är att den förvaras hos myndighet. Därutöver krävs att den är att anse som inkommen till eller upprättad hos myndigheten. För att en enskild person skall kunna tillgodogöra sig innehållet är myndigheten skyldig att tillhandahålla handlingen så att den kan läsas avlyssnas eller på annat sätt uppfattas 2 kap. 12 § 1 st TF. Myndigheterna har en skyldighet att tillhandahålla handlingar i läsbart skick men avgör själva hur detta sker. En begäran att få ta del av en allmän handling kan endast vägras om stöd för hemlighållande finns i bestämmelse om sekretess enligt Sekretesslagen.[26] Att en uppgift är krypterad innebär inte i sig något skäl att undanhålla allmänheten rätten att ta del av innehållet i klartext och endast om någon sekretessbestämmelse blir tillämplig kan innehållet i den krypterade texten hemlighållas. En myndighet som av säkerhetsskäl förvarar en allmän handling i krypterad form är skyldig att dekryptera texten för att tillmötesgå en enskild persons önskan om att få ta del av handlingen. Myndigheterna måste ha kontroll på vilka privata konfidentialitetsnycklar som anställda utnyttjar.[27] Är någon anställd bortrest eller slutar sin anställning måste myndigheten ha möjlighet att få tillgång till information som kan vara krypterad.

3.2.2 Skydd av personlig integritet

Enligt 2 kap. 3 § 2 st RF har varje medborgare i den utsträckning som medges i lag ett skydd mot att den personliga integriteten kränks genom att

[26] Sekretesslagen 1980:100
[27] En privat konfidentialitetsnyckel skall inte göras tillgänglig för andra. I vissa fall kan en arbetsgivare behöva ha tillgång till sina anställdas privata signaturnycklar, d v s de nycklar de anställda använder i tjänsten.

uppgifter om honom registreras med hjälp av automatisk databehandling. I Datalagen anges de svenska reglerna på detta område. Den som ansvarar för ett personregister skall skydda registret mot oavsiktlig eller otillåten förstörelse eller mot otillåten ändring eller spridning och kryptering av data kan vara ett sätt att uppfylla datalagens krav. Datainspektionen kräver att känsliga uppgifter som skall föras över på allmänna nät skall krypteras för att skyddas mot obehörig insyn. Enligt 1 kap. 2 § RF skall det allmänna värna om den enskildes privatliv och familjeliv. Andra exempel på integritetsskyddande lagstiftning är bestämmelserna i Brottsbalkens 5 kap. Om brott mot frihet och frid samt Lagen om övervakningskameror.[28] Europakonventionen om skydd för de mänskliga rättigheterna och grundläggande friheterna gäller som lag i Sverige. Enligt artikel 8 i konventionen har alla rätt till skydd för sitt privat och familjeliv, sitt hem och sin korrespondens. Inskränkningar i rätten får göras bl a för att förebygga oordning eller brott samt för att inskränka andra personers fri och rättigheter.

3.3 Krypteringsalgoritmer

3.3.1 Allmänt om algoritmer

När ett digitalt meddelande skickas kan det skapa olägenhet om någon obehörig lyckas läsa meddelandet. Beroende på meddelandets innehåll kan man vidta olika försiktighetsåtgärder ett brev kan t ex rekommenderas eller skickas med kurir. För att den moderna informationsteknikens möjligheter att skicka meddelanden och data skall kunna tillvaratas måste det finnas en möjlighet att skicka viktiga meddelanden och lagra känslig information utan att någon obehörig kan ta del av innehållet.

För att förhindra obehöriga att läsa meddelande kan klartexten förvanskas så att endast den som är behörig kan läsa texten och med det menas att

[28] 1990:484

klartexten krypteras och får en kryptotext. En krypteringsalgoritm är informationen som beskriver hur klartexten förvanskas, och informationen i en krypteringsalgoritm kan ha en mängd olika varianter. Varianten hålls hemlig men inte nödvändigtvis algoritmen.[29] Istället för att säga att man har olika varianter säger man att man har olika nycklar och två personer som skall kommunicera måste komma överens om vilken nyckel som skall användas för att låsa och låsa upp meddelanden. När personen vet både algoritm och nyckel kan kryptotexten omvandlas till klartext och detta kallas för att dekryptera kryptotexten. En kryptotext kan forceras genom att olika nycklar prövas till dess att man finner den klartext som ursprungligen krypterades. En förutsättning för att en algoritm skall skydda mot insyn är att det finns många nycklar till algoritmen. Om det t ex endast finns tio nycklar är det lätt att dekryptera kryptotexten med de tio möjliga nycklarna och på detta sätt hitta det riktiga meddelandet. Dekrypteras meddelandet manuellt räcker det med ett par tusen nycklar för att det skall bli omöjligt att dekryptera meddelandet inom en rimlig tid. Användandet av datorer i samhället idag för förmedling av information och kryptering och dekryptering gör att antalet nycklar är mycket omfattande.

3.4 Data Encryption Standard (DES)

Den vanligaste algoritmen som används idag är Data Encryption Standard (DES) och till DES standarden hör ca 72 miljarder nycklar och det krävs mycket stor datorkapacitet för att forcera DES krypterade meddelanden.[30] Svenska banker och finansinstitut använder sig av kryptografi för sin interna datakommunikation och ofta sker krypteringen med DES algoritmer. Ett stort antal Internet användare däribland forskare och studenter använder fritt via Internet tillgänglig kryptoprogramvara för att skydda överförda meddelanden mot obehörig insyn. En stor del av krypteringen baseras på

[29] Regeringskansliets referensgrupp för krypteringsfrågor, s. 15
[30] En kryptografisk nyckel är en parameter som används tillsammans med en kryptografisk algoritm för att transformera, kontrollera, kryptera eller dekryptera data.

programvaran PGP (Pretty Good Privacy).[31] Många PGP- användare utnyttjar nyckelhanteringssystem med s k öppen och privat nyckel och detta system är det som har störst utbredning i Sverige. I USA genomfördes under 1997 en samlad attack med 70 000 medverkande persondatorer och även större datorer under ledning av säkerhetsföretaget RSA. Syftet med försöket var att forcera *ett* DES krypterat meddelande. Resultatet blev att endast en av de medverkande persondatorerna lyckades knäcka krypteringen.

3.4.1 Bitar och nyckellängder

Vanligtvis brukar man istället för antalet nycklar ange nyckellängden och den enhet som nyckellängden anges i kallas för bitar. Tio bitar betyder ungefär tre nollor och tio bitars nyckel är ungefär ett tal med en etta och tre nollor. 20 bitars nyckel blir en etta med sex nollor d v s en miljon och 30 bitar blir ungefär en miljard. DES systemet har 56 bitars nyckel och kan beskrivas enligt denna tabell.[32]

10 bitar	1 000
20 ”	1 000 000
30 ”	1 000 000 000
40 ”	1 000 000 000 000
50 ”	1 000 000 000 000 000
56 ”	72 058 000 000 000 000

Det finns två olika krypteringsalgoritmer dels symmetriska och dels asymmetriska. DES- algoritmen är ett exempel på en symmetrisk algoritm och kännetecknas av att samma nyckel används både för att kryptera och för att dekryptera texten.[33] För att två personer skall kunna kommunicera måste man kunna byta nyckel med varandra utan att den hemliga nyckeln röjs.

[31] Pretty Good Privacy är en programvara som används för att kryptera e- post och annan filöverföring och vissa versioner finns att hämta hem gratis på Internet.
[32] Regeringskansliets referensgrupp för krypteringsfrågor, s. 16
[33] Regeringskansliets referensgrupp för krypteringsfrågor, s. 16.

Nyckelparen används för att kryptera innehållet från klartext till kryptotext men också för att dekryptera innehållet från en kryptotext till klartext. Vid kryptering av innehållet i ett meddelande använder sändaren mottagarens öppna nyckel för att kryptera och mottagaren får sedan använda sin privata nyckel för att dekryptera innehållet. Nyckeln används också till att signera data och skapa digitala signaturer och för att verifiera den digitala signaturen. Vid signeringen använder sändaren sin privata nyckel för att signera data och mottagaren använder sändarens öppna nyckel för att verifiera sändarens digitala signatur.[34]

3.5 Digitala signaturer

I detta avsnitt tänkte jag visa hur en text krypteras med en öppen konfidentialitetsnyckel och hur texten ser ut i datorläsbar form efter kryptering. Avancerad kryptering kan i praktiken endast skötas av datorer. Om en krypterad text kommer på avvägar på Internet är det i stort sett omöjligt att dekryptera texten utan tillgång till den privata konfidentialitetsnyckeln.

3.5.1 Klartext

Jag tänkte nedan visa ett exempel på hur ett meddelande kan se ut dels som vanlig text och dels som krypterad. Text: ”The Agenda was approved as proposed. However the Chairman recommended that an introductory statement by Roland Huber should be taken at the start of the meeting which would adress several subsequent items on the Agenda. Chairman`s note: For convenience of presentation, the Summary Record has been drafted to correspond to the items in approximately the same order in which they

[34] Regeringskansliets referensgrupp för krypteringsfrågor, s. 17.

appered on the Agenda. Some items have been merged to help in the presentation”.[35]

3.5.2 Öppen konfidentialitetsnyckel

10010100110110001100001011010111110000011000100
11111000011111001100001101000100111000001110000
01110000011100000011100010111000011

3.5.3 Kryptotext

I__%_i”B*f_AE´_´epì´n*_äÖré_cV_c*R*ILE_rÖ¨´_%n”ÚÖU*r´*_r_VÁ=kY…O-
_ilt___*CT^?pE4Â*m_¨*R*JT+À__3a’áN__*_0^^Èàa-ê_) Äá8)¨`ÒûXgáúMê
p+Êá(___Fô\£´m!Îùv_q_*X):ó^å”_BvxÀPè`^1_5=cop_+´£ÄÀ<E
!G_ö*Ù1_îU}_§ä__j_TÀ,c£y5TMw$Ù_%Ùe>*c,_\À*r*ö7@aûc_m^___-ê_
_I5B?Àà_%¨5*_Tc_ÏdPi¨c_nB8T*}u_¨…t___G_S*oe*_(%>k,aîl(EdÍ1[qäêoeÎ
À_s_k_s_
òn\[*_”5Î_CWd”0_A_A_Ô---´_uÌ:_|<8@M-
__D=&_^´_PG^´_!_)__ua_Ì^`i_Ô_
¨NåùÈOÒ>>¨_ôq<_>>_èÒÎ__.:7C_Ù8Bô_…

Krypteringen ger ett skydd mot obehörig insyn och eftersom datanät som Internet är osäkra är kryptering en bra metod för att skydda användarna även i de fall då informationen hamnar på avvägar beroende på tekniska fel och brister.

[35] Den algoritm som exemplet har utgått från kommer från ett företag i Schweiz och nyckellängden är på 128 bitar.

3.6 Konfidentialitet[36]

Om den organisatoriska enhet som ger ut digitala signaturer även skall förvara användarens privata konfidentialitetsnyckel och lämna ut den till rättsvårdande myndigheter vid misstanke om grov brottslighet i enlighet med lag är frågan om det kan ske utan att ägaren till nyckeln blir informerad om detta. Om så är fallet måste ett ställningstagande ske till om enheten skall vara fristående från parterna s k Trusted Third Party (TTP) eller ingå i en av parternas organisationer en s k inhouse Trusted Party (iTP).[37] En möjlighet är att nyckeldeponering och rättsvårdande myndigheters möjlighet att få tillgång till nycklar och klartext är sammankopplad med licensgivning som vid exportkontrollen av kryptoteknik.

Konfidentialitet tillgodoses genom kryptering av meddelandets innehåll. Skyddet av konfidentialitet bryts om kryptosystemet är svagt eller om kryptonyckeln görs tillgänglig. Om skyddet blir ovillkorligt försvåras eller omöjliggörs bl a hemlig teleavlyssning och vid husrannsakan kan polisen inte komma åt krypterad data i klartext. Om skyddet i framtiden blir lättanvänd, billigt och mångsidigt finns risken att olika former av kriminalitet kan komma att underlättas.

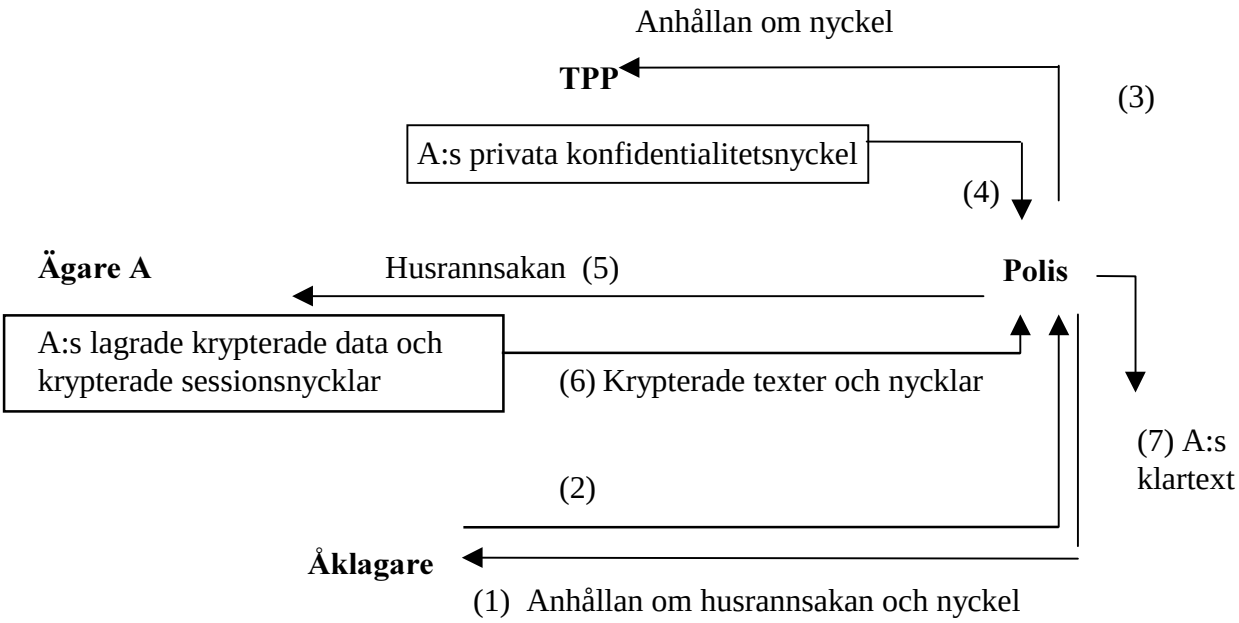
3.7 Brottsförebyggande åtgärder

3.7.1 Husrannsakan och beslag

De polisiära kraven aktualiseras vid husrannsakan, beslag och vid hemlig teleavlyssning. Vid husrannsakan hos en misstänkt ställs polisen inför problemet att informationen och bevisen finns i krypterad form på den misstänktes hårddisk. Om en privat konfidentialitetsnyckel finns deponerad hos en TTP kan polisen om erforderlig lagstiftning finns med stöd av

[36] Konfidentialitet innebär att data eller information inte är tillgänglig eller läsbar för obehöriga individer, organisationer eller processer.
[37] Trusted Third Party eller CA (Certification Authority) innebär att en krypteringsnyckel deponeras hos en betrodd tredje part. TPP:ns trovärdighet garanteras normalt genom licens. TPP:n presenterar nycklarna på ett sätt där det säkert framgår att en viss nyckel hör till en viss person, funktion eller system.

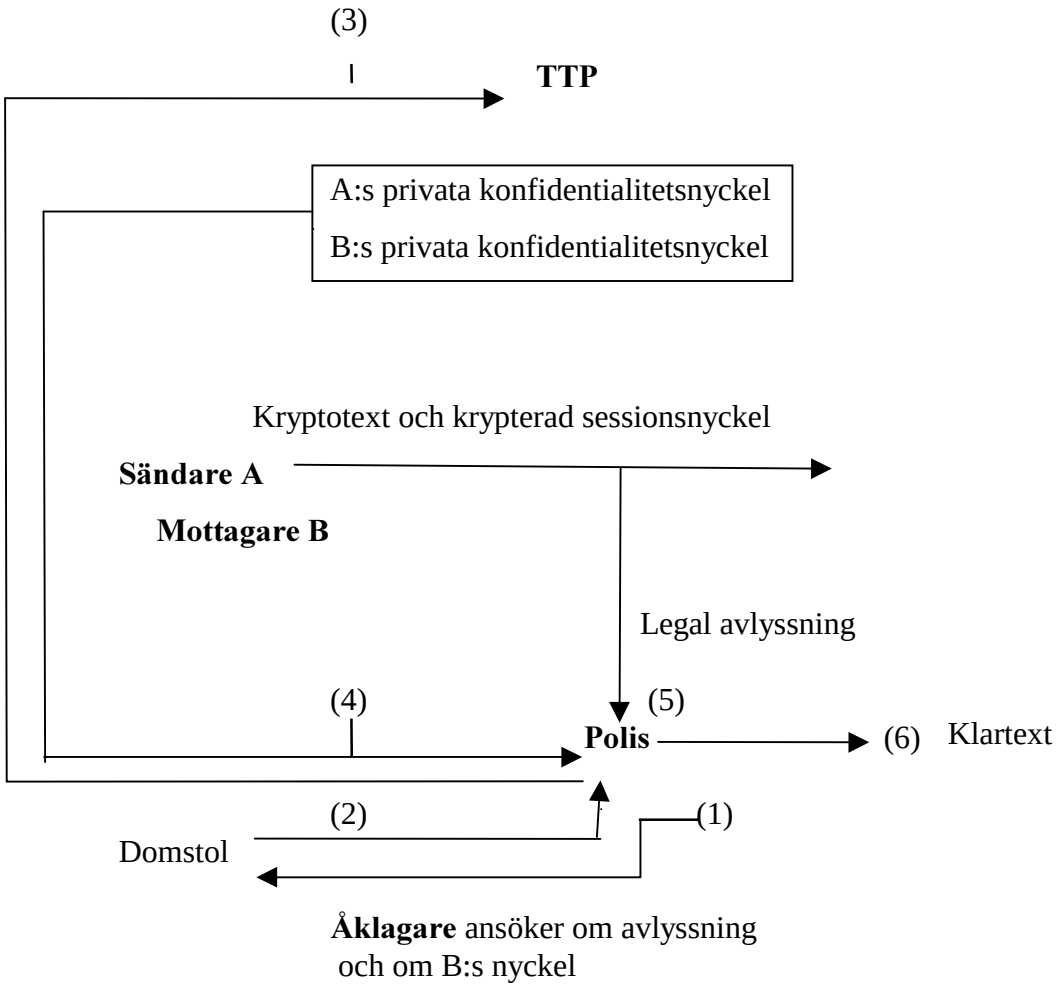
domstols eller åklagarbeslut få tillgång till informationen på hårddisken. Ett alternativ är att polisen enbart begär att få information från den misstänkte.



Polisen tar genom (1) och (2) kontakt med åklagare/domstol för att få tillstånd till husrannsakan och beslag samt att få tillstånd att hämta ut nyckeln hos en TPP. I (3) och (4) vänder sig polisen till TPP:n för att få tillgång till A:s privata konfidentialitetsnyckel. I (5) och (6) har polisen kontakt med A och får den lagrade kryptotexten. Slutligen i (7) dekrypterar polisen kryptotexten och får fram klartexten. Den privata konfidentialitetsnyckeln för lagring av data är inte samma nyckel som används för att kryptera meddelanden som skall överföras. En person som använder sig av kryptografi och som misstänks för brott har ingen skyldighet att aktivt medverka i brottsutredningar genom att t ex lämna ut sin privata konfidentialitetsnyckel.[38] De rättsvårdande myndigheterna har dock möjlighet att tvångsvis genom t ex husrannsakan få tillgång till användarens nycklar även om de förvaras hos någon annan.

3.7.2 Hemlig teleavlyssning

Om meddelanden som skickas mellan A och B är krypterade med ett starkt krypto kan inte polisen läsa dem även om man har tillstånd att avlyssna kommunikationen mellan A och B. För att läsa meddelanden måste polisen ha tillgång till nyckeln som både A och B använder. Om A och B deponerar sina privata konfidentialitetsnycklar hos en TTP kan polisen om tillstånd ges från domstol, få tillgång till de behöriga privata nycklarna.



[38] Exemplet bygger på uppgifter i Kryptopolitik- möjliga svenska handlingslinjer, Regeringskansliets referensgrupp för krypteringsfrågor, oktober 1997, s. 49

Efter framställan från åklagaren kan domstol ge polisen tillstånd som krävs i (1) och (2). Genom domstolsbeslutet kan polisen kontakta TTP:n för att få tillgång till B:s privata konfidentialitetsnyckel (3) och (4). I (5) görs den hemliga avlyssningen, vilken polisen enligt (1) och (2) har tillstånd till. I (6) dekrypterar polisen först sessionsnyckeln och med hjälp av denna själva meddelandet och får fram klartexten. Polisen har tillgång till B:s privata konfidentialitetsnyckel utan att A och B är medvetna om det.[39]

Polisen behöver tillgång till B:s privata konfidentialitetsnyckel för att avlyssna trafik till B från den misstänkte A. Polisen får information om vilken TPP som skall kontaktas genom nationell och internationell kommunikation där användarna anlitar var sin TPP i det egna landet eller i ett annat land. Om A är misstänkt för ett allvarligt brott och krypterar meddelanden till B måste polisen använda B:s privata konfidentialitetsnyckel för att läsa A:s meddelanden till B. Under vissa omständigheter är det av stor vikt att snabbt få tag i B:s nyckel utan dennes vetskap därom (vid eventuellt samarbete mellan A och B) för att förhindra allvarligare brott.

3.7.3 Exempel

Jag tänker nedan presentera två fall med utgångspunkt i att alla TPP:er är ackrediterade och har licens samt att det finns en rättslig grund för polisen att begära att en TPP skall medverka till att lämna ut den privata konfidentialitetsnyckeln utan att avslöja detta för dem som kommunicerar. Utgångspunkten är att det krypterade meddelandet innehåller en kod som talar om vilken TPP som används.

[39] Exemplet bygger på uppgifter i Kryptopolitik- möjliga svenska handlingslinjer, Regeringskansliets referensgrupp för krypteringsfrågor, oktober 1997, s. 50

3.7.4 Fall 1

A och B bor i Sverige och anlitar var sin TPP i Sverige. I detta fall kan polisen efter det att meddelandet har avlyssnats ta kontakt med berörd TPP i landet och begära att nyckeln utlämnas. TPP:n bedriver vanligtvis verksamhet 24 timmar om dygnet och det torde vara möjligt att snabbt efter ett domstolsbeslut få tag på berörda nycklar. I detta fall torde det inte vara några problem för polisen att få tag på begärda nycklar.

3.7.5 Fall 2

I detta fall bor A i Sverige och B i Finland och anlitar TPP:er i sina respektive hemländer. Den svenska polisen kan misstänka A eller B eller båda för brott begångna i Sverige och detsamma gäller för den finska polisen för brott begångna i Finland. Det första polisen gör om man misstänker brott är att komma till klarhet om vilken TPP som berörs i respektive land. Troligtvis behöver den svenska polisen söka hjälp av den finska polisen för att tillfråga den finska TPP:n om den förvarar nyckeln. TPP:n måste svara på en förfrågan utan att informera sin kund om polisens intresse. När polisen vet vilken TPP som har nyckeln gäller det att bestämma vilket lands polis som skall göra en begäran om att få nyckeln utlämnad. Polisens avlyssning sker i det egna landet men vid allvarlig brottslighet med flera inblandade parter kan flera länders polis behöva medverka.

3.7.6 JMW- Systemet

En TPP lösning måste tillgodose de rättsvårdande myndigheternas krav på effektivitet och hantering i samtliga inblandade länder. JMW- systemet är en TPP lösning som utarbetats av en expertgrupp inom EU och systemet underlättar polisens arbete.[40]

[40] Systemet utvecklades på Royal Holloway College i London och publicerades 1996. Namnet kommer från initialerna på de tre upphovsmännen N. Jefferies, C. Mitchell och M. Walker.

JMW- systemet bygger på att en användare utnyttjar en TPP i det egna landet. Om A bor i Sverige och B bor i Finland anlitas var sin licensierad TPP i Sverige respektive Finland. Hos den egna TPP:n kan deras privata konfidentialitetsnyckel återskapas och B:s privata nyckel kan vid kommunikation med A återskapas i dennes TPP och tvärtom.

För polisen i Sverige innebär JMW- systemet att A:s hela kommunikation med alla skulle kunna avlyssnas utan behov av samarbete med någon polis eller TPP i något annat land. Den svenska polisen skulle kunna avlyssna B:s kommunikation med A eller hans övriga kommunikation med Sverige utan att behöva samarbeta med den finska polisen i varje enskilt fall eller ha kontakt med B:s egen TPP.

JMW- systemet uppställer krav på att varje användares privata konfidentialitetsnyckel finns i båda TPP:erna. I fallet ovan finns A:s nyckel i den svenska TPP:n och B:s TPP i Finland. Genom att A:s nyckel finns i flera TPP:er minskar benägenheten att använda nyckelhanteringssystemet.

JMW- systemet är effektivt för de rättsvårdande myndigheterna och kan jämföras med hemlig teleavlyssning där båda länderna kan avlyssna samtalet utan det andra landets medgivande.[41] De flesta stater har intresse av att bedriva brottsbekämpning på det egna territoriet utan att behöva blanda in andra stater.

Användningen av kryptografi på World Wide Webb är fortfarande relativt låg. En rapport från december 1996 visade att av ca 650.000 webbsidor erbjöd 10% en så kallad SSL kryptering som är en kryptoteknik anpassad just för webb användning. SSL krypteringen skapar skydd vid överföring av meddelanden på Internet. Endast 5% av webbsidorna erbjöd

tredjepartscertifiering (TPP) för att kunna säkra identifieringen av användarna.

Spridningen väntas öka snabbt dels genom införande av kryptografi i program som Windows 95 och Netscape Navigator dels genom att handeln och andra elektroniska affärer via Internet blir allt vanligare.[42]

[41] EU- kommissionen (DG XIII) bedriver för närvarande ett par projekt där JMW-konceptet utvärderas. Det sker inom ramen för förberedelserna för ett eventuellt kommissionsförslag om European Trust Services (ETS).
[42] Windows 95 är ett operativsystem för PC- datorer. Netscape Navigator är ett program som gör det möjligt att ”surfa” på Internet.

4 Jurisdiktion och Internet

4.1 Allmänt

I och med Internet har människor fått tillgång till ett medium som är snabbt och globalt och det har fört med sig nya och relevanta frågor om hur vissa straffrättsliga och privaträttsliga regler skall tillämpas. Vem bestämmer över Internet ? Vem bestämmer vad som skall få förekomma på en webbsida ? Vad är att anse som brottsligt och vem avgör i så fall det ? Varje nation har sina egna lagar och har rätt att tillämpa jurisdiktionen på det egna territoriet. Internet är inte något nytt på det sättet att olika nationers rättssystem kommer i konflikt med varandra men med Internet kommer en enorm ökning av de internationella kontakterna människor i mellan från vitt skilda delar av världen och med det följer nya frågor om vad som skall gälla för det nya globala mediet.

Internet sammanlänkar en rad juridiska frågor med internationell anknytning t ex spridande av bombrecept, ärekränkningsbrott och upphovsrätt. Begrepp som tidigare upplevts som åtskilda från varandra har fått en ny gemensam nämnare. Principen om nationell jurisdiktion kan brytas genom internationella konventioner t ex genom att staterna erkänner varandras domar, liknande konventioner finns men de är inte heltäckande. Inom områden som saknar konventionsbestämmelser måste man inskränka svensk rättstillämpning till Sverige och de svenska rättssubjekten.[43]

4.1.1 Det gränsöverskridande Internet

Det finns inte några generella internationella regler vad gäller lagval på Internet men inom en del områden t ex upphovsrätten som av tradition haft gränsöverskridande karaktär har en specialanpassning skett framförallt genom internationella överenskommelser och undertecknandet av

konventioner. Konventionerna bygger först och främst på grundläggande värderingar som är gemensamma för stora delar av världen och som kan tillämpas vid eventuella tvister där det inte finns några klara regler för vad som skall gälla. EU:s allmänna attityd är att försöka harmonisera medlemsländernas lagar på områden utanför straffrätten.[44] Att anpassa reglerna på Internet och hävda att de finns en global generell konvention gällande tillämplig lag på Internet är inte möjligt eftersom någon internationell konvention som reglerar och begränsar Internet inte existerar, i alla fall inte på en global nivå.

4.1.2 Jurisdiktionsproblemet

Problemet med jurisdiktionen och lagvalet kan delas in i tre olika delmoment. För det första var finns det egentliga lagvalet och frågan om vilket lands lagar som skall tillämpas i en viss situation. För det andra, problemet med verkställbarheten och huruvida en utländsk dom kan erkännas och verkställas här i Sverige men även hur svenska domar kan komma att erkännas och verkställas utomlands. För det tredje frågan om forumval, vilket lands domstol är behöriga att pröva eventuella tvister.[45] Bestämmelserna regleras enligt varje lands nationella lagar. En och samma fråga kan bedömas olika enligt skilda rättsordningar och domstolar i skilda länder kan anse sig behöriga att pröva tvisten. Även i Sverige är emellertid regleringen i den utsträckning det finns någon sådan, olika och varierande för olika rättsområden t ex brottsbalksbrott, upphovsrätt mm.

4.2 Lagval

Svensk domstols behörighet att döma för brott behandlas i 2 kap. BrB. Om ett brott är begånget i Sverige är svensk domstol enligt

---

[43] Thomas Carlèn- Wendel, Lag och rätt på Internet, s. 32
[44] Carlèn- Wendel, s. 38. Inom privaträtten finns Romkonventionen 1980 om lagval inom avtalsförpliktelser och Brysselkonventionen 1968 om domstols behörighet och om verkställighet.
[45] Carlèn- Wendel, s. 35

territorialitetsprincipen i 2 kap. 1 § behörig att ta upp saken till prövning. När det gäller frågan om lagval gäller principen om anknytning d v s man försöker finna det land där rättsförhållandet har starkast anknytning och begreppet anknytning kan bestå i att ett brott riktas mot Sverige eller t ex att viss omtvistad egendom finns här. Principen om starkaste anknytningen ger inte alltid ett entydigt svar eftersom det kan finnas anknytningar till flera länder och inte bara till Sverige men generellt sett har domstolarna ofta en tendens att prioritera anknytningen till det egna landet.[46]

Inom straffrätten finns det för brott i allmänhet grundläggande regler för tillämpningen av svensk lag med beaktande av anknytningsprincipen i brottsbalkens 2 kap. I 2 kap. 4 § BrB anges under vilka förutsättningar ett brott skall anses begånget i Sverige.

- var den brottsliga handlingen företogs
- var brottet fullbordades
- vid försök, var det tillämnade brottet skulle ha fullbordats.[47]

För brott begångna över Internet som t ex dataintrång, bedrägeri och förtal innebär reglerna att bedömningen först och främst skall ske enligt lagen i det land där den brottsliga handlingen företogs. Svensk rätt skall tillämpas om brottet riktar sig mot svenskar eller svenska intressen, t ex om en hacker från utlandet förstör information i en svensk dator. Även om den brottsliga handlingen i detta fall har företagits utomlands kan svensk lag vara tillämplig. För att detta skall vara möjligt krävs att gärningsmannen är svensk eller har sin hemvist här samt att handlingen är straffbar även i det land där den företogs.

Under 1996 gäckade en nittonårig svensk hacker i en Göteborgsförort både den amerikanska federala polisen FBI och den svenska rikskriminalens datagrupp. Under två månader ringde nittonåringen 60 000 illegala samtal till en kostnad av ca två miljoner kronor. Genom hemliga telefonnummer som fanns tillgängliga på Internet tog han sig bakvägen in till de

[46] Carlèn- Wendel, s. 36
[47] SOU 1992:110 s. 469 ff.

amerikanska 911 operatörerna och slog ut deras larmsystem vilket ledde till att det amerikanska SOS numret i vissa delar av Florida inte gick att använda. Han manipulerade också telefonväxlar, datorer och servicelinjer så att samtalen debiterades på andra. Genom att scanna Vita Husets telefonväxel fick han tillgång till den amerikanske presidentens vardagliga schema. Nittonåringen flyttade också över porrtidningen Hustlers orderfax till sin egen dator. När FBI kopplades in fick fallet hög prioritet och under tre månader jagades den okände hackern utan resultat. FBI utformade ett speciellt schema för 911 operatörerna som skulle följas vid en eventuell ny attack. USA:s största telefonbolag AT&T hade upptäckt att en sabotör ringde för stora belopp och använde testnummer avsedda för bolagets egna tekniker. Genom att samköra sina listor med dataregistrerade telefonsamtal med FBI:s listor kunde hackern lokaliseras till Sverige. Ett år efter avslöjandet föll domen i Göteborgs tingsrätt och nittonåringen dömdes att betala 90 dagsböter a´ 30 kronor. I USA skulle åtalspunkterna räckt till ett 22-årigt fängelsestraff. Nittonåringen var amfetaminmissbrukare och hade sociala problem. Efter domen i Göteborgs tingsrätt togs 19- åringen in för psykiatrisk vård.[48]

Inom vissa delar av privaträtten som kan aktualiseras på och via Internet finns endast lagvalsregler för köp och avtal med internationell anknytning. På övriga områden inom privaträtten där det inte finns särskilda bestämmelser om var ett förhållande har sin starkaste anknytning görs en mer generell bedömning av lagval och de processuella reglerna följer i princip alltid den nationella lagen i domstolens land.

Utlänningars handlingar i utlandet kan sällan beivras i Sverige men däremot kan en svensk inte undgå lagföring i Sverige genom att förlägga handlingen till utlandet. En del regler i andra länder kan vara mer generösa vad gäller attityden till brott av utlänningar. En svensk som begår brott via Internet och som genom förfarandet gjort sig skyldig till brott i ett främmande land kan dömas där trots att vi i Sverige inte skulle ha lagfört en utlänning om

[48] Exemplet hämtat ur tidskriften PC för alla nr 5 oktober 1997 s. 22-24

situationen varit den omvända.[49] Även om en utländsk dom inte kan verkställas i Sverige kan den påverka den dömdes möjligheter att t ex resa till landet.

4.3 Domstols behörighet och verkställighet av domar

Även vad gäller domstolens behörighet tillämpas i grunden en anknytningsprincip och så snart det finns en anknytning till Sverige är svensk domstol behörig men det behöver inte vara den starkaste anknytningen för att en domstol skall vara behörig. En tvist som är prövad och avgjord av svensk domstol men som inte kan verkställas i det land där gärningsmannen befinner sig är i stort verkningslös.

Principer och regler om erkännande och verkställighet av utländska domar varierar utifrån landet ifråga men grundinställningen är att utländska domar saknar rättskraft. I Sverige beror verkställigheten på vad domen eller beslutet handlar om och i vilket land den meddelats. I allmänhet är belägenheten att verkställa utländska domar större om domen grundats på en utländsk lag som i stora drag överensstämmer med motsvarande lag i Sverige.

Domar i anledning av förfaranden som kan aktualiseras på Internet och som är meddelade i länder utanför EES kan sällan verkställas i Sverige och man kan inte räkna med att en svensk dom skall kunna verkställas utanför EES och det är sällan meningsfullt att väcka talan mot en utomeuropé i svensk domstol.[50]

[49] Carlèn- Wendel, s. 36
[50] Carlèn- Wendel, s. 38

4.4 Serverns placering

Frågan om var servern är placerad kan ha betydelse för frågan om jurisdiktionen d v s serverns faktiska geografiska placering. Vid lag och forumval har det ofta betydelse varifrån handlingen företas och det är något helt annat än frågan om var en server rent fysiskt är placerad. Att fylla en server med information är i stort sett lika lätt att göra vare sig servern befinner sig i rummet bredvid eller om servern befinner sig på andra sidan jordklotet. På Internet styrs valet av lagringsplats av pris och tillgång på ledig kapacitet. Ur ren lagvalssynpunkt är dessa val slumpmässiga och irrelevanta för frågan om betydelsen av serverns placering. Om serverns placering skall föranleda rättslig betydelse kommer valet av ”serverland” styras av en strävan att lägga tvivelaktigt material på en server i ett land som kan betraktas som ett ”legalt” paradis.[51]

För att illustrera problematiken kommer här ett exempel. En webbsida på svenska har lagts in av en amerikansk konsult på en server placerad i Spanien. Innehållet kopieras sedan till servrar i fem andra länder på uppdrag av en dansk annonsör som säljer på postorder direkt från Singapore. Här korsas en mängd nationella gränser men trots detta är det väsentliga inte var servern är placerad utan i stället faller valet av jurisdiktion, vad gäller innehållet på webbsidan, där den relevanta handlingen anses företagen och på den ort där den ansvarige har sin hemvist och där själva inmatningen har skett. Med ansvarig menas den person som har kontrollen över innehållet. I detta fallet skulle det relevanta landet vara Danmark och möjligtvis USA.[52]

Vad gäller den civilrättsliga relationen saknar serverns placering betydelse. Om någon upplåter plats på sin dator t ex ett webbhotel, kan i vissa fall ett medverkansansvar föreligga enligt lagen i det land där personen är verksam. Den nationella belägenheten har betydelse vid säkerhetsåtgärder och

[51] SOU 1996:40 s. 192
[52] Carlèn- Wendel, s. 40

exekutiva åtgärder mot själva servern t ex om den skall tas i beslag eller om filer skall raderas men inte heller detta påverkar lag och forumval.

Ett annat exempel är en svensk radiostation som på svenskspråkiga webbsidor på en server i USA sprider antisemitisk propaganda som misstänks stå i strid med den svenska grundlagen.[53] Trots att webbsidorna är placerade på en server i USA kan förfarandet falla under svensk jurisdiktion på grund av att informationen vänder sig till svenskar och den ansvarige är ett svenskt rättssubjekt. Trots att serverns fysiska placering är i USA har det inte någon betydelse för tillämpningen av 2 kap. 2 § BrB eftersom webbsidorna vänder sig till svenskar.

4.5 Sändarlandsprincipen

Sändarlandsprincipen grundas på ett EG direktiv och reglerar jurisdiktionen över TV- sändningar inom den Europeiska Unionen.[54] Bestämmelserna om jurisdiktionen över gränsöverskridande tv-sändningar har implementerats i svensk radio och tv-lagstiftning och principen innebär att lagen i det land varifrån sändningen utgår bestämmer tillämpliga sändningsregler. Oavsett vilken tolkning man ger tv-direktivet är det inte möjligt att analogt tillämpa detta på Internet. I direktivets artikel 1 stadgas att det inte innefattar ”kommunikationstjänster som tillhandahåller data eller andra meddelanden som efterfrågas individuellt såsom telefax, databaser och andra liknande tjänster”.[55] Inom EU har man valt sändarlandsprincipen av skäl och orsaker som inte blir aktuella på Internet samt att inom EU är medlemsländernas lagstiftning någorlunda likartad och förutsägbar.

EG direktivet om radio och televisionssändningar är lätt att tillämpa och upprätthålla samtidigt som det ger ett förutsägbart och meningsfullt resultat vad gäller radio och tv, men förhållandena på Internet är däremot helt

[53] Carlèn- Wendel, s. 41
[54] EG- direktiv 89/552/EEG
[55] EG- direktiv 89/552/EEG

annorlunda och tv direktivet är inte avsett att analogt tillämpas och överföras till Internet. Sändarlandsprincipen är alltså inte bestämmande för lag och forumval på Internet.[56] Radio och tv- bolag är stora och lätta att identifiera och det är relativt enkelt att fastställa varifrån en sändning utgår eller var programföretaget är etablerat.

4.6 Nationell och internationell reglering

4.6.1 Censur av Internet

Att föröka införa censur av utländska och svenska webbsidor med hjälp av en granskningsmyndighet som godkänner respektive underkänner webbsidor skulle innebära en allvarlig inskränkning i våra grundläggande rättigheter och värderingar. Något som däremot diskuteras är att ålägga de svenska Internet leverantörerna en möjlighet att blockera svenskt tillträde till sådana webbsidor som svensk domstol funnit förbjudna. Skillnaden mellan denna form av granskning och censur är att förhandsgranskningen grundas på en i efterhand konstaterad olaglighet och att reglerna är förenliga med de svenska yttrandefrihetsprinciperna. Ur en rent juridiskt perspektiv måste det röra sig om rena spridningsbrott eller alternativt att den berörda Internet leverantören anses som medverkande. Åläggande kan endast komma ifråga vid spridningsbrott eller alternativt i fall då medverkan i sig kan förbjudas eller straffas.

Internet leverantörer som tillåter olagligt material eller tillhandahåller plats och utrymme för sådant på sina servrar riskerar redan idag ansvar för medverkan i vissa fall. Skälet till att det idag är relativt svårt att hålla Internet leverantörerna ansvariga är helt enkelt att det för flertalet brott krävs uppsåt eller för vissa brott oaktsamhet. Det innebär att en Internet leverantör i princip endast kan åläggas ansvar om han är medveten om att olaglig verksamhet förekommer och att han då aktivt bidrar till denna. För att ett sådant system skall fungera och vara hanterligt måste man inskränka den

[56] EG- domstolens domar i målen C- 34- 36/95

svenska lagens tillämpning till förfarande som har en direkt anknytning till svenska intressen och till Sverige.[57]

4.6.2 Självreglering

I några EU medlemsstater har Internet leverantörer tillsammans med systemoperatörer skapat ett system som går ut på ”self regulation”.[58] I Storbritannien har man godkänt en s k ”Code of conduct” en organisation som har till uppgift att undersöka tvivelaktigt material som förekommer på Internet. Systemet är uppbyggt på så sätt att allmänheten kan ringa in eller på annat sätt rapportera material som man anser olagligt. Liknande organisationer är under uppbyggnad i Tyskland och Nederländerna. EU komissionen har välkomnat utvecklingen mot en allt mer omfattande självreglering av det material som förekommer på Internet och upprättandet av ett europeiskt nätverk där Internet leverantörer och systemoperatörer kan samarbeta för att förhindra illegala aktiviteter på och via Internet. Syftet är att man i framtiden skall utveckla det internationella samarbetet där Internet användarna själva kommer att spela en viktig roll i sökandet efter illegala aktiviteter.

En Internet leverantör som upptäcker olagligt material på den egna servern skall vidta åtgärder för att ta bort materialet. Uppgifterna kan komma från vanliga Internet användare i t ex Sverige eller något annat land. Eftersom material som ligger på en speciell server lätt kan kopieras till en annan server i ett annat land måste åtgärden åtföljas av de andra ländernas Internet leverantörer för att nå full verkan.[59] Ett globalt samarbete mellan organisationer, Internet leverantörer och systemoperatörer skulle få stor

[57] Se kapitel 7.
[58] Illegal and harmful content on the Internet. COM (96) 487, Communication to the European Parliment, the Council, the Economic and Social Committee and the Committee of the Regions. www2.echo.lu/legal/en/internet/content/communic.html
[59] Illegal and harmful content on the Internet. COM (96) 487.

genomslagskraft vad gäller att få bort olagligheter från Internet och andra nätverk.
Om olagligt material inte kan plockas bort från servern t ex för att den är placerad i ett land där materialet i sig inte är olagligt kan ett alternativ vara att neka tillträde redan hos Internet leverantörerna. De rent tekniska möjligheterna att blockera tillträdet till vissa servrar är ännu relativt begränsade samtidigt som leverantörernas tillförlitlighet sätts på prov.

Under våren 1997 diskuterades bland svenska nätoperatörer att inrätta en särskild etiknämnd för att lägga fast normer för vad som skall godtas och vilket material operatörerna skall utesluta och spärra från sina tjänster.

4.7 Lag och forumval i upphovsrättsfrågor

I och med att de internationella konventionerna på upphovsrättens område till stor del är överensstämmande är skyddet relativt likartat i de länder som ratificerat konventionerna. Konventionerna reglerar dock inte hur gränsöverskridande nyttjanden skall hanteras och frågorna om lagval och jurisdiktion då får lösas enligt vanliga regler. Frågan om vilket lands lag som skall tillämpas är inte av lika stor betydelse inom upphovsrättens område som inom straffrätten eftersom lagreglerna är relativt likartade i flertalet länder och skyddet är i stort sett detsamma. Vad gäller forumval torde det normala vara att väcka talan i det land där svaranden finns eftersom man då undviker eventuella problem med verkställighet.

I Bernkonventionens artikel 5.2 finns en bestämmelse som stadgar att lagen i det land där skyddet påkallas skall tillämpas. Med detta menas lagen i det land varifrån den otillåtna handlingen t ex en exemplarframställning företagits. Enligt Thomas Carlén- Wendel är det avgörande inte var servern rent fysiskt är placerad utan varifrån handlingen utförts.[60] I vanliga fall är det i det land där den som har kontroll över siten har sitt hemvist. Om en

[60] Carlèn- Wendels, s. 80

webbsida innehåller ett upphovsrättsintrång och den riktar sig personer i ett visst land är lagen i det landet tillämplig.

För domstols behörighet gäller att talan kan väckas i ett land som har anknytning till intrånget. Att en webbsida kan nås från ett visst land är inte i sig tillräckligt för att det skall vara fråga om anknytning. Behörigheten måste föreligga både i det land där handlingen skett och där personen som gjort intrånget har sin hemvist.

5 Intrång i immateriella rättigheter

I och med att informationen digitaliserats har hanteringen av information blivit betydligt lättare både vad gäller spridning, kopiering och bearbetning. Piratkopiering av datorprogram är ett allt mer framträdande inslag inom den ekonomiska brottsligheten. Internet har skapat helt nya förutsättningar för otillåten spridning och kopiering av datorprogram. Program kan göras tillgängliga för var och en via Internet och piratkopieringen av datorprogram anses vara det största problemet när det gäller intrång i upphovsrätten.

Den stora skillnaden mellan den nya digitala tekniken och den gamla analoga är att kopiering kan ske utan någon som helst kvalitetsförsämring och Internet har öppnat oändliga möjligheter att sprida datorprogram och andra upphovsrättsliga alster utan någon som helst kontroll. Detta är en ny form av ekonomisk brottslighet som är mycket svårkontrollerad med de metoder som hitintills använts för att förhindra intrång i upphovsrätten. Samtidigt ligger det mycket pengar i potten både för programtillverkarna som förlorar stora inkomster p g a den olagliga kopieringen, men även för de personer och organisationer som sysslar med illegal tillverkning av programvaran.

Någon definition på vad som är att anse som datorprogram finns inte varken i den svenska upphovsrättslagstiftningen, doktrin eller i förarbeten.[61] Oberoende av definitionen skyddas datorprogrammen oavsett form d v s både den digitala koden och källkoden skyddas av upphovsrätten.

[61] Carlèn- Wendel, s. 75

5.1 Upphovsrättsintrång

Upphovsrättsintrång är straffbart med böter eller fängelse i högst två år om det sker uppsåtligt eller av grov oaktsamhet (53 § URL). Utöver det skall alltid ersättning utgå för nyttjandet och sker intrånget uppsåtligt eller av oaktsamhet skall även skadestånd utgå enligt 54 § URL.

5.2 Upphovsrätten till datorprogram

Datorprogram omfattas av Upphovsrättslagen och skyddas som ett litterärt verk. Upphovsrätten ger innehavaren ensamrätt att framställa exemplar av datorprogram och göra programmen tillgängliga för allmänheten. Speciellt vad gäller datorprogram är all kopiering även för enskilt bruk förbjuden, om man inte har medgivande från rättighetsinnehavaren. Den straffrättsliga sanktionen finns alltså i Upphovsrättslagens 53 §. Vad gäller datorprogram finns det vissa inskränkningar som stadgar att justeringar får göras för att man skall kunna använda programmet på ett riktigt och funktionellt sätt.

Det är tillåtet att framställa brukskopior som är nödvändiga för att praktiskt kunna använda programmet. Således är det tillåtet att kopiera programmet ifrån den Cd - Rom skiva som det levererats på till datorns hårddisk. Det är också tillåtet att göra säkerhetskopior och att använda dessa om informationen på originalfilen skulle förstöras eller raderas. Någon annan kopiering än säkerhets- och brukskopior är inte tillåten om inte licens och avtalsvillkoren i det enskilda fallet medger det. Det är även tillåtet att i viss utsträckning ändra i programkoden och med det menas att man får rätta fel i programmet utan att ha tillstånd från licensgivaren. Det är även tillåtet att ändra i programmet för att få det att fungera tillsammans med andra program.[62]

Undantagsvis kan licensvillkoren ge köparen rätt att använda programmet både i en stationär och i en bärbar dator under förutsättning att det klart

[62] Carlèn- Wendel, s. 76

framgår av licensavtalet. När det gäller kopiering för enskilt bruk är kopiering under vissa förutsättningar inte straffbart. Förutsättningarna är att varken originalet eller kopian används i näringsverksamhet eller offentlig verksamhet. Det skall vara fråga om en rent privat användning och det skall vara ett original som används vid kopieringen.

5.3 Internationella överenskommelser

Genom territorialitetsprincipen anses immateriella rättigheter vara exklusiva och nationella varför den svenska upphovsrättsliga lagstiftningen först och främst skyddar svenska verk.[63] De nationella lagarna har i mångt och mycket samma innehåll beroende på de internationella överenskommelser och konventioner som finns på området. Likabehandlingsprincipen innebär att Sverige ger samma skydd åt utländska verk och deras rättighetsinnehavare som åt svenska. Upphovsrätten är av mycket internationell karaktär och det finns ett stort intresse att samarbeta för att uppnå effektiva internationella bestämmelser och för att få ett fungerande rättsskydd även utanför de olika nationernas gränser.

Det finns ett antal internationella konventioner på området för att tillgodose dessa intressen och viktigast är Bernkonventionen (för skydd av litterära och konstnärliga verk från 1886, senast ändrad 1970) samt Romkonventionen (om skydd för utövande konstnärer, fonogramframställare och radioföretag från 1961). Konventionernas administration sköts av FN organet WIPO som arbetar med att åstadkomma en internationell samsyn på information i digital form.[64]

Under 1996 antogs två nya konventioner dels WIPO Copyright Treaty och dels WIPO Performances and Phonograms Treaty.[65] I båda konventionerna finns preciseringar av vilka upphovsrättsregler som gäller för datorprogram och databaser. WIPO Copyright Treaty stadgar att datorprogram skall

[63] Koktvedgaard/Levin, Lärobok i immaterialrätt, s. 37, 281
[64] WIPO är en förkortning för World Intellectual Property Organisation. WIPO är en s k ”Specialized Agency” under FN. För närvarande har organisationen ca 150 medlemsländer.
[65] Författningstext.

skyddas som litterära verk och att samma regler skall gälla för samtliga stater som ratificerat konventionen. Detta innebär att utländska domar kan komma att användas för att tolka upphovsrättsreglerna. WIPO Copyright Treaty behandlar också behovet av att kunna skydda de tekniska anordningarna som används för att skydda information i digital form t ex kopieringsskydd av programvara. Enligt konventionen blir det olagligt att bryta kopieringsskydd och liknande anordningar som anbringats för att skydda digitalinformation mot olaglig kopiering. En grundregel är att den som utvecklat och bekostat programvaran, bilden eller texten har en exklusiv rätt att göra produkten tillgänglig för allmänheten ”by wire or wireless means, including the making available to the public of their in such way that members of the Public may access them from a place and at a time individually chosen by them”.[66] Regeln omfattar distribution över Internet. En harmonisering av lagstiftningen gör det lättare för programvaruföretag och användare att ta reda på vilka regler som gäller i olika länder detta för att undvika att något visst land p g a sin lagstiftning blir tillflyktsort för piratkopiering av datorprogram.

5.4 Olaglig kopiering

På Internet finns det ett stort antal databaser där man kan hämta piratkopierat material. Databaserna fungerar som BBS:er och innebär att personer skickar in material som lagras på BBS:en och blir tillgängligt för alla andra besökare att hämta hem.[67] En person som skickar upp andras upphovsrättsligt skyddade material till en BBS för sig skyldig till upphovsrättsintrång.

Att hämta hem material från en BBS för enskilt bruk är däremot inte otillåtet såvida det inte är datorprogram som hämtas hem. Att hämta hem datorprogram är otillåtet även om det sker för enskilt bruk. För

[66] Författningstext.
[67] De elektroniska anslagstavlorna kallas också Bulletin Board Systems och är en kombination av en databas och en datoriserad anslagstavla med möjlighet för entusiaster att kommunicera med varandra, uppg hämtad ur Carlèn- Wendels, s. 15

rättighetsinnehavaren är det i stort sett omöjligt att försöka identifiera de tusentals bidragsinsändarna för att beivra den otillåtna spridningen via BBS:en.

I praktiken kan den olagliga kopieringen av datorprogram delas upp i tre olika kategorier.[68]

a. Den olagliga kopieringen som görs av slutanvändare.
b. Olaglig kopiering via traditionell distribution vanligtvis genom hårddiskinstallation från Cd - ROM och disketter.
c. Den olagliga kopieringen som sker via elektronisk distribution genom databaser och elektroniska anslagstavlor på Internet.

5.4.1.1 Olaglig kopiering som görs av slutanvändare

Ett typiskt fall är att ett företag, myndighet eller annan organisation kopierar och använder programvaran i större utsträckning än vad licensen tillåter. En organisations användning av programvara kan delas upp i nätverksanvändning och ”stand-alone” användning.[69] Detta utesluter i sig inte en viss nätverksanvändning t ex för att spara utskrifter och filer. Ett nätverk kan användas som distributionsform för stand-alone användning d v s att användare laddar ner programvara från nätverkets server till den egna datorns hårddisk. Nätverksanvändningen innebär att programvaran finns på nätverkets server och att persondatorn eller arbetsstationen arbetar med programvaran från servern.

Beräkningen av hur stor användning som är tillåten vid nätverksanvändning varierar beroende på vad som regleras i licensavtalet. Ett av alternativen är att omfattningen av licensen anges i antal samtidiga användare d v s det kan finnas ett större antal personer som har tillgång till programmet men det avgörande är hur många personer som samtidigt använder programmet. Ett annat alternativ är att man räknar hur många användare som har tillgång till

[68] IT- Kriminalitet- checklista för målsägare (Broschyren är ett samarbete mellan IT-företagen, Buisness Software Alliance BSA, Larmtjänst och Rikskriminalpolisen)
[69] ”Stand alone”- användning innebär att programvaran installeras på en enskild dators hårddisk och används direkt på datorn

programmet oavsett hur många som faktiskt använder det. Licenserna kan också variera något från dessa två alternativ.

Ett typiskt fall av slutanvändare som gör sig skyldig till olaglig kopiering är en organisation som installerar fler program än vad man har licens till eller att nätverksanslutningen överstiger den avtalade. I vissa fall finns licensavtal men i andra saknar slutanvändaren helt licens.

På Internet gäller samma upphovsrättsregler som tillämpas på litterära och konstnärliga verk i övrigt. En av skillnaderna mellan datorprogram och andra verk är att det som skyddas hos datorprogrammet är algoritmen d v s funktionen och strukturen hos programmet och inte i sig den litterära eller konstnärliga aspekten.[70] En textfil eller en digitaliserad bild utgör inte i sig ett datorprogram på grund av att de är maskinläsbara utan istället är de att anse som vanliga litterära och konstnärliga verk som lagrats i digital form på en dator.

5.4.1.2 Traditionell distribution

5.4.1.2.1 Hårddiskinstallation

Den vanligaste formen av traditionell distribution är hårddiskinstallation. I Sverige finns det en förhållandevis stor tillverkning av datorer och det förekommer att försäljare installerar programvara, framförallt operativsystem på nya datorers hårddiskar, utan att originallicenser medföljer. Vad som skall följa med i en originallicens varierar givetvis beroende på programvaruleverantören men normalt levereras alltid ett licens- eller äkthetsbevis.

[70] Carlèn- Wendel, s. 75

5.4.1.2.2 Counterfeit/ Cd tillverkning/ Floppy (Disk)

Med counterfeit menas direkta kopior av programvara, programmedia, dokumentation och eventuellt licensavtal och licensbevis.[71] I allt större utsträckning sker kopieringen på Cd - skivor eftersom de i större utsträckning används av programvaruleverantörerna för att distribuera programvaran. Kopieringen omfattar i princip hela produktpaketet, manualer, samt förpackning och det kan vara mycket svårt för en kund att skilja kopian från originalet. De flesta programvaruleverantörerna har dock olika kännetecken på programvaran som kan vara dolda eller svåra att kopiera t ex hologram.[72]

Produktionen av Cd - skivor med olagliga kopior av programvaror har kraftigt ökat i Sverige och en bidragande orsak till detta är att tekniken för att producera egna skivor med s k Cd - brännare har blivit mycket billig. Skillnaden i kvalité mellan original och kopia vad gäller datorprogram är obefintlig och det sker i stort sett ingen som helst försämring vid kopieringen från originalet. Cd - skivor med olagligt kopierad programvara kan innehålla program för 10 000- tals kronor och marknadsföringen av Cd - skivorna sker genom annonsering i dagspressen, Gula Tidningen och text-TV. Marknadspriset för en Cd - skiva med program för 10 000- tals kronor är normalt mellan 600- 800 kronor och vanligtvis anges endast ett mobiltelefonnummer i annonsen dit intresserade kan vända sig för beställning.[73]

Programkopiering via vanliga disketter var tidigare vanligt förekommande men har alltmer ersatts av kopiering på Cd - skivor. Tillvägagångssättet är i stort detsamma för Cd - skivorna förutom att disketternas minneskapacitet är

[71] Counterfeit är det engelska begreppet och betyder förfalskad, oäkta

[72] Möjligheterna att förfoga över datorprogram är i stor utsträckning beroende av avtals-/licensvillkoren som säljaren/rättighetsinnehavaren ställt upp. Särskilt vid programvaruförsäljning har bruket av wrap klausuler (förseglings eller omslags- klausuler) blivit vanligt förekommande. Det innebär att avtalsvillkoren finns skrivna på programvaruförpacknigen och anger att köparen accepterar villkoren, vanligtvis licensvillkoren, genom att bryta förpackningen. En annan variant är att villkoren finns inlagda i ett installationsprogram där användaren förutsätts att acceptera villkoren genom att klicka på en ”accept” knapp innan installationen påbörjas.

[73] IT- kriminalitet- checklista för målsägare, s. 8

betydligt mindre än Cd - skivans vilket innebär att det krävs flera disketter för ett enda program.

De svenska IT företagens organisation SITO har framhållit att den omfattande piratkopieringen leder till förluster för näringslivet och till en omfattande administration från näringslivets sida för att ingripa mot piratverksamhet. Enligt SITO finns det möjlighet att öka det tekniska skyddet t ex genom krypterade signaturer. Även polis och andra myndigheter måste utveckla sin kompetens vad gäller IT frågor samtidigt som frågorna måste få en högre prioritet.[74] Behovet av spetskompetens kommer troligtvis att öka.

5.4.1.3 Elektronisk distribution

En distributionsform som snabbt sprider sig är förmedlingen av information via databastjänster. Det kan handla om traditionella elektroniska anslagstavlor, Bulletin Board System, eller databaser som är tillgängliga via Internet. Databaserna används för förmedling av elektronisk post och annan information men det är även möjligt att distribuera programvara genom databaser.

En elektronisk databas kan beskrivas som en dator som via modem och telenät (även Internet) kan stå i förbindelse med andra datorer. De som driver en databas kallas för systemoperatörer. Användarna kan skicka datafiler, inklusive programfiler, till databasen genom s k upload och systemoperatören kan lägga in filer i databasen som görs tillgängliga för andra.[75] Elektroniska databaser kan användas för olaglig kopiering samt olovlig spridning av programvaror. Ofta rör det sig om nya program som ibland inte ens är utgivna.

[74] Ds 1997:51 s. 105

[75] ”Upload” innebär att man lägger upp information på en server eller databas och på så sätt gör det möjligt för andra användare att genom s k ”download” hämta hem t ex programvara och datafiler till den egna datorn.

5.4.1.3.1 Elektronisk distribution via Internet

Det amerikanska företaget LucasArts Entertainment Co i San Rafael råkade den 6 juli 1994 ut för ett allvarligt upphovsrättsintrång. Företaget hade precis avslutat arbetet med ett nytt program som skulle lanseras den 20 juli 1994 då en av företagets anställda via sin PC och sitt modem skickade en fullständig kopia av programmet till en adress på Internet. Det enda som saknades var dekrypteringsnycklarna för att låsa upp koderna som krävdes för att vidarekopieringen skulle kunna ske helt obehindrat.

Bakom Internet adressen stod en grupp hackers som inom ett par minuter via Internet vidarebefordrade programmet till en server i Moskva där en rysk systemoperatör dekrypterade koderna och sedan skickade programmet tillbaka till USA via Internet. När programmet kommit tillbaka lades det upp på en server i USA och gjordes på så sätt tillgängligt för Internet användare över hela världen att ladda ner. Inom 24 timmar från det att den anställde på företaget hade skickat informationen från sin dator fanns hela programmet tillgängligt på Internet, dekrypterat och färdigt att använda, och detta tre veckor innan den egentliga lanseringen.[76]

5.5 Kontrollsystem

Det är till stor del en rent teknisk fråga om man i framtiden skall kunna begränsa spridningen av upphovsrättsligt skyddade datorprogram. Digital lagring och överföring skapar nya möjligheter att skydda program genom att bygga in osynliga koder med ursprungsinformation och andra tekniska styrmedel i programmen. En möjlighet är att lägga in en personlig id kod i programmet. Koden registreras hos tillverkaren som har en server som regelbundet scannar Internet och rapporterar i vilken utsträckning det förekommer kodade program.[77] I framtiden kan alla webbläsare komma att innehålla moduler som automatiskt identifierar verk som finns på webbläsaren.

[76] Uppgifter i Los Angeles Times 1994-11-03.

5.6 Internationell omfattning

Business Software Alliance (BSA) är en branschorganisation för programvaruindustrin och enligt BSA:s statistik var 47% av programvarorna som användes i Sverige 1996 olagliga.[78] BSA har beräknat följande förluster p g a piratkopiering av datorprogram globalt och i Europa.

- ***Hela världen*** ca 12 miljarder ecu[79]
- ***Hela Västeuropa*** ca 4,8 miljarder ecu
- Tyskland ca 1,5 miljarder ecu
- Frankrike ca 0,6 miljarder ecu
- Storbritannien ca 0,4 miljarder ecu
- Italien ca 0,3 miljarder ecu
- Spanien ca 0,2 miljarder ecu
- **Sverige ca 0,1 miljarder ecu**
- Belgien ca 0,06 miljarder ecu
- Portugal ca 0,04 miljarder ecu[80]

I förhållande till den tekniska utvecklingen och samhällets datorisering är det fortfarande relativt lätt att kopiera och sprida datorprogram. Den privata kopieringen för eget bruk förekommer i mycket stor utsträckning och kan därvid göras tillgängliga för varje datoranvändare via Internet. Det förekommer även en omfattande marknadsföring av piratkopior i organiserade former.

5.7 Upphovsrätten på Internet

På Internet gäller samma upphovsrättsregler som i samhället i övrigt och det är naturligtvis tillåtet att surfa på Internet och ladda ner och titta på text, bilder och i viss mån musik oavsett det att den egentliga exemplarframställningen föreligger redan då det elektroniska dokumentet tas emot av datorn som används.

---

[77] Carlèn- Wendels, s. 84
[78] Microsoft Magazine nr 1-1997 s. 69
[79] En ecu är ungefär 8 svenska kronor.

Detta beror dels på att det sker för eget bruk och att rättighetsinnehavaren får anses medge exemplarframställningen som uppkommer då man tittar på eller laddar ner bilder t ex från Internet. Däremot är det inte utan vidare tillåtet att permanent lagra alster på hårddisken framförallt inte på t ex ett företags server. Även utskrifter från en skrivare med sådana alster är beroende av dels var gränsen för enskilt bruk går och dels vad den egentliga rättighetsinnehavaren kan anses ha medgivit genom att lägga upp materialet på Internet.[81] Att skicka och ladda upp information och annat upphovsrättsligt skyddat material till en offentlig databas eller en BBS är i princip alltid förbjudet framförallt vad gäller datorprogram och andra digitala kataloger.

En person som lägger ut information på webbsidor och i databaser måste till viss del inse att möjligheterna att kontrollera och beivra upphovsrättsintrång fortfarande är relativt begränsade. Med utgångspunkt i detta är det av stor vikt att den som lägger upp information på Internet inte själv begår upphovsrättsintrång genom att lägga in redan skyddade verk i sina alster utan att ha tillstånd att göra så. En person som driver en databas eller en BBS som är tillgänglig för allmänheten att besöka torde ha ett ansvar som medverkande vid eventuella upphovsrättsintrång som förekommer i materialet på servern.[82]

5.8 BBS-målet

I ett HD avgörande från 1997 det s k BBS målet var frågan om en databas till vilken allmänheten kunde sända in bl a upphovsrättsligt skyddade datorprogram som därigenom blev tillgängliga för andra att hämta hem. HD fann att systemoperatören inte var ansvarig för de upphovsrättsintrång som skedde på hans databas eftersom han, enligt vad som framkommit i målet, inte aktivt befattade sig med materialet.

---

[80] Ds 1997:51 s. 105
[81] Carlèn- Wendel, s. 81-82 ff.

BBS målet är omdiskuterat och kritiserat och man bör inte dra alltför långtgående slutsatser av fallet. Om systemoperatören däremot aktivt flyttat omkring de inskickade programmen från en uppload till en download area eller på annat vis granskat och valt vilka av de inskickade programmen som skulle göras tillgängliga för allmänheten skulle antagligen utgången blivit en annan.[83] De personer som skickat in upphovsrättsskyddat material till BBS:en torde alla ha gjort sig skyldiga till upphovsrättsintrång. Deras ansvar var dock inte föremål för prövning i målet.

[82] Se kapitel 7.
[83] Se fotnot nr 75, vad gäller begreppen upload respektive download.

6 Elektroniska betaltjänster och elektroniska pengar

Betalningsförmedling innebär att någon t ex en bank åtar sig att föra över pengar från en gäldenär till en borgenär.

6.1 Betalningsförmedling grundar sig på:[84]

- en betalningsanvisning t ex en check eller ett kontokorts nota

eller

- ett betalningsuppdrag t ex gireringar över post- eller bankgiro.

En betalningsanvisning kan vara elektronisk och som exempel kan anges vissa betalningar med kontokort och med s k förbetalda kort. Även betalningsuppdrag kan vara elektroniska såsom överföringar mellan konton i en bankomat eller per telefon.
Elektroniska pengar förekommer i form av förbetalda kort eller s k cyber money. Detta innebär att värdeenheter laddas på ett kontantkort, på en dator eller på en diskett. Betalning kan sedan ske med kortet eller från en dator.
Betaltjänstutredningen har i sitt betänkande Betaltjänster föreslagit att de betaltjänster som tillhandahålls allmänheten yrkesmässigt skall lagregleras näringsrättsligt och civilrättsligt.[85]

Lagen föreslås gälla för betalningsförmedling och andra betaltjänster som utförs med hjälp av kontokort, personlig kod eller annat legitimationsmedel som hör till kontot men även växel och check i de hänseenden dessa inte regleras särskilt i växellagen och checklagen. Näringsrättsligt föreslås att betaltjänster skall uppfylla vissa kvalitetskrav och krav på betalningsredskap och att den normala revisionen i företaget också skall innefatta betaltjänsternas funktion och säkerhet. Civilrättsligt krävs att information

[84] Ds 1997:51 s. 77
[85] SOU 1995:69 s. 170

skall lämnas till kunderna vid marknadsföring och avtal om betaltjänster.[86] Vidare ges särskilda regler om ansvaret för obehörigt utnyttjande av kundens konto och den betalningstjänstansvariges skyldigheter i samband med utförandet av tjänsten.

Utvecklingen inom elektroniken och datateknikens områden har gått mycket snabbt under de senaste åren och ett exempel på detta är den ökade användningen av ”smarta kort”, d v s plastkort försedda med en integrerad elektronisk krets som gör det möjligt att ladda betydande mängder information. Korten kan även utföra vissa beräkningar och logiska operationer.[87]
Ett annat exempel är det kraftigt ökade utbudet av varor och tjänster på Internet. Inom det finansiella området har utvecklingen medfört att nya former för betalningar skapats genom tillkomsten av elektroniska pengar.

Man brukar dela in betalningar med elektroniska pengar i två kategorier dels sådana som utförs med smarta kort d v s kontantkort och dels sådana som utförs via datornät med värdeenheter som laddats på en diskett eller på hårddisken i en dator.[88]

6.2 Kontantkort

Kontantkortet innehåller information om att kortet kan användas för betalningar upp till ett visst belopp och kortet laddas med elektroniska enheter motsvarande ett bestämt värde i pengar. Kortet kan sedan användas för betalning av varor och tjänster hos betalningsmottagare som innehar den nödvändiga tekniska utrustning som krävs. Betalningsmottagaren vänder sig i sin tur till den som utfärdat enheten för att lösa in de elektroniska enheterna mot kontanter. Varje gång en betalning sker med kortet minskar

[86] SOU 1995:69 s. 176
[87] Dir 1997:1
[88] För båda kategorierna av kort gäller att utfärdarna i regel kräver betalning i förskott för de värdeenheter som laddas på korten.

antalet enheter med motsvarande belopp. Vissa kontantkort kan sedan laddas upp på nytt sedan de elektroniska pengarna tagit slut. Kontantkorten kan vara anslutna till ett öppet eller ett slutet system. I det slutna systemet kan det värde som finns reserverat på kortet bara användas för betalning hos en eller ett fåtal betalningsmottagare.[89] I det öppna systemet kan kontantkorten användas för betalning hos en större krets av mottagare. De öppna systemen för kontantkort finns i bl a Danmark, Belgien, Nederländerna, Frankrike, Italien, Finland, Portugal, och Storbritannien. I merparten av dessa länder tillhandahålls systemen av banker. I Danmark, Belgien och Frankrike är det emellertid möjligt även för andra företag än banker att tillhandahålla öppna system.[90]

I Sverige har användningen av kontantkort i huvudsak varit begränsad till kort av engångskaraktär i slutna systemen. Under 1996 lanserade Sparbanken och Nordbanken i samarbete ett öppet system för kontantkort i Halmstad och Uppsala. Avsikten är att systemet skall introduceras i hela Sverige under 1997-1999.

För betalningsmottagarna inom handeln innebär kontantkortet att kostnaderna för hantering av sedlar och mynt minskar samtidigt som risken för rån kraftigt reduceras. För kortinnehavaren innebär det att han slipper att ha kontanter på sig och istället kan använda kortet i butiker. I de flesta länder är rätten att utfärda kontantkort förbehållen banker och olika kreditinstitut. Frågan om vilka institut som skall ha rätt att utfärda elektroniska pengar hänger nära samman med frågan om vilken rättslig status dessa pengar skall ha.[91] Syftet med de elektroniska pengarna och framförallt kontantkorten är ju att ersätta kontanter och förenkla hushållens betalningsrutiner. De flesta system för kontantkort har planerat att sätta en högsta gräns för det belopp som kan laddas på kortet men troligtvis finns det ingenting som i framtiden hindrar att korten laddas med obegränsade belopp. Elektroniska pengar behöver inte vara knutna till en viss person eller ett speciellt individuellt konto men däremot kan den som utfärdat korten av

[89] Ett exempel på ett sådant kort är Telias vanliga telefonkort.
[90] Dir 1997:1

kontrollskäl vilja ha ett system som ger möjlighet att följa transaktionerna på ett enskilt kort.

6.3 Elektroniska pengar på datorn

Elektroniska pengar kan också bestå av värdeenheter som laddas på en diskett eller på hårddisken på en dator.[92] En person kan med sin dator via Internet köpa varor och tjänster och betala med de värdeenheter som finns laddade på disketten eller hårddisken. Härigenom öppnas nya vägar och möjligheter att utan förmedling av bank eller företag göra överföringar och betalningar via datornätet eller direkt mellan två datorer. Det blir allt vanligare att banker och andra kreditinstitut erbjuder sina kunder vissa finansiella tjänster via elektroniska förmedlingstjänster.[93] Vanligtvis rör det sig om sådana tjänster som även kan utföras via telenätet som överflyttning av pengar mellan olika konton. Arbete pågår också med att utveckla olika lösningar för att göra handeln samt användningen av konto eller kreditkort via Internet så säker som möjligt.[94]

6.4 Ökad risk för brottslighet

Ett nytt och effektivare betalningsväsende förutsätter också en hög säkerhet hos de nya systemen. Ju större brister som finns ju större blir risken för att systemens svagheter utnyttjas i brottsligt syfte. Kontokort kan förfalskas på olika sätt med hjälp av Internet. Genom Internet är det möjligt att få tillgång till eller räkna fram äkta kontokortnummer. Genom att lägga in ett äkta kortnummer på ett förfalskat kontokort kan ett förfalskat kort användas som äkta. När kortet dras genom en kortavläsare avkänns kortet som äkta. Denna form av IT brottslighet används i stor skala av kriminella grupper från länder

---

[91] Regeringskansliets referensgrupp för krypteringsfrågor, s. 57
[92] Även kallade cyber money eller network money
[93] ”Home banking” Innebär att en rad tjänster av finansiell karaktär kan skötas från en PC i hemmet. Redan nu är det relativt vanligt förekommande och de flesta banker har numera elektroniska förmedlingstjänster att erbjuda sina kunder.
[94] Se 6.4 och 6.4.1 om de s k SET- systemet.

i framförallt Asien och Afrika. I Sverige har vi hittills varit relativt förskonade från denna typ av kontokortsbedrägerier men även vi i Sverige kommer med största sannolikhet att få se en ökning av denna typ av brottslighet.

En liknande kriminalitet är telefonbedrägerier som innebär att en vara beställs på telefon med obehörigt åberopande av kontokortnummer för betalning. Även dessa bedrägerier bygger på att det är möjligt att få tillgång till de äkta kontokortnumren. I Sverige är dock handeln via telefonorder relativt begränsad. De svenska företagen har av konkurrensskäl blivit tvungna att alltmer acceptera sådana betalningsformer och som en följd av detta kan man förutsätta att telefonbedrägerierna kan komma att bli ett allt större problem även i Sverige.[95]

Det finns även brott med kontokort som förutsätter en viss medverkan från butikssidan. Ett exempel på detta är att använda ett kontokortunderlag utan yttre text eller märkning men med en magnetiskt inlagd kod. När kortet dras igenom avläsaren luras det elektroniska kontrollsystemet av den ”äkta” magnetiska koden trots att kortet i sig ser annorlunda ut. En förutsättning för att lyckas är att den som betjänar kunden spelar med och lämnar ut varor eller kontanter trots att kortets utseende visar att det inte är äkta.

Den omfattande utvecklingen och satsningen på elektronisk handel både i USA och inom EU kommer med stor sannolikhet leda till att den ekonomiska brottsligheten ökar. I en rapport framlagd i april 1997 av The Financial Action Task Force varnas för att hastigheten, säkerheten och anonymiteten i de nya Internet betalningarna medför att myndigheternas och de rättsvårdande institutionernas traditionella metoder för att lösa bedrägerier och förskingring tappar i effektivitet.[96] Ett av kraven är att bankerna skall åläggas en större upplysningsplikt om man upptäcker misstänkta betalningar. De ökade möjligheterna till kryptering medför att myndigheternas resurser för brottsspaning i samband med denna typ av brott

[95] Ds 1997:51 s. 80
[96] Financial Action Task Force består av experter från 26 länder.

minskar. Även de juridiska frågorna vad gäller elektroniska pengar och betaltjänster ställs i viss mån på sin spets. Handel med elektroniska pengar innebär ju att en digital summa pengar övergår från person A till person B samtidigt som A:s konto minskas med motsvarande summa. Detta medför att man måste kunna förhindra dubbelspenderingar. En av de viktigaste frågorna att lösa är hur digitala signalmönster för elektroniska pengar skall kunna kopieras via nät samtidigt som de skyddas mot otillåtna dubbelspenderingar. Det råder en viss tvekan om elektroniska pengar kan stjälas på samma sätt som sedlar, mynt och checkar eftersom de närmast har karaktären av att vara immateriella.[97]

De vanligaste kontokorten utfärdas i många fall av stora kontokortföretag med en global verksamhet och av dessa är Visa det största.[98] I dag är ca 20.000 banker över hela välden anslutna till Visa och det totala antalet visa kort i världen var 1994 ca 390 miljoner. Dessa 390 miljoner kort accepteras av 10 miljoner säljföretag i 205 länder.[99] Ett krav för att systemen med betalkort skall fortsätta att fungera är att säkerheten anpassas efter utvecklingen inom IT området. Kontokortföretagen lägger mycket arbete på att höja säkerheten i de system som används och det sker genom ett internationellt samarbete mellan banker och företag. Ett av problemen med att utveckla pålitliga och säkra system är att lagstiftningen och den tekniska skyddsnivån varierar mellan de olika länderna. Detta medför att man i vissa läder trots allt varit tvungna att använda sig av en lägre säkerhetsnivå. Nedsatt säkerhet i vissa länder får inte bara konsekvenser där utan även i andra länder eftersom kriminella grupper satt i system att använda kontokort i andra länder för att på så sätt lättare kunna kringgå säkerhetsrutinerna.

Vid en jämförelse med Sverige kan man konstatera att Sverige är ett av få länder där kontokorts användare regelmässigt måste visa legitimation i samband med att kortet används. I en del andra länder anses det som en ohövligt gentemot kunden att begära legitimation och dessutom kan kunden

[97] Regeringskansliets referensgrupp för krypteringsfrågor, s. 57
[98] Visa är en ideell förening som består av banker och andra närstående företag.

inte alltid förutsättas ha med sig legitimation. Den svenska identitets kontrollen medför att säkerheten hålls på en hög nivå i Sverige jämfört med övriga länder. Både från polishåll och från kontokortbranschen har det sagts att det största hotet i framtiden när det gäller det brottsliga användningen av kontokort är att de kriminella grupperna skaffar sig kontakter inne i banker och företag för att få hjälp med att komma förbi de allt mer avancerade säkerhetssystemen.

6.5 Säkrare betalningar på Internet

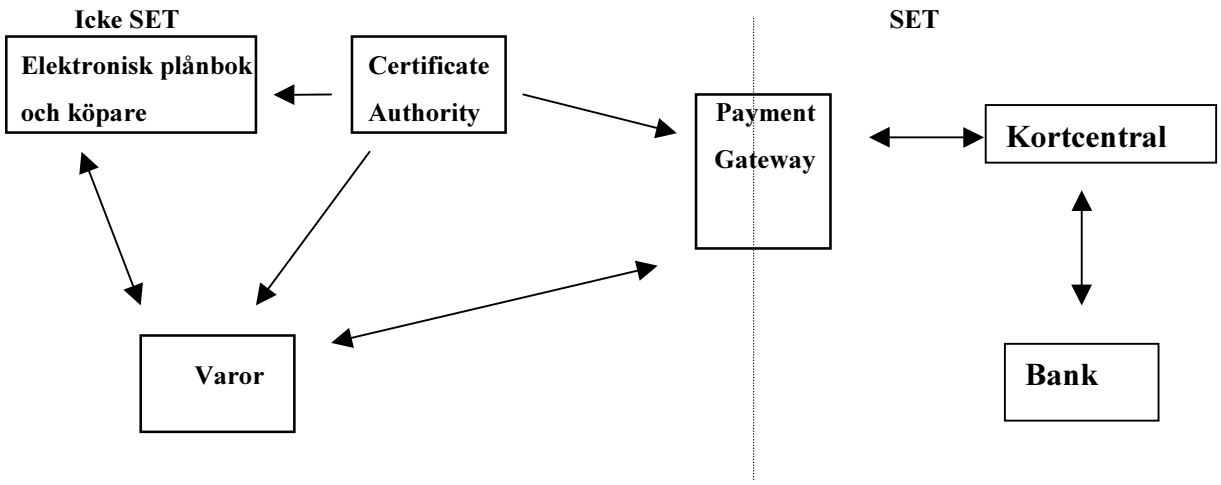
Många Internet användare, banker, finansinstitut och leverantörer väntar på nya och säkrare systen för att kunna göra betalningar via nätet. Med ett större säkerhetstänkande och bättre system kan den elektroniska handeln utvidgas och göras tillgänglig för alla. Vad som är speciellt intressant för marknaden är att även småbelopp kan debiteras på ett säkert och kostnadseffektivt sätt.

[99] Ds 1997:51 s. 79

6.4.1 SET- systemet

SET är en ny öppen standard avsedd för betalkorthandel via öppna nätverk såsom Internet.[100] SET är ett nytt system som möjliggör kryptering av kontokortsinformation och som skall kunna säkra de betalningar som görs via Internet. SET har tagits fram av Mastercard och Visa tillsammans med en rad olika dataföretag som Netscape, IBM och Microsoft. Den första versionen av SET lanserades i maj 1997 och var fri och öppen för alla att använda.[101] Under hösten 1998 kommer en ny version att lanseras som gör det möjligt att använda aktiva kort anslutna till en dator via en speciell kortläsare.

SET- Systemets aktörer[102]



Visa och Mastercard har enats om en ny standard för hur datachipsbaserade kontokort skall vara utformade. Iden bakom det nya systemet är att köparens PC och säljarens dator med stöd av s k SET protokoll skall kunna definiera SET transaktioner, som begäran om köp, säljtransaktioner och annat för affärer över Internet. Vad som händer är att betalningen dras av från köparens kredit eller betalkonto på dennes bank. Säljarens dator är ansluten via en Payment Gateway till sin egen bank. Köparen skaffar ett speciellt

[100] SET står för Secure Electronic Transaction.
[101] Regeringskansliets referensgrupp för krypteringsfrågor, s. 30
[102] Skissen hämtad från Kryptopolitik- möjliga svenska handlingslinjer, oktober 1997

kredit- eller betalkort som för att vara giltigt måste förses med ett certifikat som utges av ett speciellt certifieringsorgan. Detta certifikat innehåller köparens nyckel d v s en kryptografisk kod för just det speciella kontokortet, giltighetstiden för den öppna nyckeln, giltighetstiden för köparens privata nyckel, och identifikation av den digitala signaturen för den som utfärdat certifikatet.[103]

Den stora fördelen med systemet är att banken kan ge säljaren tjänsten garanterad betalning på just de SET transaktioner som säljaren själv godkänner. SET systemet innebär en stor fördel eftersom varken kortnummer eller kontonummer sänds i klartext via Internet. Köparen vet vem som är säljare men handlar anonymt i förhållande till säljaren som inte kan se kortnumret. Säljaren kan endast dekryptera den information som krävs för att leverera varan eller tjänsten. Inte heller banken får reda på vilka varor som köparen har beställt och varorna kan levereras till vilken adress som helst. Systemet innebär att köparens risk reduceras och köparen kan på sedvanligt sätt vid betalning via betalkort begära att ett visst debiterat belopp återförs till kontot om det blivit något fel.[104] Anledningen till att jag tagit med detta helt nya system är att det väntas få stor betydelse för den framtida användningen av kryptografi inom betalningsväsendet. Visa tillsammans med Mastercard har en kundkrets på 800 miljoner användare och 25 000 banker över hela världen är anslutna till det betalsystem som de båda har infört. Det är mycket sannolikt att det är SET systemet som i framtiden kommer att vara standard vid betalningar över Internet och andra nätverk.

6.5.1 Pilotprojekt

I Danmark pågår ett pilotprojekt med en äldre version av SET systemet och i försöket deltar bland annat IBM, Mastercard och den danska betalningscentralen PBS. I oktober 1996 inledde Visa och 38 banker från 16 europeiska, därav 4 nordiska, ett stort gemensamt pilotprojekt för tillämpning av det nya systemet. I Sverige förbereder Handelsbanken, Postgirot, SE-banken, Sparbanken Sverige tillsammans med Visa ett projekt

[103] Regeringskansliets referensgrupp för krypteringsfrågor, s. 30- 31 ff.

som skall ingå i ett större europeiskt försök och man beräknar att försöksverksamheten skall komma igång under januari 1998.

I Sverige har man valt IBM som leverantör av den gemensamma s k Payment Gateway och 8000 kunder med Visa kort från någon av de fyra bankerna skall kunna betala med sitt kort i de 30-tal Internet butiker som skall anslutas till projektet.

[104] Regeringskansliets referensgrupp för krypteringsfrågor, s. 30- 31 ff.

7 Förslag till lag om ansvar för elektroniska anslagstavlor

7.1 Lagförslag[105]

Tillämpningsområde

1 § *Denna lag gäller elektroniska anslagstavlor. Med en elektronisk anslagstavla avses i denna lag en tjänst för elektronisk förmedling av meddelanden. I lagen avses med meddelande text, bild, ljud, eller information i övrigt.*

2 § *Lagen gäller dock inte*

1. *tillhandahållande endast av nät eller andra förbindelser för överföring av meddelanden eller av andra anordningar som krävs för att kunna ta i anspråk ett nät eller annan förbindelse,*
2. *förmedling av meddelanden inom en myndighet eller mellan myndigheter eller inom ett företag eller en koncern,*
3. *tjänster som skyddas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen, eller*
4. *meddelanden som är avsedda bara för en viss mottagare eller en bestämd krets av mottagare (elektronisk post).*

7.1.1 Elektroniska anslagstavlor

Ett datanät består av datorer och annan teknisk utrustning som sammankopplats så att data kan överföras från ett ställe till ett annat. Ett datanät kan vara konstruerat antingen för digitala eller analoga signaler. Ett nät som är konstruerat för att överföra analoga signaler kräver ett modem för att kunna översätta digitala signaler till analoga och tvärtom.

[105] Prop. 1997/98:15

En elektronisk anslagstavla eller förmedlingstjänst kan i stort jämföras med vad som på engelska kallas Bulletin Board System. BBS är en dator eller server dit allmänheten eller speciellt utvalda personer med accesskoder kan sända in egna meddelanden och ta del av vad andra användare sänt in. Den vanligaste formen av tjänst är konferenssystem som består av en databas där användare kan lägga in meddelanden och se vad andra skrivit. I en del fall har konferenssystemet en moderator med befogenhet att ta bort meddelanden. Grupperna av användare kan vara öppna eller slutna d v s öppna endast för vissa användare. En del av tjänsterna bedrivs genom att man använder distributionslistor.[106] I begreppet elektroniska meddelanden innefattas inte bara text utan även rörliga bilder och ljud. Ett meddelande på en elektroniska anslagstavlor lagras på ett sätt som gör det enkelt att söka efter informationen man vill komma åt. Det enklaste sättet att organisera anslagstavlorna är genom att hänvisa till vissa meddelanden. Hänvisningar kan göras på två olika sätt dels genom menyer som består av listor över dokument som användaren kan använda och dels genom hyperlänkar där texten i dokumentet innehåller klickbara fält som i sin tur leder vidare till andra dokument.[107]

Information till användarna

3 § *Den som tillhandahåller en elektronisk anslagstavla skall lämna information till var och en som ansluter sig till tjänsten om sin identitet och i vilken utsträckning inkomna meddelanden blir tillgängliga för andra användare.*

[106] Distributionslistor är en tilläggsfunktion till e- post och innebär att en avsändare istället för att sända in meddelandet till ett antal uppräknade mottagare sänder det till distributionslistans elektroniska adress. Listans adress leder vidare till en automatiskt fungerande enhet som styrs av en lista över medlemmarnas elektroniska adresser och sänder inkomna meddelanden vidare till övriga adressater.

[107] Länkar har en central funktion i programmeringsspråket HTML. Genom länkarna kan webbläsaren förflytta läsaren från ett dokument till ett annat samt hämta bilder och ljud till det aktuella dokumetet.

7.1.2 Skälen till en reglering

Internets kraftiga expansion har medfört att spridning av meddelanden kan ske på ett enkelt och snabbt sätt till en stor mängd personer och utöva inflytande över barn och ungdomar som använder sig av tjänsterna.[108]
Från myndighetshåll menar man att det råder brist på kontroll över vissa elektroniska tjänster som misstänks användas för brottsliga syften. Man menar på att det behövs en reglering för att bygga upp ett rättsmedvetande för hanteringen av elektroniska anslagstavlor eftersom tradition och historia saknas på området. I förslaget menar man på att ”Det finns därför starka skäl för att införa en särreglering på området som syftar till att ge tjänsterna en acceptabel struktur och som framförallt klart fastställer tillhandahållarens ansvar för förekomsten av vissa meddelanden i tjänsten”.[109] Avgörande är om den personen som använder tjänsten kan ta del av andras meddelanden och samtidigt sända sina egna meddelanden till andra användare. Datoranvändning som syftar till annat än att användarna skall kunna kommunicera är inte en sådan tjänst som träffas av lagen. Meddelanden som förmedlas manuellt med tekniska hjälpmedel utgör inte en tjänst för elektronisk förmedling och traditionella teletjänster såsom telefaxapparater och gruppsamtal omfattas inte av regleringen.[110]

7.1.3 Ansvarsfördelning

Elektroniska anslagstavlor och förmedlingstjänster innehåller information där det ibland är svårt att utreda varifrån ett visst meddelande härstammar. Utredningen kan försvåras av att det i vissa former för datakommunikation används anonyma användarbetäckningar och krypterad text.[111] Systemoperatören som sköter de administrativa och tekniska rutinerna reglerar i stor utsträckning vilket utrymme som ges för missbruk av

[108] Prop. 1997/8:15 s. 8
[109] Prop. 1997/8:15 s. 8
[110] Prop. 1997/8:15 s. 9
[111] Se kapitel 3

tjänsten.[112] Tillhandahållaren skall hålla uppsikt över den tjänst som förmedlas via anslagstavlan. Den föreslagna lagen slår fast ett självständigt straffrättsligt ansvar för tillhandahållaren som i och med förslaget blir skyldig att ta bort vissa typer av meddelanden.

Om flera personer är att anse som tillhandahållare av samma tjänst sker bedömningen utifrån vem eller vilka av de berörda som har det bestämmande inflytandet och kontrollen över tjänsten. En juridisk person eller myndighet som tillhandahåller en elektronisk anslagstavla skall följa de allmänna principerna om företagaransvar som finns i praxis. Man kan säga att förslaget utgör en straffrättslig särreglering som är specifik inom IT området.[113]

Uppsikt över tjänsten

4 § *Den som tillhandahåller en elektronisk anslagstavla skall, för att kunna fullgöra sin skyldighet enligt 5 §, ha sådan uppsikt över tjänsten som skäligen kan krävas med hänsyn till omfattningen och inriktningen av verksamheten.*

7.1.4 Uppsiktsskyldighet

En systemoperatör som tillhandahåller en elektronisk anslagstavla skall inte passivt kunna se på utan att ingripa när andra användare missbrukar tjänsten. Uppsiktsskyldigheten bör uttryckligen knytas till de faktiska förhållandena som avses.[114]

Att ha en ständigt kontroll av alla meddelanden som skickas till anslagstavlan är i stort sett omöjligt men däremot bör det finnas någon form

[112] Enligt regeringens förslag bör en särreglering inriktas på systemoperatören som tillhandahåller tjänsten, vem denne eller dessa är får avgöras mot bakgrund av omständigheterna i det enskilda fallet.

[113] Att införa en lag om elektroniska anslagstavlor anses vara ett naturligt led eftersom lagen omfattar både en reglering av ansvaret för vissa meddelanden och föreskrifter som är mer av ordningskaraktär.

[114] Enligt regeringens förslag är tillhandahållaren skyldig att hålla en sådan uppsikt som skäligen kan krävas med hänsyn till omfattningen och inriktningen av verksamheten och det praktiska förfarandet skall bedömas utifrån det enskilda fallet.

av återkommande kontroll. Det anses inte förenligt med uppsiktsplikten att kontroller inte sker regelbundet under längre perioder.[115]

Tjänster som tillhandahålls yrkesmässigt kräver en noggrannare kontroll än tjänster som bedrivs av privatpersoner eftersom dessa inte har lika många besökare. En elektronisk anslagstavla bör inte lämnas utan tillsyn längre tid än en vecka och det gäller både yrkesmässiga och privata förmedlingstjänster. En möjlighet att underlätta kontrollen av innehållet och materialet är att med hjälp av en ”klagomur” ge övriga användare möjlighet att nå tillhandahållaren för att informera om förekomsten av tveksamma meddelanden.[116]

Skyldighet att ta bort vissa meddelanden

5 § *Om en användare sänder in ett meddelande till en elektronisk anslagstavla skall den som tillhandahåller tjänsten ta bort meddelanden från tjänsten eller på annat sätt förhindra vidare spridning av meddelandet, om*

1. *meddelandets innehåll uppenbart är sådant som avses i bestämmelserna i 16 kap. 5 § brottsbalken om uppvigling, 16 kap. 8 § brottsbalken om hets mot folkgrupp, 16 kap. 10 a § brottsbalken om barnpornografibrott eller 16 kap. 10 b § brottsbalken om olaga våldsskildring, eller*
2. *det är uppenbart att användaren har gjort intrång i upphovsrätt eller i rättighet som skyddas genom föreskrift i 5 kap. lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk genom att sända in meddelandet.*

För att kunna fullgöra sin skyldighet enligt första stycket har den som tillhandahåller tjänsten rätt att ta del av meddelandet som förekommer i tjänsten.

Skyldigheten enligt första stycket och rätten enligt andra stycket gäller också den som på tillhandahållarens uppdrag har uppsikt över tjänsten.

[115] Vad som är en rimlig tidsintervall avgörs i proportion till hur många användare som kopplar upp sig mot anslagstavlan.

7.1.5 Skyldighet att ta bort vissa meddelanden

För tillhandahållare och systemoperatörer som inte självmant ingriper för att förhindra missbruk och olaglig spridning av brottsliga meddelanden skall det införas ett självständigt straffrättsligt ansvar för underlåtenhet att ta bort vissa meddelanden. Om skyldigheten att ta bort meddelanden gällde alla slag av brottsliga gärningar skulle reglerna bli mycket svåra att följa eftersom informationsflödet ibland är för stort för att den som tillhandahåller tjänsten systematiskt skall kunna granska och bedöma alla meddelanden som förmedlas.

För att göra det praktiskt möjligt för tillhandahållaren att efterleva lagen föreslås att det straffbara området begränsas till vissa brott mot allmän ordning samt intrång i upphovsrätten. Vad gäller brotten mot allmän ordning är det ofta möjligt att göra en bedömning som endast utgår ifrån det specifika meddelandets innehåll och vad tillhandahållaren känt till. Tillhandahållarens skyldighet att ta bort meddelanden knyts till frågan om meddelandet har ett sådant innehåll som avses i 16 kap. 5, 8, 10 a eller 10 b § Brottsbalken om uppvigling, hets mot folkgrupp, barnpornografibrott och olaga våldsskildring. Denna typ av meddelanden är relativt enkla att identifiera och en bedömning kan göras utifrån objektiva grunder.[117] Vad gäller upphovsrättsligt skyddade meddelande kan ansvaret för tillhandahållaren knytas till om användaren genom att skicka in meddelandet har gjort intrång i upphovsrätten eller i en rättighet som skyddas genom bestämmelserna i 5 kap. Lagen om upphovsrätt till litterära och konstnärliga verk.[118]

Skyldigheten att ta bort vissa meddelanden finns när det är uppenbart att innehållet strider mot 16 kap. brottsbalken, eller att användaren har gjort sig skyldig till upphovsrättsintrång. Det kan ske genom en bedömning av hur

[116] Prop. 1997/8:15 s. 15
[117] Prop. 1997/8:15 s. 17
[118] 1960:729

tydligt meddelandets innehåll är. En annan förutsättning för att lagen skall bli tillämplig är att den endast omfattar meddelanden som sänts in till tjänsten av en användare.

Lagen är inte tillämplig när spridning av meddelanden underlättas genom att användarna t ex genom hyperlänkar hänvisas till andra tjänster som visar sig innehålla straffbara meddelanden. För att ett fullbordat brott skall anses ha begåtts krävs inte att någon spridning till andra användare faktiskt har ägt rum utan det räcker att meddelandet hålls tillgängligt för användarna vid den tidpunkten då meddelandet borde ha tagits bort.

Om tillhandahållaren ber någon annan att hålla uppsikt över tjänsten kan även den personen omfattas av bestämmelserna. En operatör vars verksamhet faller in under undantaget i andra paragrafen kan i det enskilda fallet bli ansvarig om operatören är den som faktiskt sköter den elektroniska anslagstavlan på uppdrag av tillhandahållaren.

Skyldigheten att ta bort vissa meddelande innebär däremot inte informationen måste utplånas hos tillhandahållaren. Data som behövs för att utreda och bevisa brott skall bevaras om möjligt så att polis och åklagare kan fullgöra sina uppgifter. Under vissa omständigheter kan det vara straffbart att förvanska eller radera meddelanden t ex vid fall av bevisförvanskning enligt bestämmelserna i 15 kap. 8 § Brottsbalken.

Straff

6 § *Den som uppsåtligen eller av oaktsamhet bryter mot 3 § döms till böter.*

7 § *Den som uppsåtligen eller av grov oaktsamhet bryter mot 5 § första stycket döms till böter eller fängelse i högst sex månader eller, om brottet är grovt, till fängelse i högst två år. I ringa fall skall inte dömas till ansvar.*
Första stycket tillämpas inte, om det för gärningen kan dömas till ansvar enligt brottsbalken eller lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk.

7.1.6 Straff

Skyldigheten att ta bort och förhindra fortsatt spridning uppkommer när tillhandahållaren får kännedom om förekomsten av meddelandet.[119] För att förhindra att tillhandahållaren håller sig ovetande om meddelanden som finns på anslagstavlan kan straffansvar inträda för den som av grov oaktsamhet underlåter att ta bort vissa meddelanden eller förhindrar vidare spridning. Vid en bedömning om förfarandet är att se som grovt oaktsamt utgår man ifrån hur tillhandahållaren uppfyllt sin uppsiktsplikt över tjänsten. Om uppsiktsplikten har missköts och det fått till följd att tillhandahållaren underlåtit att ta bort sådana meddelanden som stadgas i 5 § första stycket kan straffansvar bli aktuellt. Om en elektronisk anslagstavla vid flertal tillfällen innehållit straffbara meddelanden kan kravet på åtgärder av tillhandahållaren sättas högre och ett större inslag av aktiva och förebyggande åtgärder krävas. Straffskalan för normalgraden av brott mot skyldigheten att förhindra spridning av vissa meddelanden kan sträcka sig från böter till fängelse i sex månader. Om brottet är grovt kan straffet vara fängelse i högst två år. Grovt brott föreligger om meddelanden som anges i 5 § första stycket har haft mycket stor omfattning eller det är fråga om upprepade förseelser. I ringa fall bör man inte kunna dömas till ansvar. Med ringa fall menas t ex att ett enstaka meddelanden förekommit på en elektroniska anslagstavla som i övrigt bedriver en seriös verksamhet.

Vad gäller frågan om skyldigheten att ta bort vissa meddelanden bör ansvar inte inträda om tillhandahållaren kan dömas till ansvar enligt bestämmelserna i Brottsbalken. Om en tillhandahållare kan dömas för brott enligt bestämmelserna i 5 § första stycket antingen som gärningsman eller som medverkande skall bestämmelsen inte tillämpas och detsamma gäller om gärningen ryms inom något annat straffbart förfarande i Brottsbalken.

[119] Enligt förslaget är brott mot informationsskyldigheten straffbart både när det sker med uppsåt och när det sker av oaktsamhet. Eftersom brottet närmast är att se som en

Även i förhållande till straffbestämmelserna i upphovsrättslagen är bestämmelserna i förslaget subsidiära.

Förverkande

8 § *Datorer och andra hjälpmedel som har använts vid brott enligt 7 § denna lag får förklaras förverkade, om åtgärden behövs för att förebygga fortsatt brottslighet eller det annars finns särskilda skäl. Förverkande får helt eller delvis underlåtas om förverkandet är oskäligt.*

7.1.7 Förverkande

Det har ansetts viktigt att ha en förverkandebestämmelse som komplement till straffbestämmelsen främst för att förhindra fortsatt brottslighet. Genom en förverkandebestämmelse får åklagare och polis en möjlighet att förverka datorer och andra hjälpmedel t ex datorprogram som använts vid brott. Förverkande kan också ske när det framstår som stötande att gärningsmannen får behålla de hjälpmedel med vilka han begick brotten. Enligt förslaget bör förverkande endast bli aktuellt vid brott mot skyldigheten att förhindra spridning av vissa meddelanden.[120]

7.2 Konsekvenser av förslaget

Utredningen som föregåtts av lagförslaget har uppskattat antalet elektroniska anslagstavlor i Sverige till ca 6500. Enligt utredningen tar det i genomsnitt en timme i veckan att vidta åtgärder för att förhindra spridning. Timkostnaden beräknas till 500 kronor och årskostnaden för förslaget för dem som tillhandahåller elektroniska anslagstavlor beräknas bli ungefär 169 miljoner kronor.[121] Förutom tillhandahållarens kostnader för tillsyn av tjänsten tillkommer kostnader för att utforma tjänsten så att

---

ordningsförseelse bör endast böter kunna följa på brottet och något behov av att införa ansvar för grovt brott finns inte.

[120] Prop. 1997/8:8 s. 21

[121] Prop. 1997/8:15 s. 23-24 ff.

informationskravet uppfylls. Förslaget innebär också att åklagare och polis får ett nytt instrument för att bekämpa denna form av brottslighet.

7.3 Polisens tillträde till elektroniska anslagstavlor

Telekommunikationens internationella karaktär med uppkopplingar i många led via nätverk i andra länder gör det svårt för polisen att vidta nödvändiga åtgärder för att identifiera en gärningsman. Okonventionella spanings och utredningsmetoder som t ex infiltration och förtäckt husrannsakan är inte tillåtna inom ramen för den öppna polisverksamheten. Vid uppkoppling mot vissa databaser förekommer beskedet att poliser inte äger tillträde. Är databasen allmän d v s man behöver inte ange lösenord kan naturligtvis en polisman koppla upp sig, men när användaren måste ange sin identitet begränsas förutsättningarna för spaning.[122]

En polisman har i princip samma befogenheter som en privatperson men inom den öppna polisverksamheten godtas det inte att oriktiga identitetsuppgifter lämnas, inte ens om övriga användare använder täcknamn. Vid spaning uppträder polisen visserligen i civila kläder och ger sken av att vara privatpersoner eftersom det är en förutsättning för att inte avslöja att den vidtas i tjänsten. Att jämföra en civilklädd polisman med att under oriktigt namn bereda sig tillträde till databaser är inte helt utan problem eftersom en civilklädd polisman inte ställs i en
situation där medvetet oriktiga identitetsuppgifter krävs för att fullfölja åtgärden.
En polisman som är okänd i aktuella kretsar bör kunna använda sitt riktiga namn och på så sätt få tillgång till t ex databaser och andra elektroniska förmedlingstjänster. Erfarna poliser på området kan bli stoppade vid uppkoppling eller hindras från att få tillgång till material som styrker brott. Problemet kan lösas i praktiken genom att en polis som är okänd i aktuella kretsar kopplar upp sig i eget namn under ledning av erfarna IT utredare

[122] SOU 1996:40 s. 209

varefter båda kan ta del av informationen och uppgifterna på den elektroniska anlagstavlan.

I vissa fall krävs muntliga kontakter och i vissa fall personliga kontakter för att beredas tillträde som användare. I dessa fall kan en polisman inte bereda sig tillträde utan beslut om husrannsakan. För att få tillträde utan användning av tvångsmedel skulle polismannen bli tvungen att låna en användares identitet eller vilseleda om sin identitet vid samtal med den som tillhandahåller tjänsten, och när det behövs skaffa rekommendationer från en annan användare.[123] Polismannen skulle bli en infiltratör istället för en informatör. De uppgifter som behövs för ett åtal kan i vissa fall återfinnas vid en utvärdering av material som beslagtagits men för dessa åtgärder krävs en hel del teknisk kunskap om hur systemen används och fungerar.

7.4 Brottsligt förfarande vid spaning

Trots att databaser och andra elektroniska förmedlingstjänster innehåller uppgifter om att poliser och åklagare inte äger tillträde medför inte detta att poliser och åklagare som kopplar upp sig begår brott. Personen som tillhandahåller förmedlingstjänsten kan inte förfoga över olovlighetsrekvisitet i t ex bestämmelsen om dataintrång i datalagens 21 §. Även reglerna om brottsprovokation kan komma i konflikt med rutinerna för att ta del av innehållet på en elektronisk anslagstavla. Att säkra material på en databärare hos polisen kan leda till otillåten exemplarframställning enligt upphovsrättslagen. Antingen kan en polisman som genomför åtgärden uppfylla brottsrekvisiten eller kan den som tillhandahåller tjänsten provoceras till brott. Vid motsvarande åtgärder i traditionell miljö inriktas åtgärderna mot traditionella fysiska exemplar.[124] Dessa exemplar är tillgängliga för var och en och kan läsas och fotograferas av en polisman utan han riskerar brott. I IT miljö kan användningen av tvångsmedel krävas för att frita från straffansvar.

[123] SOU 1996:40 s. 210
[124] SOU 1996:40 s. 211

8 Sammanfattning

Tittar man på den samlade bilden av IT - brottsligheten kan man nog säga att den befinner sig under snabb utveckling. Ett av de svåra problemen som rättsväsende och polis ställs inför är att antalet datorbrott som inte kommer polisen till kännedom är relativt stort. Enligt det amerikanska justitiedepartementet kan mörkertalet när det gäller IT brottsligheten i USA vara så hög som 99%, d v s att endast ett datorbrott av hundra upptäcks. Det är viktigt att vi i Sverige på ett tidigt stadium försöker förhindra en liknande utveckling här. Trots att vi ligger långt fram vad gäller den tekniska delen av informationsteknologin har utvecklingen i framförallt USA visat vad som är att vänta i Sverige och Europa om ett par år. Den accelererande utvecklingen av elektronisk handel över Internet är det tydligaste beviset på att användare i privat och offentlig verksamhet samt marknadsaktörer gör sig beredda på en explosiv utveckling. Elektronisk handel via Internet har blivit vanligt i Sverige och transaktioner kan ske på ett enkelt och bekvämt sätt men det ställer också höga krav på säkerheten i systemen. Anledningen till att jag tagit med ett kapitel om kryptering är att det kommer att bli av allt större betydelse för den framtida kommunikationen via Internet. Under lång tid har kryptering varit förbehållet försvaret och utrikesförvaltningen men utvecklingen har nu lett till att många användare kräver att få använda kryptering för att på ett säkert sätt kunna använda nya informationstjänster och infrastrukturer för information och kommunikation som växer fram nationellt och internationellt. Problemet med kryptopolitiken är att försöka få en enad och fungerande policy på området. Olika länder har kommit olika långt vad gäller utvecklingen beroende på att kryptofrågorna berör så många intressen att det är svårt att hitta den balans som krävs för en internationell reglering på området. Intrång i upphovsrätten är det problem som fortfarande bedöms som mest svåråtkomligt. Även i Sverige förekommer det en omfattande piratkopiering av datorprogram. Denna form av ekonomisk brottslighet är mycket svår att få grepp om och det krävs inte mycket tekniskt kunnande för att vidarekopiera programvara. Ungefär hälften av de

program som sitter i svenska PC datorer idag är piratkopierade. Om man skall rangordna vilka områden som bör prioriteras för att förhindra Internet brottslighet skulle jag vilja rekommendera att man i första hand skall ta tag i piratkopieringen av programvara eftersom denna form av ekobrottslighet är mycket omfattande. För det andra är det viktigt att handel och transaktioner via Internet kan ske på ett säkert sätt utan möjlighet att manipulera information och förhoppningsvis kommer det nya SET systemet att utgöra den nya standarden i framtiden.

9 Litteratur och källförteckning

Brinck, Ohlson, Thornell, *Straffrätt enligt brottsbalken*, Umeå 1993.

Carlén- Wendels Thomas, *Nätjuridik- Lag och rätt på Internet*, Juristförlaget Norstedts Tryckeri AB, Stockholm 1997.

Datorrelaterade missbruk och brott- en kartläggning gjord av Effektivitetsrevisionen, Riksrevisionsverket 1997:33

Dämvik Mats, *Internet- ett verktyg vid forskning i utländsk och internationell rätt*, IRI- rapport 1993:2 Institutet för rättsinformatik, Stockholm 1993.

International review of penal law, *Computer crimes and other crimes against information technology*, Vol. 64 No 1-2 1993.

IT- kriminalitet- Checklista för målsägare, ett samarbete mellan IT-Företagen, Buisness Software Alliance (BSA), Larmtjänst och Rikskriminalpolisen 1997.

Jareborg Nils, Asp Petter, Svensk internationell straffprocessrätt, Iustus Förlag AB, Uppsala 1995.

Koktvedgaard Mogens/Levin Marianne, Lärbok i immaterialrätt, upplaga 3. Fritzes Förlag AB, Stockholm 1995.

Kryptopolitik- möjliga svenska handlingslinjer, en rapport från Regeringskansliets referensgrupp för krypteringsfrågor, oktober 1997.

Seipel Peter, *Juristen och datorn*, Introduktion till rättsinformatiken, upplaga 5
CE Fritzes AB, Kristianstad 1994.

Wallin Anders, *Kriminella teknikzonen, straffrättsliga perspektiv på brott och hacking i globala datanät*, IRI- rapport 1994:2

Offentligt tryck

Propositioner

prop 1997/8:15

Statens offentliga utredningar

SOU 1992:110
SOU 1996:40
SOU 1995:69

Övrigt

Dir. 1997:1

Departementsserien

Ds 1997:51

EU- material

COM (96) 487- Illegal and harmful content on the Internet. Communication to the European Parliment, the Council, the Economic and Social Committee and the Committees of the Regions.

Directive 89/552/EEG

C- 34-36/95. EG- domstolens beslut i målen.

Lagtext och konventioner

Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk

Datalagen (1973:289)

Bernkonventionen (för skydd av litterära och konstnärliga verk, från 1886, ändrad 1971)

Romkonventionen (om skydd för utövande konstnärer, fonogramframställare och radioföretag från 1961)

WIPO Copyright Treaty

WIPO Performance and Phonograms Treaty

Tidningar och tidskrifter

Dissedenten, mars 1995, Juridiska föreningen i Lund.

PC för alla, nr 5, oktober 1997

Informatik, nr 3, 1997

Los Angeles Times 1994-11-03

Microsoft magazine, nr 5, 1996

Microsoft magazine, nr 6, 1996

Microsoft magazine, nr 1, 1997

Microsoft magazine, nr 3, 1997

Microsoft magazine, nr 4, 1997

Rättsfall

NJA 1996 s. 74

RH 1997:61