Regeringens proposition till Riksdagen med förslag till lag om ändring av strafflagen

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås att framställning och spridning av s.k. datavirus skall kriminaliseras genom en ny bestämmelse i strafflagen. Med datavirus avses datorprogram eller programinstruktioner som är planerade att störa informationsbehandling eller ett data- eller telesystems funktion eller skada data eller program i ett sådant system. Den föreslagna brottsrubriken är orsakande av fara för informationsbehandling. Straffskalan föreslås vara böter eller fängelse i högst två år.

Dessutom föreslås i denna proposition att bestämmelsen om olaga befattningstagande med infört gods skall ändras så att det maximistraff som bestämts för brottet skall höjas från fängelse i sex månader till fängelse i ett år och sex månader. Med tanke på lindrigare fall föreslås det att till kapitlet skall fogas en ny paragraf, där det skall bestämmas om lindrigt olaga befattningstagande med infört gods. Påföljden för detta brott skall vara böter.

Lagen avses träda i kraft så snart som möjligt efter det att den har antagits och blivit stadfäst.

INNEHÅLLSFÖRTECKNING

MOTIVERING

1. 34 kap. strafflagen

1.1. Inledning

Allmänt

Ett datorprogram är en framställning av en informationsbehandlingsuppgift i form av en serie funktioner som är avsedda att verkställas av en processor. Processorn är en anordning som automatiskt behandlar numeriska uppgifter och som styrs av ett program som lagrats i dess minne. Då processorn tolkar programinstruktionerna, kan den inte utvärdera deras innehåll, utan kopierar och sprider också skadliga instruktionskoder.

Allmänt talar man om datavirus eller adb-virus då man avser sådana datorprogram eller programinstruktioner som är avsedda att störa informationsbehandling eller ett data- eller telesystems funktion eller skada den information eller programvara som systemen innehåller. Det finns ingen vedertagen terminologi i fråga om dessa program och terminologin är i det avseende vilseledande att viruset endast utgör en - om än den vanligaste - typen av sådana program. Det är kännetecknande för virus att de inte kan fungera självständigt utan att de alltid behöver ett annat program som värd. Virusen kan spridas av sig själva från ett program till ett annat i en dator och via datanät vidare från en dator till en annan. De s.k. trojanska hästarna avviker från virus i och med att de inte själva sprider kopior av sig själva utan klarar av att spridas endast med hjälp av användaren, dvs. användaren måste kopiera det program som den trojanska hästen har infekterat. Logiska bomber är sådana trojanska hästar som har programmerats att aktiveras först då något logiskt villkor uppfylls. Maskar är program som fungerar självständigt och som via nätet kan kopiera sig själva till andra datorer.

Som gemensamma engelskspråkiga benämningar för alla ovan nämnda och andra motsvarande programtyper används bl.a. termerna "malware" och "malicious code". I finskan eller svenskan har det inte etablerats någon motsvarande gemensam benämning. På finska har man dock i vissa sammanhang använt termerna "tuho-ohjelma" och "tuholaisohjelma". För att göra denna presentation enklare används senare i motiveringen ordet "virus" som benämning för alla ovan nämnda program.

Oftast sprids virusen antingen via disketter eller datanät. En diskett som har varit i en dator som blivit infekterad för smittan vidare till alla andra datorer i vilka disketten används. Sådana program som gratis får kopieras från datanätens offentliga postlådor eller anslagstavlor kan fungera som världsomfattande metoder för att sprida virus.

Den största delen av de mer än 40 000 virus som man för närvarande känner till har tillverkats för att fungera i DOS-miljö. Bootsektorvirusen infekterar disketternas eller hårdskivornas bootsektor, där de kan kopiera sig själva till vilken diskett som helst som används i datorn och som inte är skrivskyddad. Om en virusinfekterad diskett finns i diskettstationen då datorn kopplas på, kopierar viruset sig självt till datorns hårdskiva.

Datafilvirusen är numerärt den allmännaste virustypen som sprids i samband med vanliga programfiler. Under de allra senaste åren har makrovirusen som i första hand sprider sig via textfiler börjat bli allmännare, och i dag känner man redan till mer än 3 500 sådana virus. Makrovirusen är lättare att konstruera än traditionella virus och det finns också risk för att virustillverkning vilket hittills varit en hobby för experter på datateknik, åtminstone i viss mån kommer att bli allmännare bland vanliga användare av datateknik.

I Finland har man hittat flera hundra olika virus, och av dessa har tiotals konstruerats i Finland.

De största av de förändringar som inträffat under den senaste tiden hänför sig till Internet. Det finns ett stort antal sådana skadliga program i omlopp som t.ex. skickar ut en användares lösenord eller andra konfidentiella uppgifter i en maskin via Internet eller som medger att en utomstående distansanvänder den maskin eller det system som är föremål för angreppet.

Antalet virustyper innehåller inte någon information om frekvensen för deras förekomst, vilken är flerdubbel jämfört med antalet virustyper. I ett enstaka fall kan det vara fråga om ett tjugotal separata datorer, såsom i det fall vid Finlands riksdag som det redogörs för senare, eller om över 6 000 anslutningar såsom i fallet med ARPANET-nätet.

Alla virus förorsakar någon form av skada. En stor del av virusen är sådana att de endast sprids, men även dessa upptar i varje fall utrymme på hårdskivan, orsakar kompatibilitetsproblem och gör datorernas funktioner långsammare samt förorsakar avsevärda kostnader som föranleds av rengöring och andra motsvarande åtgärder. Direkt ekonomisk skada kan förorsakas då ett aktiverat virus t.ex. förstör eller modifierar filer. I sådana fall kan i synnerhet följdverkningarna vara överraskande och mycket betydande. T.ex. felaktiga beslut som fattats inom förvaltningen eller inom företag på basis av uppgifter som modifierats av ett virus kan leda till avsevärda skador, för att inte tala om de följder som uppkommer inom datorstyrd verksamhet - som exempel kan nämnas den eventuella inverkan ett virus kan ha på kontrollsystemen inom järnvägs- eller flygtrafiken. Det är också fullt möjligt att använda virus som en form av elektronisk krigföring.

Även förebyggande virusbekämpning förorsakar avsevärda kostnader för myndigheter och företag. De indirekta och direkta kostnader som förorsakats av virusfall har vuxit till betydande summor under de senaste tio åren. Allt som allt är de mångfaldiga verkningarna av denna negativa företeelse och kostnaderna för virusbekämpningen i industriländerna av en sådan storleksklass att experterna redan t.o.m. anser dem inverka på olika länders samhällsekonomi. Talrika virusbekämpningsföretag har redan listats på börsen på Wall Street. Det behövs således även av ekonomiska orsaker ett klart ställningstagande av lagstiftaren och ett tillräckligt effektivt straffhot för att påverka motivationen hos viruskonstruktörerna.

Om skyddsobjekten vid datateknikbrott

Målsättningen är att uppnå datasäkerhet, vilket innebär att informationen, systemen och tjänsterna genom lagstiftning och övriga åtgärder såväl under normala omständigheter som under undantagsförhållanden erhåller tillbörligt skydd mot sådana hot och skador som riktar sig mot deras konfidentiella karaktär, integritet och tillgänglighet och som förorsakas av fel i maskinvaror och programvaror, av naturföreteelser eller mänskliga gärningar som sker uppsåtligen, av oaktsamhet eller på grund av olyckshändelser.

Skyddsobjektet vid datateknikbrott har t.ex. i Nederländernas lagstiftning uttryckts med termen "informationsbehandlingsfrid" och i rättslitteraturen förekommer också det latinska "Pax Computationis", vilket kort beskriver det som t.ex. i Förenta Nationernas handbok om datateknikbrott, i OECD:s, Europeiska rådets och Finlands statsråds datasäkerhetsbeslut noggrannare förklaras med hjälp av tre grundbegrepp, dvs. uppgifternas konfidentiella karaktär (Confidentiality), integritet (Integrity) och tillgänglighet (Availability). Virusprogrammen kränker således alltid grunderna för informationsbehandlings- och informationskommunikationsfriden.

Dataöverföringen är för närvarande, vare sig den sker trådlöst eller inte, en allt viktigare del av informationsbehandlingen och det är både nationellt och internationellt av största vikt att dataöverföringen får ske ostört. Datatekniska upptagningar, vare sig det är fråga om en magnetisk (såsom en hårdskiva eller en diskett), optisk (CD-skiva), elektronisk (ROM-minneskrets) eller mekanisk (t.ex. ett sådant hålkort som tidigare var vanligt) upptagning, grundas den på en binär framställning, där integriteten har lika viktig praktisk och juridisk betydelse som vid dataöverföring. Redan en modifiering av en siffra i det binära systemet, antingen en nolla eller en etta (en bit, vilket är en förkortning av orden Binary Digit), vilket empiriskt alltid och ovillkorligen också är en fysisk förändring, förorsakar oundvikligen en förändring av den enkla kontrollsumman eller av ett mer utvecklat säkerhetssystem, den s.k. signaturkoden.

Som äkthetsgaranti för traditionella (pappers)handlingar har man genom tiderna använt sigill och underskrifter. Innan man t.ex. har kunnat och i framtiden vid en domstol kan ge ett testamente materiell betydelse, måste dess äkthet och ursprung fastställas. Bevisandet av äktheten av elektroniska handlingar, vilka uttryckligen nämns som en typ av bevismedel i strafflagen, och deras framtida juridiska relevans över lag, grundas och kommer att grundas på ostridbara kännetecken på jämförbara filer, dvs. t.ex. på de s.k. signaturkoder som räknas på basis av filerna. Koderna är också en del av förfarandet med digital signatur. Om inte dessa koder, t.ex. en teckenserie som vittnet innehar (t.ex. B1 4E 2A BD 96 08 8B A4 67 83 D1 09 FE 52 56 6C) stämmer överens

med den teckenserie som domaren räknar ut på sin dator, är handlingarna inte till innehållet desamma.

Virusprogrammen kan således i framtiden förorsaka omfattande rättslig osäkerhet, och genom att förstöra grunden för elektroniska handlingars tillförlitlighet förhindra att ärenden uträttas och att handel sker på elektronisk väg. Det är således inte enbart fråga om att data förstörs. Om filer förstörs t.ex. inom hälsovården är det lätt att förstå att detta kan ha fatala verkningar både med tanke på individen och också mer vidsträckt. Det är också i stor utsträckning fråga om den integritet (Integrity) som nämnts i samband med begreppet datasäkerhet och i kapitlet om skyddsobjektet vid datateknikbrott och som avser riktigheten och äktheten av data och information samt bevarandet av dessa egenskaper.

Exempel på virusfall i praktiken

I riksdagens mikrodatorer hittades i december 1993 dataviruset Telefonica. Viruset var nyare än det antivirusprogram som användes, varför smittan avslöjades först då viruset förstörde hårdskivan i en mikrodator. Allt som allt hann viruset infektera tjugo arbetsstationer. Riksdagsmännen uppmanades att göra säkerhetskopior tillräckligt ofta samt att akta sig för olagliga programkopior och spel. Deras hemdatorer förseddes med tidsenliga antivirusprogram.

Från Kanada sändes i januari 1995 ett paket som innehöll 2 806 virus till en diskussionsgrupp i Internet. Paketet placerades senare på en finsk www-sida tillgängligt för allmänheten. I Finland var viruspaketet tillgängligt på en xgw-server som upprätthålls av ett av de små företag som erbjuder Internet-anslutningar. Vissa arga kunder försökte dock göra en polisanmälan angående detta. Den person som var föremål för anmälningarna var fast övertygad om att det i detta sammanhang var fråga om hans yttrandefrihet.

Centralkriminalpolisen måste efter att ha tagit emot anmälan konstatera att det inte i Finland enligt gällande rätt är straffbart att enbart göra virus tillgängliga för allmänheten fastän det är fråga om ett stort antal virus. Enligt centralkriminalpolisen var det inte fråga om yttrandefrihet, eftersom det när allmänfarliga datorprogram gjordes tillgängliga för allmänheten inte var fråga om sådant innehåll eller meddelande som förutsätts för rättsobjektet som erhåller skydd såsom grundrättighet. Centralkriminalpolisen ansåg att en fortsättning av sådant handlande enligt de allmänna rättsprinciperna om öppnande av källor till fara lagligen kunde förhindras genom att anslutningen i fråga stängdes av.

Telecom Finland Oy frågade trafikministeriet om bolaget kan häva en sådan persons anslutning som i egenskap av producent av tjänster sprider virusprogram inom Internet-nätet, eller på något annat sätt förhindra kontakterna till den service som tillhandahåller virusprogram. Trafikministeriet fattade den 16 juni 1995 ett beslut genom vilket man också mer allmänt gav anvisningar om avstängning av teleförbindelser i vissa fall. I beslutet ansågs det att det inte ankommer på trafikministeriet att ta ställning till innehållet som sådant i de budskap som förmedlas eller ställs till förfogande i telenät. Trafikministeriet konstaterade dock att man genom oskyddade virusprogram som allmänt ställts till förfogande i Internet via någon server uppsåtligen eller oavsiktligen kan förorsaka skada i en dator som fungerar som en del av telenätet. Genom de virusprogram som ställs till förfogande kan man förorsaka störning också i en dator som tillhör en annan användare av telenätet och som är ansluten till nätet via ett modem, fastän en sådan dator inte är en del av telenätet eller en dataterminal som är direkt ansluten till telenätet. Trafikministeriet beslöt med stöd av 10 § 2 mom. telemarknadslagen (183/1987), att en teleinrättning har rätt att stänga av en anslutning också då det påvisas att det via teleanslutningen allmänt erbjuds virusprogram genom vilka man kan förorsaka störning antingen för telenätet eller för andra användares telekommunikation.

Vilket slag av störning eller skada det kan vara fråga om har i offentligheten i stor utsträckning blivit klart redan i samband med det s.k. "Internet Worm"-fallet i USA under hösten 1988. Ett destruktionsprogram lamslog till slut över 6 000 datorer i U.S. Army Research Computer Network (ARPANET)-nätet. Gärningsmannen dömdes våren 1991 i en besvärsdomstol till villkorligt fängelse i tre år, 400 timmar samhällstjänst samt 10 000 dollar i böter.

Enligt tyska datasäkerhetsexperter (Bundesamt für Sicherheit der Informationstech-

nik, BSI, Bonn) är det ett faktum att det är mycket enkelt att utveckla program som är beskaffade som Internet Worm, att de är avsevärt svårare att upptäcka och att de eventuellt klarar av att tränga in i flera datorer och operativsystem än förut (Internet Worm var konstruerat så att det på en gång trängde in i bara två datortyper som var försedda med olika operativsystemversioner). Programmen innehåller enkla metoder som döljer spåren efter gärningsmannen och som i praktiken gör det omöjligt att få reda på gärningsmannens identitet.

BSI arrangerade i februari 1997 i Bonn en internationell konferens gällande lagstiftningsproblematiken i samband med datateknikvirus, där det konstaterades att brottsstatistiken och statistiken över virusfall inte beskriver den egentliga storleken av problemet. Brottsanmälningar och uppklarade fall som förts vidare till domstol har närmast förekommit i Storbritannien. T.ex. i Exeter dömdes i december 1995 en person för virusspridning till ett ovillkorligt fängelsestraff på ett år och sex månader. Denna dom offentliggjordes i vid utsträckning i pressen och via Internet och konstaterades tydligt ha en verkan som sänkte antalet virus som statistikförts i England år 1996.

Framtidsvisionerna fördystras av att det för närvarande i näten finns ett utbud av paket som påminner som det ovan nämnda paketet på 2 806 virus och också av att dessa virus ofta är av värre slag än tidigare, samt uttryckligen av att det finns allt flera anvisningar och automatiserade verktyg för konstruktion av virus. Dessa faktorer talar också för en kriminalisering.

1.2. Nuläge

Enligt den gällande strafflagen är det inte i och för sig straffbart att tillverka eller sprida virus. Först då ett aktiverat virus har orsakat skada kan man i vissa fall straffa den på vars åtgärder det beror att viruset har infekterat ett datasystem.

För skadegörelse döms enligt 35 kap. 1 § 2 mom. strafflagen (39/1889) också den som för att skada någon orättmätigt förstör, skadar, döljer eller hemlighåller information som har upptagits på ett datamedium eller någon annan upptagning. Enligt 2 § är det fråga om grov skadegörelse bl.a. då det genom skadegörelsen vållas synnerligen stor ekonomisk skada eller synnerligen kännbar skada för den drabbade, med beaktande av dennes förhållanden, och skadegörelsen även bedömd som en helhet är grov. För skadegörelse utdöms böter eller fängelse i högst ett år och för grov skadegörelse fängelse i minst fyra månader och högst fyra år. Om skadegörelsen bedömd som en helhet är ringa, är det fråga om sådan lindrig skadegörelse som avses i 3 §, för vilken straffet är böter. Skadegörelsen är straffbar endast om den sker uppsåtligen. Skadegörelse och lindrig skadegörelse är målsägandebrott då de riktas mot privat egendom.

Ett virus kan förorsaka att lagrad information försvinner eller förstörs. Då detta sker, uppfylls det objektiva rekvisitet för skadegörelsebrott. För att den som förorsakat virussmitta skall kunna straffas för sin gärning, förutsätts det dock att han har förfarit uppsåtligt i avsikt att skada någon annan. Spridningen av ett virus kan ske mycket slumpartat och utgångsläget torde vara att viruskonstruktören eller -spridaren inte har i sinnet att skada någon särskild information som finns i en viss dator eller på ett visst datamedium. Viruskonstruktören har kanske t.ex. för att testa sin skicklighet endast konstruerat ett virus utan att ha för avsikt att få det att sprida sig, och spridningen har å sin sida förorsakats av någon annans oaktsamhet. I dylika och i andra motsvarande fall är det minst sagt ifrågasatt om orsakandet av den skada som eventuellt till slut uppkommer kan tillräknas någon som uppsåtligt skadegörelsebrott. Det är också ifrågasatt om bestämmelserna om skadegörelse med tanke på sin ordalydelse kan tillämpas på spridande av ett sådant virus som endast orsakar indirekt skada och som inte leder till att lagrad information försvinner eller förstörs, fastän det även i detta fall är fråga om en kränkning av integriteten vid informationsbehandlingen, eftersom även en modifiering av endast en bit t.ex. vid räknandet av signaturvärdet ger ett avvikande slutresultat och gör att den elektroniska handlingen förlorar sitt bevisvärde.

För sabotage döms enligt 34 kap. 1 § 2 mom. strafflagen också den som bl.a. genom att obehörigen ingripa i ett datasystems funktion, förorsakar allvarlig fara för energiförsörjningen, den allmänna hälsovården, försvaret, rättsvården eller någon med dessa jämförbar viktig samhällsfunktion. Om sabotaget begås så att en stor mängd människor

utsätts för allvarlig fara för liv eller hälsa, så att någon viktig samhällsfunktion på grund av den hotande skadans långvarighet, omfattning eller av någon annan orsak utsätts för synnerligen allvarlig fara eller under krig eller andra undantagsförhållanden och brottet även bedömt som en helhet är grovt, är det fråga om sådant grovt sabotage som aves i 3 §. Straffet för sabotage är fängelse i minst fyra månader och högst fyra år och för grovt sabotage fängelse i minst två och högst tio år. Försök till båda brotten är straffbart.

I vissa fall kan orsakandet av virussmitta innebära ett sådant ingrepp i ett datasystems funktion att straffbestämmelserna om sabotage kan tillämpas. Till skillnad från skadegörelsebrotten förutsätts det inte vid sabotage att skada uppkommer, utan det är tillräckligt att det förorsakas fara, så i detta avseende överskrids tröskeln för straffbarhet redan innan viruset aktiveras. Å andra sidan är bestämmelserna om sabotage till sitt innehåll sådana att de förhållandevis sällan blir tillämpliga.

1.3. Bestämmelser om virus i vissa stater

Kriminaliseringar som är förknippade med tillverkning eller spridning av virus är bland de europeiska staterna för tillfället gällande i Nederländerna, Italien, Schweiz, Ryssland och Storbritannien. Dessutom bereds kriminaliseringar i Sverige och Tyskland.

Nederländerna

Enligt en bestämmelse från år 1992 i den nederländska strafflagen, utdöms straff för den som uppsåtligen eller orättmätigt ställer till förfogande eller sprider sådana data som är avsedda att förorsaka skada genom att kopiera sig själva inom ett datasystem. Som påföljd för brottet föreskrivs fängelse i högst fyra år eller högst 100 000 gulden i böter.

Italien

Till den italienska strafflagen fogades år 1996 en bestämmelse enligt vilken den som sprider, förmedlar eller lagrar ett av honom själv eller någon annan tillverkad datorprogram som är avsett att skada ett data- eller telesystem eller data eller programvara som ingår i eller hör till systemet genom att avbryta systemets funktion antingen helt eller delvis eller genom att förändra dess funktion, gör sig skyldig till ett sådant brott som avses i bestämmelsen.

Schweiz

Enligt en bestämmelse i den schweiziska strafflagen som trädde i kraft vid ingången av år 1995, är det straffbart att skapa, importera, sprida, ställa till förfogande och erbjuda ett sådant program som är avsett att förstöra eller modifiera sådana data som lagrats eller överförts elektroniskt eller på något annat motsvarande sätt eller att göra dem obrukbara. Det är dessutom straffbart att ge anvisningar för tillverkning av sådana program. Straffet för detta brott är fängelse i högst tre år eller högst 40 000 schweiziska franc i böter. Om gärningsmannen har haft för avsikt att dra nytta av brottet, är straffet fängelse i högst fem år.

Ryssland

I den ryska strafflagen finns en bestämmelse om skapande, användning och spridande av skadliga datorprogram. Enligt denna bestämmelse skall den som tillverkar ett sådant program eller omarbetar ett existerande program så att det blir sådant att det genom att förstöra, undertrycka, modifiera eller kopiera information förorsakar skada i informationsbehandling, datasystem eller datanät, straffas med fängelse i högst tre år och böter. Det är också straffbart att använda och sprida ett sådant program eller en anordning som innehåller ett sådant. Om gärningen har förorsakat allvarliga följder, är påföljden fängelse i minst tre och högst sju år.

Storbritannien

Storbritanniens Computer Misuse Act (CMA) från år 1990 är en lag som gäller datateknikbrott och som innehåller tämligen allmänna straffbestämmelser. I motsats till de länder som behandlats ovan finns det inte i Storbritannien någon uttrycklig bestämmelse om tillverkning eller spridande av virus, men i den paragraf i CMA som har en mycket allmän och omfattande utformning kriminaliseras också sådan verksamhet som spridande av virus innebär. Enligt bestämmelsen är all slags verksamhet som orättmätigt modifierar innehållet i en dator straffbar. Som straff för brottet anges fängelse i högst

fem år, böter eller både böter och fängelse.

Sverige

I Sverige avläts år 1992 ett förslag till en ny paragraf i brottsbalken som innehåller bestämmelser om allmänfarliga brott (SOU 1992:110). Enligt denna paragraf skall den straffas som framställer datorprogram eller programinstruktioner (datavirus) som konstruerats så att de olovligen kan påverka data för automatisk informationsbehandling eller tekniska hjälpmedel för sådan behandling. Det skall också vara straffbart att sprida sådana program eller instruktioner och därigenom framkalla allmän fara för att sådana data utplånas, ändras eller undertrycks eller för att sådana hjälpmedel skadas eller störs i sin funktion. Påföljden för brottet föreslås vara böter eller fängelse i högst två år, eller om brottet är grovt, fängelse i minst sex månader och högst sex år. Dessutom föreslås det att i brottsbalken skall tas in en bestämmelse med ett motsvarande straffhot i fråga om vårdslöst spridande av datavirus.

Det svenska förslaget utgör en del av ett mycket omfattande lagstiftningsinitiativ gällande datateknikbrott som inte har fortskridit speciellt snabbt. I de utlåtanden som givits beträffande virusparagrafen har man för det mesta förhållit sig positivt till tanken på att kriminalisera spridande av virus. Däremot har man inte ansett det särskilt motiverat att kriminalisera tillverkning, vilket beror på att förberedelse till det brott som avses i bestämmelsen enligt förslaget skall vara straffbart.

Tyskland

I Tyskland har man vid den ovan nämnda BSI konferensen presenterat ett förslag till virusparagraf. Enligt utkastet skall den som orättmätigt producerar, sprider, erbjuder eller ställer till förfogande sådana program eller data som är avsedda att förstöra, modifiera eller göra information eller programvara användningsoduglig, ger anvisningar för konstruktion av sådana program eller tillverkar medel som lämpar sig för konstruktion av sådana, straffas med fängelse i högst fem år eller med böter.

1.4. Föreslagna ändringar

I denna proposition föreslås det att en ny 9 a § skall fogas till 34 kap. strafflagen, som gäller allmänfarliga brott. I paragrafen kriminaliseras orsakande av fara för informationsbehandling. Såsom ovan konstaterats i samband med beskrivningen av nuläget, strävar man i allmänhet inte genom spridande av virus efter att skada någon särskild information som finns på en viss plats. Eftersom tillverkning och spridande av virus är ett typiskt brott som orsakar allmän fara, föreslås det att bestämmelsen skall tas in i 34 kap. strafflagen.

Enligt paragrafens *1 punkt* straffas den som för att orsaka olägenhet för informationsbehandling eller för ett data- eller telesystems funktion, tillverkar eller ställer till förfogande ett sådant datorprogram eller sådana programinstruktioner som har planerats för att äventyra informationsbehandling eller ett data- eller telesystems funktion eller för att skada data eller programvara som ingår i ett sådant system, eller sprider ett sådant datorprogram eller sådana programinstruktioner.

Av gärningsmannen förutsätts uppsåt, vilket i detta sammanhang inbegriper en avsikt att orsaka olägenhet för informationsbehandling eller för ett data- eller telesystems funktion. Begreppet "informationsbehandling" är ett omfattande begrepp som är avsett att innefatta all behandling och överföring av data som sker med hjälp av datateknik.

Med ett datasystem avses detsamma som i bestämmelsen om dataintrång i 38 kap. 8 § strafflagen, dvs. ett sådant datasystem där data behandlas, lagras eller överförs elektroniskt eller med någon annan sådan teknisk metod (se RP 94/1993 rd s. 152). Begreppet datasystem är i den bemärkelsen vidsträckt, att det inte enbart avser ett nät som består av flera databahandlings- och överföringsanordningar, utan också en enskild dator kan utgöra ett sådant datasystem som avses i paragrafen.

Med ett telesystem avses detsamma som med telenät i 38 kap. 3 § strafflagen till den del det är fråga om ett nät som lämpar sig för överföring av data som behandlats i ett datasystem. Enligt motiveringen till den sist nämnda bestämmelsen (RP 94/1993 rd s. 147) är ett telenät en helhet bestående av överföringsledningar samt övriga teleanordningar och telekonstruktioner, genom vilken samtal och andra meddelanden kan sändas med elektromagnetiska vågor. Ett telenät

kan t.ex. bestå av en organisations interna telefon- eller datakommunikationsnät. Med data- och telesystem avses således alla system som lämpar sig för automatisk databehandling, från en enskild dator till världsomfattande datanät.

Med olägenhet aves förutom direkt skada som uppkommer t.ex. genom att filer försvinner eller modifieras, även vilken som helst annan sådan inverkan på ett data- eller telesystems funktion som på något sätt kränker den rätt att använda systemet som tillkommer systemets innehavare eller någon annan som är berättigad att använda det, dvs. den s.k. informationsbehandlingsfriden. Det kan således vara fråga om en sådan olägenhet t.ex. då funktionen i ett system som infekterats med ett virus blir långsammare eller då det utrymme på en hårdskiva som upptas av viruset inte kan användas av den som har rätt att använda systemet.

Detta krav på uppsåt innebär att straffbarheten inte omfattar sådana situationer där t.ex. en person som är förtrogen med databehandling vill testa sin programmeringsskicklighet genom att skapa ett virusprogram utan att han har för avsikt att i något skede låta sitt verk spridas längre än till sin egen dator. Endast sådana gärningar där gärningsmannen från första början har haft för avsikt att sprida viruset och förorsaka olägenhet för informationsbehandlingen skall vara straffbara.

Som gärningssätt anges att tillverka, ställa till förfogande och sprida ovan nämnda program mm. Med tillverkning avses konstruktion av ett nytt program eller modifiering av ett existerande program så att det blir sådant som avses i paragrafen. Att ställa ett program till förfogande innebär närmast att ett virusprogram görs tillgängligt i ett datanät så att det allmänt kan kopieras. En typisk spridningsåtgärd är däremot t.ex. att en infekterad diskett används i en dator. Uppsåt förutsätter inte en uttrycklig spridningsavsikt, men gärningsmannen måste vara medveten om virusets existens och inse att dess spridning är en mycket sannolik följd av hans handlande.

Med uttrycket "datorprogram eller programinstruktioner" avses alla ovan i kapitel 1.1. beskrivna egentliga virus och program som påminner som dem. Programmen eller programinstruktionerna måste uttryckligen vara planerade så att de till sina egenskaper i första hand lämpar sig för att äventyra informationsbehandling eller ett data- eller telesystems funktion eller för att skada information eller programvara som ingår i ett sådant system. Programmet skall således vara konstruerat uttryckligen för detta syfte och gärningsmannen skall vara medveten om detta. Om ett program utan att dess konstruktör avsett det har fått någon egenskap som har ovan nämnda verkningar, är det inte fråga om ett sådant program som avses i paragrafen.

Straffbarheten förutsätter inte att gärningen i praktiken förorsakar konkret olägenhet för informationsbehandling eller för ett data- eller telesystems funktion, eller att den information eller programvara som systemet innehåller i praktiken skadas. Det är tillräckligt att programmen eller programinstruktionerna är planerade att förorsaka fara eller skada. I praktiken innebär detta t.ex. att om ett virus som har infekterat ett datasystem upptäcks innan det hunnit aktiveras och förorsaka skada, kan viruskonstruktören då de övriga förutsättningarna är uppfyllda åläggas straffansvar för sin gärning. Om man i en persons dator hittar ett virus som denna konstruerat, men som inte ännu har spritts, kan konstruktören straffas om det framgår att han uttryckligen har tillverkat viruset i avsikt att förorsaka skada för informationsbehandling eller ett data- eller telesystems funktion, dvs. få viruset att sprida sig.

Sådan fara eller skada som avses i paragrafen kan i första hand uppkomma till följd av att ett virus efter att det har aktiverats helt eller delvis avbryter ett data- eller telesystems funktion eller förändrar systemets funktion eller den information som systemet innehåller.

Ett virus som infekterat ett system kan avbryta systemets funktion helt eller delvis. Det kan också förändra systemets funktion så att systemet t.ex. producerar annan slags information än vad som ursprungligen var avsikten. Beträffande detta enskilda datasystem är det då fråga om en situation som till verkningarna påminner om sådant informationsbehandlingsbedrägeri som avses i 36 kap. 1 § 2 mom. strafflagen. A andra sidan förändras ett systems funktion redan av att ett virus som t.ex. infekterat hårdskivan i en dator förbrukar skivutrymme och gör datorns funktion långsammare. Redan en förändring av en bit påverkar dessutom integriteten vid informationsbehandlingen, vilket innebär att den lagrade informationens be-

visvärde kan bli lidande.

Ett virus kan också modifiera data som ingår i ett system antingen genom att utplåna dem eller på något annat motsvarande sätt. I ett sådant fall är det fråga om en situation som till verkningarna kan jämföras med sådan skadegörelse som avses i 35 kap. 1 § 2 mom. strafflagen.

Enligt paragrafens *2 punkt* straffas också den som ställer till förfogande anvisningar för tillverkning av ett sådant datorprogram eller sådana programinstruktioner som avses i 1 punkten eller som sprider sådana anvisningar. Med anvisningar avses i detta sammanhang sådana detaljerade anvisningar på basis av vilka en person som i någon mån är förtrogen med informationsbehandling kan konstruera ett virus. Att sprida eller ställa sådana anvisningar till förfogande är med avseende på gärningens potentiella farlighet i det närmaste fullt jämförbart med att sprida eller ställa ett färdigt virus till förfogande, vilket betyder att det är motiverat att samma straffhot skall gälla i fråga om denna gärning. Eftersom anvisningarna dock inte kan spridas av sig själva på samma sätt som ett färdigt program, förorsakas det inte ännu sådan fara enbart av att anvisningar skrivs att det skulle finnas skäl att göra också tillverkningen straffbar.

Medan det är möjligt att sprida eller ställa ett virus till förfogande endast genom användande av datateknik, kan anvisningar ställas till förfogande eller spridas förutom med hjälp av datateknikens metoder också t.ex. i en tryckt skrift.

Även i fråga om att sprida och ställa anvisningar till förfogande är det en förutsättning för straffbarhet att gärningsmannen har handlat i avsikt att orsaka olägenhet förinformationsbehandling eller för ett data- eller telesystems funktion.

Den föreslagna brottsrubriken är *orsakande av fara för informationsbehandling*. Ordet "automatisk" har avsiktligen lämnats bort ur rubriken, eftersom man i allmänt språkbruk så småningom håller på att frångå begreppet "automatisk informationsbehandling". Det framgår av paragrafens innehåll att bestämmelsen uttryckligen gäller informationsbehandling som grundas på datateknik.

Som straffskala föreslås böter eller fängelse i högst två år. Skalan är densamma som i 34 kap. 9 § strafflagen som gäller förberedelse till allmänfarligt brott. Den föreslagna bestämmelsen påminner till sin karaktär delvis om den nämnda paragrafen. Skalan ger lagtillämparen tillräckligt med spelrum, eftersom de gärningar som avses i paragrafen till sin farlighet kan vara mycket olika. Som värst kan gärningen i praktiken innebära att det förorsakas fara som kan jämföras med sådan fara för någons liv eller hälsa som avses i 21 kap. 13 § strafflagen. I de allra allvarligaste fallen kan bestämmelsen om sabotage i 34 kap. 1 § 2 mom. strafflagen tillämpas på gärningen.

Med tanke på utredningen av dessa brott är det även viktigt att straffskalan är tillräckligt sträng för att ge förundersökningsmyndigheterna befogenheter att använda behövliga tvångsmedel.

Denna paragraf skall inte tillämpas om det i någon annan lag föreskrivs strängare eller lika strängt straff för gärningen.

Om ett virus har aktiverats och orsakat olägenhet eller skada eller konkret fara för dessa, kan man beroende på uppsåtet hos den som har konstruerat eller spritt viruset, i fråga om gärningen tillämpa t.ex. bestämmelsen i 35 kap. 2 § strafflagen om grov skadegörelse, bestämmelsen i 36 kap. 1 § 2 mom. om bedrägeri och bestämmelsen i 2 § om grovt bedrägeri samt bestämmelsen i 38 kap. 5 § om störande av post- och teletrafik och bestämmelsen i 6 § om grovt störande av post- och teletrafik, för vilka det anges lika stränga eller strängare straffhot än för orsakande av fara för informationsbehandling. Då bestämmelsen i 35 kap. 1 § 2 mom. om skadegörelse kan tillämpas på gärningen, skall både bestämmelsen om skadegörelse och den föreslagna bestämmelsen tillämpas. Detta är motiverat på grund av att framställning och spridande av virus i alla händelser är en gärning som så slumpartat orsakar konkreta följder, att det straff som utdöms för gärningen inte enbart kan vara beroende av gärningens följder, vilka i praktiken kan vara mycket små trots gärningens stora potentiella farlighet.

2. 46 kap. strafflagen

2.1. Nuläge

46 kap. strafflagen reviderades i samband med det första skedet av strafflagens totalreform genom en lag som trädde i kraft den 1 januari 1991. I 6 § i detta kapitel intogs bestämmelser om olaga befattningstagande

med infört gods. Denna paragraf ersatte den tidigare paragrafen i 38 kap. 13 § där det bestämdes bötesstraff för den som anskaffade, dolde eller forslade gods som införts till landet med undansnillande av tullavgift eller genom lurendrejeri. Som straff för olaga befattningstagande med infört gods anges böter eller fängelse i högst sex månader. Det finns inga separata bestämmelser om lindriga och grova gärningsformer.

Med avseende på de gärningssätt som uppräknas i bestämmelsen om olaga befattningstagande med infört gods ("döljer, anskaffar, omhändertar eller förmedlar"), motsvarar paragrafen bestämmelsen om häleri i 32 kap. 1 § strafflagen. Som förbrott till olaga befattningstagande med infört gods kan det vara fråga om regleringsbrott, grovt regleringsbrott, lindrigt regleringsbrott, smuggling, lindring smuggling, skattebedrägeri, grovt skattebedrägeri och lindrigt skattebedrägeri. Som förbrott till häleri anges stölds-, förskingrings-, rån-, utpressnings-, bedrägeri-, ocker- eller betalningsmedelsbedrägeribrott, gäldenärsbedrägeri, grovt gäldenärsbedrägeri och uppsåtligt gäldenärssvek. Straffskalan för häleribrott är böter eller fängelse i högst ett år och sex månader och för grovt häleri kan man döma ut fängelse i minst fyra månader och högst fyra år och för yrkesmässigt häleri fängelse i minst fyra månader och högst sex år. Påföljden för häleriförseelse är böter.

Motiveringen till 46 kap. 6 § strafflagen i regeringens proposition (RP 66/1988 rd s. 174-175) innehåller inte någon ingående utredning av frågan om straffskalan och i motiveringen tas det inte heller ställning till behovet av en grovhetsindelning. Praxis har särskilt under de senaste åren utvisat att rekvisitet för olaga befattningstagande med infört gods kan uppfyllas också av sådant förfarande vars objekt är mycket värdefull egendom. I april 1997 dömdes en person som hade omhändertagit fyra miljoner cigarretter som hade smugglats till Finland för olaga befattningstagande med infört gods. Om förbrottet hade varit t.ex. stöld istället för smuggling, hade utgångspunkten varit att gärningsmannens förfarande otvivelaktigt skulle ha bedömts på basis av bestämmelsen om grovt häleribrott.

I samband med att det har blivit lättare att överskrida gränser har det också blivit lättare att genomföra sådana brott som kommer i fråga som förbrott till olaga befattningstagande med infört gods och som kan rikta sig mot mycket värdefull egendom. Således är det motiverat att straffskalorna för olaga befattningstagande med infört gods revideras så att de bättre motsvarar straffskalorna för häleribrott.

2.2. Föreslagna ändringar

Olaga befattningstagande med infört gods

Det föreslås att straffskalan i 46 kap. 6 § strafflagen skall ändras så att maximistraffet istället för de gällande sex månaderna skall vara fängelse i ett år och sex månader. Då blir straffskalan densamma som för grundformen av häleri. Den föreslagna straffskalan gör det möjligt att behandla ett ärende vid endomarsammansättning då sådan behandling anses ändamålsenlig. Dessutom ger den föreslagna straffskalan förundersökningsmyndigheterna möjlighet att använda tillräckliga tvångsmedel, vilket inte för närvarande är möjligt.

Lindrigt befattningstagande med infört gods

Den största delen av de brott som uppfyller rekvisitet för olaga befattningstagande med infört gods är i själva verket mycket obetydliga. En typisk sådan gärning är t.ex. köp av några alkoholflaskor eller cigarrettkartonger som olagligen har införts i landet. Med tanke på sådana gärningar är det motiverat att lagen innehåller en separat bestämmelse om en lindrigare gärningsform, för vilken straff fortsättningsvis kan dömas ut genom strafforderförfarande. Därför föreslår man att det i lagen skall tas in en ny bestämmelse om lindrigt befattningstagande med infört gods (46 kap. 6 a §), för vilket påföljden skall vara böter.

Begränsningsstadgande, förverkande av egendom och procedurstadgande

Då en ny 6 a § fogas till kapitlet på det sätt som föreslagits, förutsätts det att de tekniska revideringar som föranleds av paragrafen görs i begränsningsstadgandet i 7 §, i stadgandet om förverkande av egendom i 8 § och i procedurstadgandet i 12 §.

3. Propositionens verkningar

Denna proposition utvidgar till de delar den gäller 34 kap. i viss mån området för straffbart förfarande, men detta förväntas inte föranleda någon betydande ökning av arbetsmängden för polis- eller åklagarmyndigheterna eller domstolarna. Det föreslagna tillägget till 34 kap. kan genom att det möjliggör användning av tvångsmedel vid förundersökningen å andra sidan förhindra uppkomsten av sådana eventuellt kännbara skador som kan förorsakas av det förfarande som avses i paragrafen. Propositionen har inga organisatoriska verkningar och den föranleder inga kostnader för staten.

4. Beredningen av propositionen

Denna proposition som till innehållet motsvarar den förfallna propositionen 233/1997 rd., har beretts vid justitieministeriet såsom tjänsteuppdrag. I samband med beredningen av revideringen beträffande 34 kap. har sakkunniga som representerat olika myndigheter och företag hörts.

5. Ikraftträdande

Lagen föreslås träda i kraft så snart som möjligt efter det att den har antagits och blivit stadfäst.

Med stöd av vad som anförts ovan föreläggs Riksdagen följande lagförslag:

Lag

om ändring av strafflagen

I enlighet med riksdagens beslut

ändras i strafflagen av den 19 december 1889 (39/1889) 46 kap. 6 §, 7 § 2 och 3 mom., 8 § 3 mom. och 12 §, sådana de lyder i lagen 769/1990, samt

fogas till 34 kap. en ny 9 a § samt till 46 kap. en ny 6 a § som följer:

34 kap.

Om allmänfarliga brott

9 a §

Orsakande av fara för informationsbehandling

Den som för att orsaka olägenhet för informationsbehandling eller ett data- eller telesystems funktion,

1) tillverkar eller ställer till förfogande ett sådant datorprogram eller sådana programinstruktioner som har planerats för att äventyra informationsbehandling eller ett data- eller telesystems funktion eller för att skada data eller programvara som ingår i ett sådant system, eller sprider ett sådant datorprogram eller sådana programinstruktioner, eller

2) ställer till förfogande anvisningar för tillverkning av ett sådant datorprogram eller sådana programinstruktioner som avses i 1 punkten eller sprider sådana anvisningar,

skall, om inte strängare eller lika strängt straff föreskrivs för gärningen i annan lag, för *orsakande av fara för informationsbehandling* dömas till böter eller fängelse i högst två år.

46 kap.

Om regleringsbrott och smuggling

6 §

Olaga befattningstagande med infört gods

Den som döljer, anskaffar, omhändertar eller förmedlar egendom vilken vid införseln i landet har varit föremål för ett brott som avses i 1—5 § eller 29 kap. 1—3 §, eller som annars tar befattning med sådan egendom trots att han vet att egendomen har förts in på detta sätt, skall för *olaga befattningstagande med infört gods* dömas till böter eller fängelse i högst ett år och sex månader.

6 a §

Lindrigt olaga befattningstagande med infört gods

Om olaga befattningstagande med infört gods, med beaktande av egendomens värde eller övriga omständigheter i samband med brottet, bedömt som en helhet är ringa, skall gärningsmannen för *lindrigt olaga befattningstagande med infört gods* dömas till böter.

7 §

Begränsningsstadgande

— — — — — — — — — — — — — — —

För ett brott som avses i 6 och 6 a § döms inte den som är delaktig i ett brott som har begåtts vid införseln av godset.

Bestämmelser i 6 och 6 a § tillämpas inte på den som har gemensamt hushåll med gärningsmannen och som endast använder eller förbrukar egendom som gärningsmannen har anskaffat för det gemensamma hushållets normala behov.

8 §

Förverkande av egendom

— — — — — — — — — — — — — — —

Ett transportmedel, vilket har använts för ett brott som avses i 1—6 a § eller för skattebedrägeri som avses i 6 och 6 a § och vilket har byggts om för att göra det lättare att dölja brottsobjektet eller för att på något annat sätt underlätta brott, kan dömas förverkat till staten. Också andra transportmedel kan dömas förverkade, om de huvudsakligen har använts för ett sådant brott.

12 §

Procedurstadgande

Den för vilken eller med vars samtycke ett brott som avses i 1—6 a § har begåtts, och den som har känt till ett sådant brott och till vilken egendomen har överförts efter det brottet begicks, kan dömas till en förverkandepåföljd enligt detta kapitel trots att åtal inte har väckts mot honom eller gärningsmannen eller trots att gärningsmannen inte har ådömts straff.

Denna lag träder i kraft den .

Helsingfors den 7 maj 1999

Republikens President

MARTTI AHTISAARI

Justitieminister *Johannes Koskinen*

Bilaga

Lag

om ändring av strafflagen

I enlighet med riksdagens beslut
ändras i strafflagen av den 19 december 1889 (39/1889) 46 kap. 6 §, 7 § 2 och 3 mom., 8 § 3 mom. och 12 §, sådana de lyder i lagen 769/1990, samt
fogas till 34 kap. en ny 9 a § samt till 46 kap. en ny 6 a § som följer:

Gällande lydelse	*Föreslagen lydelse*
46 kap.	
Om regleringsbrott och smuggling	
6 §	
Olaga befattningstagande med infört gods	
Den som döljer, anskaffar, omhändertar eller förmedlar egendom vilken vid införseln i landet har varit föremål för ett brott som avses i 1—5 § eller 29 kap. 1—3 §, eller som annars tar befattning med sådan egendom trots att han vet att egendomen har förts in på detta sätt, skall för *olaga befattningstagande med infört gods* dömas till böter eller fängelse i högst sex månader.	Den som döljer, anskaffar, omhändertar eller förmedlar egendom vilken vid införseln i landet har varit föremål för ett brott som avses i 1—5 § eller 29 kap. 1—3 §, eller som annars tar befattning med sådan egendom trots att han vet att egendomen har förts in på detta sätt, skall för *olaga befattningstagande med infört gods* dömas till böter eller fängelse i högst *ett år och* sex månader.
	6 a §
	Lindrigt olaga befattningstagande med infört gods
(ny)	*Om olaga befattningstagande med infört gods, med beaktande av egendomens värde eller övriga omständigheter i samband med brottet, bedömt som en helhet är ringa, skall gärningsmannen för* ***lindrigt olaga befattningstagande med infört gods*** *dömas till böter.*
7 §	
Begränsningsstadgande	
För olaga befattningstagande med infört gods döms inte den som är delaktig i ett brott som har begåtts vid införseln av godset.	För ett brott som avses i 6 och 6 a § döms inte den som är delaktig i ett brott som har begåtts vid införseln av godset.
Stadgandet i 6 § tillämpas inte på den som	*Bestämmelser* i 6 *och 6 a* § tillämpas inte

Gällande lydelse	*Föreslagen lydelse*
har gemensamt hushåll med gärningsmannen och som endast använder eller förbrukar egendom som gärningsmannen har anskaffat för det gemensamma hushållets normala behov.	på den som har gemensamt hushåll med gärningsmannen och som endast använder eller förbrukar egendom som gärningsmannen har anskaffat för det gemensamma hushållets normala behov.
8 §	
Förverkande av egendom	
Ett transportmedel, som har använts för ett brott som avses i 1—6 § eller skattebedrägeri som avses i 6 § och som har byggts om för att göra det lättare att dölja brottsobjektet eller för att på något annat sätt underlätta brott, kan dömas förverkat till staten. Också andra transportmedel kan dömas förverkade, om de huvudsakligen har använts för ett sådant brott.	Ett transportmedel, *vilket* har använts för ett brott som avses i 1—6 *a* § eller *för* skattebedrägeri som avses i 6 *och 6 a* § och *vilket* har byggts om för att göra det lättare att dölja brottsobjektet eller för att på något annat sätt underlätta brott, kan dömas förverkat till staten. Också andra transportmedel kan dömas förverkade, om de huvudsakligen har använts för ett sådant brott.
12 §	
Procedurstadgande	
Den för vilken eller med vars samtycke ett brott som avses i 1—6 § har begåtts, och den som har känt till ett sådant brott och till vilken egendomen har överförts efter det brottet begicks, kan dömas till en förverkandepåföljd enligt detta kapitel trots att åtal inte har väckts mot honom eller gärningsmannen eller trots att gärningsmannen inte har ådömts straff.	Den för vilken eller med vars samtycke ett brott som avses i 1—6 *a* § har begåtts, och den som har känt till ett sådant brott och till vilken egendomen har överförts efter det brottet begicks, kan dömas till en förverkandepåföljd enligt detta kapitel trots att åtal inte har väckts mot honom eller gärningsmannen eller trots att gärningsmannen inte har ådömts straff.
	Denna lag träder i kraft den .