Regeringens proposition 2003/04:164

Sveriges antagande av rambeslut om angrepp mot informationssystem

Prop. 2003/04:164

Regeringen överlämnar denna proposition till riksdagen.

Stockholm den 27 maj 2004

Göran Persson

Thomas Bodström
(Justitiedepartementet)

Propositionens huvudsakliga innehåll

I propositionen föreslås att riksdagen godkänner det inom Europeiska unionen upprättade utkastet till rambeslut om angrepp mot informationssystem. Rambeslutet innehåller bestämmelser om vilka handlingar som skall vara straffbelagda som angrepp mot informationssystem och vilka straffrättsliga påföljder dessa brott skall kunna leda till. Bestämmelserna avser att träffa t.ex. spridande av datavirus. Dessutom finns bestämmelser om bl.a. ansvar och påföljder för juridiska personer, domsrätt och utbyte av uppgifter. I propositionen redovisas en bedömning av de lagändringar som rambeslutet föranleder i svensk rätt. Några förslag till ändrad lagstiftning lämnas dock inte. Sådana kommer att läggas fram i ett senare sammanhang.

Innehållsförteckning

1 Förslag till riksdagsbeslut

Regeringen föreslår att riksdagen godkänner det inom Europeiska unionen upprättade utkastet till rambeslut om angrepp mot informationssystem.

2 Ärendet och dess beredning

Den 19 april 2002 presenterade Europeiska kommissionen ett förslag till rambeslut om angrepp mot informationssystem (EGT C 203 E, 27.8.2002, s. 109). En faktapromemoria om förslaget upprättades och överlämnades till riksdagen (2001/02:FPM110).

Europaparlamentet yttrade sig över förslaget den 22 oktober 2002 (A5-0328/2002, EUT C 300 E, 11.12.2003, s. 16).

Förslaget till rambeslut behandlades vid fem tillfällen i rådets arbetsgrupp för materiell straffrätt och den 23 och 24 januari samt den 19 och 20 februari 2003 av den samordningskommitté av höga tjänstemän som inrättats i enlighet med artikel 36 i Fördraget om Europeiska unionen. Förslaget behandlades sedan av Coreper den 26 februari 2003. Därefter träffade rådet för rättsliga och inrikes frågor en politisk överenskommelse om innehållet i rambeslutet vid sitt möte den 27 och 28 samma månad.

Regeringen har under förhandlingsarbetet fortlöpande informerat och samrått med riksdagen. I samband därmed har regeringen gett in en promemoria till riksdagen inför rådet för rättsliga och inrikes frågor den 27 och 28 februari 2003 (RD 2002/03:2952, EUJu2003/311/EU).

Vid Europeiska rådets möte den 25 och 26 mars 2004 antogs, mot bakgrund av terroristattackerna i Madrid den 11 samma månad, en deklaration om bekämpande av terrorism. I deklarationen slås fast att ett antal rambeslut beträffande vilka det föreligger politiska överenskommelser, däribland rambeslutet om angrepp mot informationssystem, skall antas i juni 2004. För att rådet skall kunna anta rambeslutet måste det först godtas av de nationella parlamenten i de medlemsstater där det krävs parlamentsgodkännande och sedan måste parlamentsreservationerna hävas. Antagandet kräver enhällighet.

Utkastet till rambeslut i senaste svensk version är fogad till denna proposition som *bilaga 1*. I *bilaga 2* finns ett utkast till uttalande av kommissionen som skall tas till rådets protokoll i samband med att rambeslutet antas.

I denna proposition behandlas frågan om riksdagens godkännande av utkastet till rambeslut och görs en bedömning av de lagändringar som rambeslutet föranleder. Några förslag till lagstiftning om genomförande av åtagandena i rambeslutet lämnas inte av skäl som anges i avsnitt 5. Sådana förslag kommer att läggas fram i ett senare sammanhang. Svea hovrätt, Justitiekanslern (JK), Riksåklagaren, Rikspolisstyrelsen, Säkerhetspolisen, Post- och telestyrelsen, Krisberedskapsmyndigheten, Försvarsmakten, Försvarets radioanstalt, Uppsala universitet och Sveriges advokatsamfund har under hand beretts tillfälle att lämna synpunkter på ett utkast till propositionen (dnr Ju2004/4752/L5). Ett remissförfarande av traditionellt slag har inte tillämpats vid beredningen, eftersom det har ansetts oundgängligen påkallat av den tidsram som gäller för EU:s antagande av rambeslutet att i stället ta underhandskontakter med myndigheter och andra. En sådan beredning kan under de angivna omständigheterna ersätta en traditionell remissbehandling (jfr bet. 2002/03:KU10 s. 64).

Myndigheterna har varit positiva till eller inte haft någon erinran mot regeringens förslag att riksdagen skall godkänna utkastet till rambeslut. De har vidare instämt i eller inte invänt mot regeringens bedömning av vilka lagändringar som rambeslutet torde föranleda. Myndigheterna har

dock lämnat vissa andra synpunkter, bl.a. har några framfört att det bör införas ett grovt dataintrångsbrott eller en strängare straffskala för dataintrång även om inte rambeslutet kräver det. Advokatsamfundet däremot har ansett att samfundet inte kan tillstyrka att rambeslutet antas av de skälen att ett traditionellt remissförfarande inte föregått propositionen och att propositionen saknar lagförslag.

3 Bakgrund

3.1 Frågans tidigare behandling inom EU

Europeiska rådet antog den 3 december 1998 i Wien en handlingsplan för att på bästa sätt genomföra bestämmelserna i Amsterdamfördraget om upprättandet av ett område med frihet, säkerhet och rättvisa (EGT C 19, 23.1.1999, s. 1–15). I handlingsplanen anges i punkten 46 att Europeiska unionen bör vidta åtgärder för att, om det anses nödvändigt, fastställa minimiregler avseende brottsrekvisit och påföljder på bl.a. områdena terrorism och organiserad brottslighet. I handlingsplanen nämndes vidare databrott.

Den 15 och 16 oktober 1999 höll Europeiska rådet ett särskilt möte i Tammerfors om skapandet av ett område med frihet, säkerhet och rättvisa i unionen. Europeiska rådet förklarade då att insatserna för att enas om gemensamma definitioner, brottsbeskrivningar och påföljder i ett första skede bör begränsas till ett antal sektorer med särskild betydelse, däribland högteknologisk brottslighet.

Vid Europeiska rådets möte i Santa Maria da Feira den 19 och 20 juni 2000 godkände Europeiska rådet en övergripande handlingsplan för *e*Europa. Handlingsplanen innefattade åtgärder för att förbättra säkerheten på Internet och skapa en samordnad och enhetlig strategi för bekämpande av databrottslighet.

Under 2000 offentliggjorde Europeiska kommissionen ett meddelande med titeln ”Ett säkrare informationssamhälle – ökad säkerhet i informationsinfrastrukturen och bekämpning av datorrelaterad brottslighet” (KOM [2000] 890 slutlig). I meddelandet föreslogs en strategi för att bekämpa problemen med databrottslighet. I ytterligare ett meddelande från kommissionen 2001 med rubriken ”Nät- och informationssäkerhet: förslag till en europeisk strategi” analyserades problem rörande nätsäkerhet och presenterades också en strategisk plan för åtgärder inom området (KOM [2001] 298 slutlig). I de båda kommissionsmeddelandena angavs att det finns behov av en snabb tillnärmning av den materiella straffrätten i Europeiska unionen när det gäller angrepp mot informationssystem. Det sistnämnda meddelandet följdes upp med rådets resolution av den 6 december 2001 om nät- och informationssäkerhet.

I två resolutioner från Europaparlamentet den 19 maj 2000 respektive den 5 september 2001 behandlades också problem med informationssäkerhet och högteknologisk brottslighet.

Kommissionen arbetar sedan 2000 med en resultattavla som innehåller en redogörelse för de framsteg som görs för att skapa ett område med frihet, säkerhet och rättvisa i EU. Varje halvår uppdaterar kommissionen

resultattavlan genom ett meddelande till rådet och Europaparlamentet. I meddelandet för andra halvåret 2001, som presenterades den 30 oktober (KOM [2001] 628 slutlig), angav kommissionen att den avsåg att lägga fram ett förslag till rambeslut om gemensamma definitioner, brottsbeskrivningar och påföljder för angrepp mot informationssystem.

3.2 Närmare om rambeslutsprocessen

I artikel 29 i Fördraget om Europeiska unionen (FEU) anges att unionens mål skall vara att ge medborgarna en hög säkerhetsnivå inom ett område med frihet, säkerhet och rättvisa genom att bl.a. utforma gemensamma insatser på områdena polissamarbete och straffrättsligt samarbete. Målet skall uppnås genom förebyggande och bekämpande av brottslighet, vare sig denna är organiserad eller inte, särskilt terrorism, människohandel och brott mot barn, olaglig narkotikahandel och olaglig vapenhandel, korruption och bedrägeri.

Av artikel 30.1 a FEU följer att de gemensamma insatserna på polissamarbetets område skall omfatta operativt samarbete mellan de behöriga myndigheterna, inbegripet polisen, tullen och andra specialiserade brottsbekämpande organ i medlemsstaterna för att förebygga, upptäcka och utreda brott.

Enligt artikel 31.1 e FEU skall det straffrättsliga samarbetet omfatta gradvisa beslut om åtgärder som fastställer minimiregler avseende brottsrekvisit och påföljder på områdena organiserad brottslighet, terrorism och olaglig narkotikahandel.

Artikel 34.2 b FEU anger att rådet genom enhälligt beslut på initiativ av en medlemsstat eller Europeiska kommissionen skall fatta rambeslut om tillnärmning av medlemsstaternas lagar och andra författningar. Rambesluten skall vara bindande för medlemsstaterna när det gäller de resultat som skall uppnås men skall överlåta åt de nationella myndigheterna att bestämma form och tillvägagångssätt.

Den 19 april 2002 presenterade kommissionen ett förslag till rambeslut om angrepp mot informationssystem (EGT C 203 E, 27.8.2002, s. 109). Vid rådet för rättsliga och inrikes frågor den 27 och 28 februari 2003 träffades en politisk överenskommelse om innehållet i rambeslutet. Dessförinnan hade Europaparlamentet yttrat sig över förslaget.

Vid Europeiska rådets möte den 25 och 26 mars 2004 antogs en deklaration om bekämpande av terrorism. Enligt deklarationen skall rambeslutet antas i juni 2004.

3.3 Europarådets konvention om IT-relaterad brottslighet

Rambeslutet om angrepp mot informationssystem har till stor del förebild i Europarådets konvention om IT-relaterad brottslighet (Convention on Cybercrime ETS no.:185). Konventionen antogs av Europarådets ministerkommitté den 8 november 2001. Sverige undertecknade konventionen den 23 november samma år. Sverige har också den 28 januari 2003 undertecknat ett tilläggsprotokoll till konventionen. Protokollet innefattar

åtaganden att kriminalisera rasistiska och främlingsfientliga handlingar som begås med hjälp av datorsystem.

Konventionen innehåller bestämmelser om vilka handlingar som skall vara straffbelagda som olagligt intrång i datorsystem, datastörning och störning av datorsystem (artiklarna 2, 4 och 5). Dessa artiklar och bestämmelser i konventionen om definitioner (artikel 1) har tjänat som förebild för rambeslutets motsvarande reglering. Därutöver innehåller konventionen ytterligare straffbestämmelser om IT-relaterade brott bl.a. olaglig avlyssning, datorrelaterad förfalskning och datorrelaterat bedrägeri. Konventionen innehåller också ett flertal straffprocessuella bestämmelser och bestämmelser om internationellt samarbete.

Frågan om konventionen och protokollet bör ratificeras av Sverige bereds för närvarande inom Justitiedepartementet. Eftersom konventionen innehåller bestämmelser som går utöver de som finns i rambeslutet och också rör helt andra områden, kräver konventionen till stor del andra överväganden än de som rambeslutet föranleder. För att inte fördröja ett antagande av rambeslutet kommer rambeslutet att behandlas fristående från frågan om ratificering av konventionen. Frågan om ett kommande genomförande av rambeslutet bör samordnas med en eventuell ratificering av konventionen får besvaras i ett senare sammanhang. Det kan dock redan nu konstateras att de lagändringar som kan bedömas nödvändiga för att genomföra rambeslutet i princip torde motsvara vad som krävs enligt konventionens bestämmelser om intrång i datorsystem och störningar av data och datorsystem.

4 Innehållet i rambeslutet om angrepp mot informationssystem och gällande svensk rätt

4.1 Inledning

Rambeslutet syftar till att tillnärma medlemsstaternas straffrättsliga lagstiftning när det gäller angrepp mot informationssystem och därigenom förbättra samarbetet mellan rättsliga och andra myndigheter.

Rambeslutet innehåller bestämmelser om definitioner (artikel 1), olagligt intrång i informationssystem (artikel 2), olaglig systemstörning (artikel 3), olaglig datastörning (artikel 4), kriminalisering av anstiftan, medhjälp och försök (artikel 5), påföljder och försvårande omständigheter (artiklarna 6 och 7), ansvar och påföljder för juridiska personer (artiklarna 8 och 9), behörighet (artikel 10) och utbyte av uppgifter (artikel 11). Dessutom finns bestämmelser om genomförande och ikraftträdande av rambeslutet (artiklarna 12 och 13).

Av artikel 47 i Fördraget om Europeiska unionen följer att rambeslutet inte inverkar på gemenskapsrätten. Det gäller särskilt de rättigheter eller skyldigheter som är förknippade med skydd för privatlivet eller uppgiftsskydd enligt direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation. Avsikten är inte heller att ålägga medlemsstaterna att kriminalisera

t.ex. intrång i immateriella rättigheter. Rambeslutet hindrar inte heller tillämpningen av direktiv 98/84/EG om det rättsliga skyddet för tjänster som bygger på eller utgörs av villkorad tillgång. Dessa områden omfattas alltså av befintlig gemenskapslagstiftning.

4.2 Ingressen

I ingressen till rambeslutet anges att rådet antar rambeslutet med beaktande av dels Fördraget om Europeiska unionen, särskilt artiklarna 29, 30.1 a, 31.1 e och 34.2 b, dels kommissionens förslag och Europaparlamentets yttrande. Vidare hänvisas till bl.a. tidigare åtgärder på området.

I ingressen uttalas att det har konstaterats att det förekommer angrepp mot informationssystem, särskilt till följd av hotet från den organiserade brottsligheten. Enligt ingressen finns det en ökande oro för terroristattacker mot informationssystem som ingår i medlemsstaternas vitala infrastruktur. Vidare betonas att informationssystemens nationsöverskridande och gränslösa karaktär innebär att angrepp mot sådana system ofta är gränsöverskridande.

Mot denna bakgrund understryks behovet av bl.a. gemensamma definitioner och brottsrekvisit samt påföljder. En sådan tillnärmning av medlemsstaternas strafflagstiftning sägs kunna förbättra samarbetet mellan rättsliga och andra behöriga myndigheter och bidra till kampen mot organiserad brottslighet och terrorism.

4.3 Artikel 1 Definitioner

I *artikel 1* definieras vissa begrepp som används i rambeslutet, särskilt i artiklarna om vilka gärningar som skall vara straffbelagda i medlemsstaterna. Punkterna a och b innehåller definitioner av tekniska begrepp, nämligen informationssystem och datorbehandlingsbara uppgifter. I punkterna c och d anges vad som avses med begreppet juridisk person respektive begreppet orättmätigt.

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

Datorbehandlingsbara uppgifter är enligt *punkt b* framställning av fakta, information eller begrepp i en form som lämpar sig för behandling i ett informationssystem, inklusive program som lämpar sig för att få ett informationssystem att utföra en viss uppgift.

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

Punkt d innehåller en definition av begreppet orättmätigt. Definitionen innebär att ett intrång är orättmätigt eller att en störning är orättmätig om handlingen sker utan tillstånd från ägaren eller annan rättighetshavare till

systemet eller del av detta. Definitionen innebär vidare att handlingen är orättmätig om den inte medges i nationell lagstiftning.

Betydelsen av dessa definitioner för rambeslutet och i svensk lagstiftning behandlas i samband med de artiklar där definitionerna används.

4.4 Artiklarna 2–4 Olagligt intrång i informationssystem, olaglig systemstörning och olaglig datastörning

Artikel 2 Olagligt intrång i informationssystem

Artikel 2 innebär att medlemsstaterna skall straffbelägga handlande som utgör olagligt intrång i informationssystem.

Det som skall kriminaliseras är enligt *punkt 1* uppsåtligt orättmätigt intrång i ett informationssystem som helhet eller en del av ett sådant system, åtminstone i fall som inte är ringa.

Med definitionen av informationssystem i artikel 1 a innebär bestämmelsen att det uppsåtliga intrånget skall ske i en apparat eller en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av datorbehandlingsbara uppgifter, eller i sådana datorbehandlingsbara uppgifter som lagras, behandlas, hämtas eller överförs med hjälp av dessa för att de skall kunna drivas, användas, skyddas och underhållas. Med datorbehandlingsbara uppgifter i stort avses enligt artikel 1 b framställning av fakta, information eller begrepp i en form som lämpar sig för behandling i ett informationssystem, inklusive program som lämpar sig för att få ett informationssystem att utföra en viss uppgift. Kravet på att intrånget skall vara orättmätigt innebär, vilket följer av definitionen i artikel 1 d, att intrånget skall ske utan tillstånd från ägaren eller annan rättighetshavare till systemet eller del av detta. Vidare skall intrånget inte medges i nationell lagstiftning.

Av *punkt 2* följer att varje medlemsstat får besluta att det handlande som avses i punkt 1 endast skall kriminaliseras, om brottet begås genom intrång i en säkerhetsåtgärd.

Artikel 3 Olaglig systemstörning

Enligt *artikel 3* skall medlemsstaterna kriminalisera visst handlande som olaglig systemstörning. I artikeln föreskrivs att det skall vara straffbart att uppsåtligen allvarligt hindra eller avbryta driften av ett informationssystem genom att mata in, överföra, skada, radera, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter, om gärningen utförs orättmätigt, åtminstone i fall som inte är ringa.

Definitionen av informationssystem i artikel 1 a innebär att artikeln omfattar uppsåtligt allvarligt hindrande eller avbrytande, genom någon av de nämnda åtgärderna, av driften av en apparat eller en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av datorbehandlingsbara uppgifter, eller av datorbehandlingsbara uppgif-

ter som lagras, behandlas, hämtas eller överförs med hjälp av dessa för att de skall kunna drivas, användas, skyddas och underhållas. Datorbehandlingsbara uppgifter i stort är enligt artikel 1 b framställning av fakta, information eller begrepp i en form som lämpar sig för behandling i ett informationssystem, inklusive program som lämpar sig för att få ett informationssystem att utföra en viss uppgift.

Kravet på att systemstörningen skall vara orättmätig innebär enligt artikel 1 d att det skall vara fråga om en störning som sker utan tillstånd från ägaren eller annan rättighetshavare till systemet eller del av detta. Vidare skall störningen inte medges i nationell lagstiftning.

Artikel 4 Olaglig datastörning

Artikel 4 avser olaglig datastörning. Enligt artikeln skall det vara straffbart att uppsåtligen radera, skada, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter i ett informationssystem, om gärningen utförs orättmätigt, åtminstone i fall som inte är ringa.

Enligt definitionen av datorbehandlingsbara uppgifter i artikel 1 b avses med sådana uppgifter framställning av fakta, information eller begrepp i en form som lämpar sig för behandling i ett informationssystem, inklusive program som lämpar sig för att få ett informationssystem att utföra en viss uppgift. Det straffbara området skall alltså omfatta uppsåtligt raderande etc. av sådana framställningar under förutsättning att störningen är orättmätig. Kravet på orättmätighet, vilket definieras i artikel 1 d, innebär att störningen skall ske utan tillstånd från ägaren eller annan rättighetshavare till systemet eller del av detta. Det innebär vidare att störningen inte skall medges i nationell lagstiftning.

Gällande svenska ansvarsbestämmelser

Rambeslutets bestämmelser om vilka handlingar som skall vara straffbelagda torde närmast motsvaras av de svenska straffbestämmelserna om dataintrång, skadegörelse och grov skadegörelse. Också bestämmelserna om sabotage och grovt sabotage är av intresse. I sammanhanget skall dessutom nämnas att grov skadegörelse, sabotage och grovt sabotage är straffbart som terroristbrott enligt lagen (2003:148) om straff för terroristbrott under de förutsättningar som anges i lagen.

För *dataintrång* döms den som olovligen bereder sig tillträde till upptagning för automatisk databehandling eller olovligen ändrar eller utplånar eller i register för in sådan upptagning. Med upptagning avses även uppgifter som är under befordran via ett elektroniskt eller annat liknande hjälpmedel för att användas för automatisk databehandling (4 kap. 9 c § brottsbalken). Bestämmelsen är subsidiär i förhållande till bl.a. bestämmelsen om brytande av post- eller telehemlighet (4 kap. 8 § brottsbalken).

Dataintrångsbestämmelsen infördes i brottsbalken 1998 då datalagen (1973:289) ersattes av personuppgiftslagen (1998:204) och datalagens

bestämmelse om dataintrång i 21 § överfördes till brottsbalken utan ändring i sak.

I propositionen till datalagen uttalades i fråga om bestämmelsens tekniska tillämpningsområde att med upptagning för automatisk databehandling avses uppgift som är fixerad på någon form av datamedium och som alltså antingen finns i eller kan matas in i en datamaskin. Vidare angavs att i begreppet ligger också att informationen är läsbar endast med ADB-teknik (prop. 1973:33 s. 75). Genom en lagändring 1986 i 21 § datalagen infördes tillägget att med sådan upptagning avses även uppgifter som är under befordran via ett elektroniskt eller liknande hjälpmedel för att användas för automatisk databehandling. Tillägget avsåg överföringar av uppgifter som ännu inte fixerats på ett datamedium (prop. 1985/86:65 s. 30 ff.). Syftet med tillägget var att komplettera det skydd för uppgifter som överförs via förbindelser för datakommunikation som bestämmelsen om brytande av telehemlighet och dataintrångsbestämmelsen redan gav. Enligt bestämmelsen om brytande av telehemlighet är det straffbart att olovligen bereda sig tillgång till ett telemeddelande som förmedlas av telebefordringsföretag från en avsändare till en mottagare. Med telemeddelande avses ljud, text, bild, data eller information i övrigt.

Dataintrångsbestämmelsens tillämpningsområde i tekniskt hänseende är alltså i princip knutet till uppgifter, såväl informationsinnehåll som programvara. Trots att det saknas vägledande praxis i frågan, är det en rimlig tolkning av bestämmelsen att den är tillämplig så snart det kan styrkas att någon olovligen berett sig tillträde till en dator oavsett om det kan visas att personen berett sig tillträde till vissa uppgifter i datorn.

En annan fråga om bestämmelsens tillämpningsområde gäller om dess skydd för uppgifter som är under befordran men som ännu inte har fixerats på ett datamedium endast avser uppgifter som överförs i ledningsbundna nät eller även uppgifter som överförs via radio. Lagtexten i denna del talar om befordran via ett elektroniskt eller liknande hjälpmedel. När detta tillägg tillkom 1986 torde det ha varit endast ledningsbundna nät som lagstiftaren avsåg. Då var det nämligen i huvudsak genom sådana som överföringar av uppgifter skedde. I takt med att den tekniska utvecklingen sker är det inte lika givet att överföringar görs enbart på detta sätt. Lagtextens lydelse kan inte i sig anses utesluta att även överföringar som sker på annat sätt omfattas. Dessutom skyddar bestämmelsen i övrigt fixerade uppgifter som överförs. Å andra sidan måste i sammanhanget också beaktas att etern sedan länge anses vara fri. Det innebär att det i princip är straffritt att avlyssna meddelanden som befordras via radio (se t.ex. prop. 1992/93:200 s. 166 och 2002/03:110 s. 254). Den andra bestämmelsen som skyddar uppgifter under överföring – bestämmelsen om brytande av telehemlighet – anses i enlighet med detta inte tillämplig på radiobefordrade telemeddelanden. Mot denna bakgrund framstår det som osäkert om dataintrångsbestämmelsen omfattar uppgifter som ännu inte fixerats på ett datamedium och som är under befordran via radio.

Ansvar för dataintrång förutsätter uppsåt (1 kap. 2 § brottsbalken). Det krävs också att gärningen utförts olovligen. En gärning anses inte olovlig t.ex. om den sker med samtycke av den som förfogar över upptagningen eller i överensstämmelse med regler om tvångsmedel.

Det handlande som straffbeläggs i dataintrångsbestämmelsen är för det första att någon bereder sig tillgång till en sådan upptagning som nu nämnts. Det krävs inte att detta sker i ett visst syfte eller att det medför en effekt, t.ex. skada. Inte heller behöver någon säkerhetsåtgärd kringgås.

Vidare straffbeläggs att någon ändrar eller utplånar en sådan upptagning. En ändring kan gälla den upptagning som skall databehandlas. En ändring kan också göras i det datorprogram som styr den aktuella databehandlingen. Ändringen kan vara bestående eller tillfällig (Holmqvist m.fl. Brottsbalken En kommentar Kap. 1–12, s. 4:49). Att en upptagning utplånas innebär att den helt eller delvis förstörs, tex. genom radering.

Slutligen är det straffbelagt att föra in en upptagning i ett register. Denna del av dataintrångsbestämmelsen tillkom efter påpekande av Justitiekanslern (JK) under remissbehandlingen av det betänkande som låg till grund för propositionen om datalagen (SOU 1972:47). I betänkandet saknades alltså motsvarighet till den delen av bestämmelsen. JK ansåg att tolkningen av betänkandets förslag till straffbestämmelse kunde bli föremål för tvekan med hänsyn till att ingenting sades om obehöriga införingar. Enligt JK kunde det möjligen hävdas att en införing innebär en ändring av en upptagning. Frågan borde enligt JK klarläggas (prop. 1973:33 s. 68). Mot denna bakgrund ansåg föredragande departementschefen att det till straffbestämmelsen borde läggas det fallet att någon olovligen för in en ny upptagning (a. prop. s. 106).

Någon närmare diskussion om tillägget fördes inte i propositionen. Däremot berördes vad som skall förstås med begreppet register i samband med att vissa definitioner, däribland personregister, i den föreslagna datalagen behandlades (a. prop. s. 118). I den frågan uttalades i propositionen i huvudsak följande. Under begreppet bör falla förutom register även förteckningar och andra anteckningar. Uppenbarligen avses i första hand förteckningar som omfattar ett flertal faktiska uppgifter av likartat slag. I undantagsfall bör det emellertid kunna vara fråga om endast en uppgift. För att register skall anses föreligga måste det emellertid direkt eller indirekt vara fråga om behandling från informationssynpunkt av faktiska uppgifter. Ett ADB-register kan sålunda inte anses upprättat bara genom att löpande text lagras i ett datamedium, exempelvis för att sättning skall kunna ske med hjälp av ADB-teknik. Uppenbarligen faller på grund härav åtskillig databehandling av olika slags litteratur, främst skönlitteratur, utanför datalagens tillståndssystem. Först i den mån databehandlingen tar sikte på faktiska uppgifter i den litterära framställningen – såsom för upprättande av innehållsregister eller liknande – föreligger ett register i datalagens mening. Vidare bör ett register anses föreligga, om de lagrade uppgifterna skall användas för att framställa exempelvis en telefonkatalog, ett adressregister eller en taxeringskalender.

Uttalandena tyder på att registerbegreppet ansågs vara snävare än begreppet upptagning för automatisk databehandling. Å andra sidan gjordes vissa uttalanden i propositionen i anslutning till just dataintrångsbestämmelsen som inte klart gjorde en åtskillnad mellan begreppen. Det framhölls t.ex. att ”det behövs straffbestämmelser som helt allmänt skyddar datalagrat material”, att ”det är fråga om ett skydd för alla slag av dataregister”, att det var fråga om att ”någon olovligen för in en ny upptagning i ett datasystem” och om ”otillbörligt förfarande med datamaterial som anges i förevarande paragraf” (a. prop. s 105 f. och 145). Det kan alltså

synas oklart hur begreppet register skall förstås i dataintrångsbestämmelsen.

När det gäller införingar som sker i sådana upptagningar för automatisk databehandling som inte samtidigt kan betecknas som register kan de medföra att de befintliga upptagningarna ändras. Införingarna kan också medföra att upptagningarna eller delar därav utplånas. I sådana fall omfattas införingarna av den del av dataintrångsbestämmelsen som straffbelägger ändring eller utplånande av upptagningar. Det kan dock förekomma fall då införingar i befintliga upptagningar som inte utgör register inte kan anses ändra eller utplåna upptagningarna. Ett exempel härpå utgör s.k. tillgänglighetsattacker, se närmare nedan i avsnitt 5. Sådana situationer faller i dag utanför dataintrångsbestämmelsens tillämpningsområde. Om införingar däremot görs i register utan att de samtidigt ändrar eller utplånar registren, omfattas de som redan nämnts av dataintrångsbestämmelsen i den del den uttryckligen tar sikte på införingar i register.

Att förstöra eller skada egendom, fast eller lös, till men för annans rätt därtill, är straffbart som *skadegörelse* (12 kap. 1 § brottsbalken). Om gärningen har inneburit synnerlig fara för någons liv eller hälsa eller skadan drabbat sak av stor kulturell eller ekonomisk betydelse eller skadan annars är synnerligen kännbar, är gärningen att anse som *grov skadegörelse* (12 kap. 3 § brottsbalken). För *sabotage* döms den som förstör eller skadar egendom, som har avsevärd betydelse för rikets försvar, folkförsörjning, rättsskipning eller förvaltning eller för upprätthållande av allmän ordning och säkerhet i riket, eller genom annan åtgärd, som inte innefattar endast undanhållande av arbetskraft eller uppmaning därtill, allvarligt stör eller hindrar användningen av sådan egendom (13 kap. 4 § brottsbalken). Detsamma gäller om någon annars genom skadegörelse eller annan åtgärd som nyss sagts allvarligt stör eller hindrar den allmänna samfärdseln eller användningen av telegraf, telefon, radio eller dylikt allmänt hjälpmedel eller av anläggning för allmänhetens förseende med vatten, ljus, värme eller kraft. Om fara för rikets säkerhet, för flera människoliv eller för egendom av särskild betydelse framkallats genom brottet, kan dömas för *grovt sabotage* (13 kap. 5 § brottsbalken).

Frågan om rambeslutets bestämmelser om vilka handlingar som skall vara straffbelagda kräver lagändringar i svensk rätt behandlas i avsnitt 6.1.

4.5 Artikel 5 Anstiftan, medhjälp och försök

I *artikel 5 punkt 1* anges att anstiftan av och medhjälp till brott som avses i artiklarna 2–4 skall vara straffbart. Enligt *punkt 2* skall försök att begå dessa brott också vara straffbart. Varje medlemsstat får dock enligt *punkt 3* besluta att inte tillämpa punkt 2 för de brott som avses i artikel 2, dvs. olagliga intrång i informationssystem.

Gällande svenska ansvarsbestämmelser

Enligt den allmänna medverkansbestämmelsen i brottsbalken (23 kap. 4 §) gäller ansvar som är föreskrivet för viss gärning inte endast den som

har utfört gärningen utan även den som har främjat gärningen med råd eller dåd. Med uttrycket ”råd eller dåd” avses att främjandet skall ha skett med psykiska eller fysiska medel. Enligt normalt språkbruk främjas en gärning när någon har gjort något som underlättar eller i vart fall är ägnat att underlätta gärningens utförande. I brottsbalken har dock uttrycket givits en vidare betydelse och kan även innefatta medverkan som inte utgjort någon förutsättning för brottet. Att ett främjande av en gärning är straffbart såsom medverkan, även om det inte är en förutsättning för att gärningen skall komma till stånd, medför att medverkansansvar kan komma i fråga även för den som endast obetydligt bidragit till gärningen.

Den som inte är att anse som gärningsman skall dömas för anstiftan av brottet, om han eller hon har förmått annan till utförandet, och annars för medhjälp till detta. Av detta följer att medverkan kan ha tre former enligt svensk rätt: gärningsmannaskap, anstiftan och medhjälp. Mellan dessa olika former gäller en prioritetsordning. Gärningsmannaskap har företräde framför de båda andra medverkansformerna och anstiftan ses som allvarligare än medhjälp. Varje medverkande är självständigt ansvarig, dvs. oberoende av om det är möjligt att straffa någon annan medverkande. Ansvaret är dock beroende av att en straffbelagd gärning utförts. Varje medverkande bedöms efter det uppsåt eller den oaktsamhet som ligger honom eller henne till last.

Bestämmelsen gäller vid alla brottsbalksbrott samt de brott i specialstraffrätten för vilka fängelse är föreskrivet eller för vilka en särskild föreskrift finns om att medverkan skall bestraffas.

Medverkan till brottsbalksbrotten dataintrång och straffbart försök till dataintrång samt skadegörelse, grov skadegörelse, sabotage och grovt sabotage och försök till dessa brott är alltså straffbart.

Försök till brott är straffbart i de fall det finns ett särskilt stadgande om det (23 kap. 1 § brottsbalken). Den som påbörjat utförandet av ett visst brott utan att detta kommit till fullbordan, skall dömas för försök till brottet, om det förelegat fara för att handlingen skulle leda till brottets fullbordan eller sådan fara endast på grund av tillfälliga omständigheter varit utesluten.

Försök till dataintrång som om det fullbordats inte skulle ha varit att anse som ringa är straffbelagt (4 kap. 10 § brottsbalken). Försök till skadegörelse, grov skadegörelse, sabotage och grovt sabotage är också straffbelagt (12 kap. 5 § och 13 kap. 12 § brottsbalken).

I avsnitt 6.1 behandlas frågan om eventuella lagstiftningsåtgärder i anledning av rambeslutets bestämmelser om anstiftan, medhjälp och försök.

4.6 Artikel 6 Påföljder

Artikel 6 föreskriver vilka påföljder som skall kunna dömas ut för de brott som anges i artiklarna 2–5.

Punkt 1 innebär att brotten i artiklarna 2–5, dvs. olagligt intrång i informationssystem, olaglig systemstörning och olaglig datastörning samt anstiftan av, medhjälp till och försök till dessa brott, skall vara belagda med effektiva, proportionella och avskräckande straffrättsliga påföljder.

Enligt *punkt 2* skall de brott som avses i artiklarna 3 och 4, dvs. olaglig systemstörning och olaglig datastörning, vara belagda med straffrättsliga påföljder som innebär ett maximistraff på minst ett till tre års fängelse.

Gällande svenska påföljdsbestämmelser

Straffskalan för dataintrång är böter eller fängelse i högst två år. För skadegörelse och grov skadegörelse är straffskalorna böter eller fängelse i högst ett år respektive fängelse i högst fyra år. Straffskalorna för sabotage och grovt sabotage är fängelse i högst fyra år respektive fängelse i lägst två år och högst tio år eller på livstid.

Straffet för försök bestäms högst till vad som gäller för fullbordat brott (23 kap. 1 § brottsbalken) och får inte sättas under fängelse om lägsta straff för det fullbordade brottet är fängelse i två år eller däröver.

För anstiftan och medhjälp gäller sedvanliga straffskalor. Det finns dock en möjlighet till straffnedsättning vid medverkan i vissa fall (23 kap. 5 § brottsbalken).

I avsnitt 6.2 behandlas frågan om rambeslutets bestämmelser om påföljder kräver lagstiftningsåtgärder.

4.7 Artikel 7 Försvårande omständigheter

Artikel 7 innehåller bestämmelser om försvårande omständigheter.

I *punkt 1* föreskrivs att de brott som avses i artikel 2.2 och artiklarna 3 och 4 skall vara belagda med straffrättsliga påföljder som innebär ett maximistraff på minst två till fem års fängelse, om de begås inom ramen för en sådan kriminell organisation som avses i gemensam åtgärd 98/733/RIF (gemensam åtgärd av den 21 december 1998 om att göra deltagande i en kriminell organisation i Europeiska unionens medlemsstater till ett brott), oberoende av den påföljdsnivå som anges i den gemensamma åtgärden. De gärningar som avses är olagligt intrång i informationssystem som begås genom intrång i en säkerhetsåtgärd, olaglig systemstörning och olaglig datastörning.

Punkt 2 innehåller en fakultativ bestämmelse. Enligt den får en medlemsstat även vidta de åtgärder som avses i punkt 1, när brottet har orsakat allvarliga skador eller påverkat väsentliga intressen.

Gällande svenska bestämmelser om försvårande omständigheter

I svensk rätt finns bestämmelser om försvårande omständigheter vid straffmätning (29 kap. 2 § brottsbalken). Exempelvis skall såsom en försvårande omständighet vid bedömningen av ett brotts straffvärde särskilt beaktas om brottet har utgjort ett led i en brottslig verksamhet som varit särskilt noggrant planlagd eller bedrivits i stor omfattning och i vilken den tilltalade spelat en betydande roll (2 § 6).

I avsnitt 4.6 redovisas vilka straff som kan följa på de svenska brott som rambeslutets bestämmelser i första hand aktualiserar.

Frågan om rambeslutets bestämmelser om försvårande omständigheter föranleder lagändringar behandlas i avsnitt 6.2.

4.8 Artiklarna 8 och 9 Ansvar och påföljder för juridiska personer

Artiklarna 8 och 9 innehåller bestämmelser om ansvar och påföljder för juridiska personer. Med juridisk person förstås enligt artikel 1 c enhet som har sådan status enligt tillämplig lagstiftning, med undantag av stater eller andra offentliga organ vid utövandet av de befogenheter som de har i egenskap av statsmakter samt internationella offentliga organisationer.

Artikel 8 punkt 1 föreskriver att varje medlemsstat skall vidta nödvändiga åtgärder för att se till att juridiska personer kan ställas till ansvar för brott som avses i artiklarna 2–5 och som begås till deras förmån av en person som agerar antingen enskilt eller som en del av den juridiska personens organisation och har en ledande ställning inom denna organisation. Den ledande ställningen skall vara grundad på

a) befogenhet att företräda den juridiska personen,

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

c) befogenhet att utöva kontroll inom den juridiska personen.

Enligt *artikel 8 punkt 2* skall medlemsstaterna dessutom se till att en juridisk person kan ställas till ansvar när brister i övervakning eller kontroll som skall utföras av en sådan person som avses i punkt 1 har gjort det möjligt för en person som är underställd den juridiska personen att begå sådana brott som avses i artiklarna 2–5 till förmån för den juridiska personen.

Artikel 8 punkt 3 anger att en juridisk persons ansvar enligt punkterna 1 och 2 inte skall utesluta lagföring av fysiska personer som är gärningsmän vid, anstiftare av eller medhjälpare till de brott som avses i artiklarna 2–5.

Av *artikel 9 punkt 1* följer att varje medlemsstat skall vidta de åtgärder som är nödvändiga för att se till att en juridisk person som har fällts till ansvar i enlighet med artikel 8 punkt 1 kan bli föremål för effektiva, proportionella och avskräckande påföljder. Enligt bestämmelsen skall påföljderna innefatta bötesstraff eller administrativa avgifter. Vidare får de innefatta andra påföljder som

a) frånatagande av rätt till offentliga förmåner eller stöd,

b) tillfälligt eller permanent näringsförbud,

c) rättslig övervakning, eller

d) rättsligt beslut om upplösning av verksamheten.

Enligt *artikel 9 punkt 2* skall varje medlemsstat vidta nödvändiga åtgärder för att se till att en juridisk person som har fällts till ansvar i enlighet med artikel 8 punkt 2 kan bli föremål för effektiva, proportionella och avskräckande påföljder eller åtgärder.

I svensk rätt finns bestämmelser om företagsbot (36 kap. 7–10 §§ brottsbalken). Bestämmelserna innebär att näringsidkare kan åläggas företagsbot för brott som har begåtts i utövningen av näringsverksamhet. En förutsättning är att brottsligheten har inneburit ett grovt åsidosättande av de särskilda skyldigheter som är förenade med verksamheten eller annars är av allvarligt slag. Dessutom krävs att näringsidkaren inte har gjort vad som skäligen kunnat krävas för att förebygga brottsligheten. Av bestämmelserna följer också bl.a. hur företagsbotens storlek skall fastställas.

I avsnitt 6.3 behandlas frågan om eventuella lagstiftningsåtgärder i anledning av rambeslutets bestämmelser om ansvar och påföljder för juridiska personer.

4.9 Artikel 10 Behörighet

I *artikel 10* anges under vilka förutsättningar medlemsstaterna skall ha behörighet att döma över de brott som omfattas av rambeslutet (domsrätt). Dessutom anvisas ett samrådsförfarande då flera av medlemsstaterna har behörighet att döma över samma brott.

Enligt *punkt 1* skall varje medlemsstat fastställa sin behörighet beträffande de brott som anges i artiklarna 2–5 när brottet har begåtts

a) helt eller delvis på dess territorium,

b) av en av dess medborgare, eller

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

Av *punkt 2* följer att medlemsstaten vid fastställandet av sin behörighet enligt punkt 1 a skall se till att behörigheten innefattar fall där

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

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

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

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

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

– Medlemsstaten skall vara den i vilken gärningsmannen är medborgare.

– Medlemsstaten skall vara den på vars territorium gärningsmannen påträffats.

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

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

Gällande svenska behörighetsregler

Svenska regler om straffrättslig behörighet (domsrätt) finns främst i 2 kap. brottsbalken. För brott som har begåtts här i riket döms efter svensk lag och vid svensk domstol (1 §). Detsamma gäller om det är ovisst var ett brott förövats men det finns skäl att anta att det är begånget inom riket. Ett brott anses begånget där den brottsliga handlingen företogs, så ock där brottet fullbordades eller, vid försök, där brottet skulle ha fullbordats (4 §).

För brott som har begåtts utom riket döms också efter svensk lag och vid svensk domstol, om brottet har begåtts av svensk medborgare eller utlänning med hemvist i Sverige (2 §). Den svenska behörigheten beträffande utomlands begångna brott gäller också i vissa särskilt angivna fall andra utlänningar, exempelvis utlänning som efter brottet har blivit svensk medborgare eller utlänning som vistas i Sverige, om brottet i sistnämnda fall kan medföra fängelse i mer än sex månader. Behörighetsreglerna förutsätter att gärningen inte är fri från ansvar enligt lagen på gärningsorten. Härutöver har svenska domstolar en formellt vidsträckt behörighet att döma för brott som begåtts utomlands, bl.a. för brott som har förövats mot Sverige, svensk kommun eller annan menighet eller svensk allmän inrättning och brott som har ett minimistraff på minst fyra års fängelse (3 §). Det finns dock ett principiellt krav på åtalsförordnande för utomlands begångna gärningar (5 § andra stycket).

Internationella straffrättsutredningen har i betänkandet Internationella brott och svensk jurisdiktion (SOU 2002:98) presenterat bl.a. ett förslag till en ny lydelse av 2 kap. brottsbalken. Betänkandet har remitterats och bereds för närvarande inom Justitiedepartementet. Förslaget innebär i sak inte några förändringar som har betydelse för åtagandena om behörighet i rambeslutet.

Enligt lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder, som trädde i kraft den 1 januari 2004, får inte överlämnande vägras enbart på den grunden att den som eftersöks för lagföring är medborgare i den anmodade staten. Lagen, som genomför ett rambeslut, tillämpas i förhållande till andra EU-stater i stället för tidigare utlämningsförfaranden, låt vara att bestämmelser i lagen (1957:668) om utlämning för brott övergångsvis kommer att vara tillämpliga i förhållan-

de till medlemsstater som inte hunnit genomföra rambeslutet i tid. I vissa fall kommer också lagen (1959:254) om utlämning för brott till Danmark, Finland, Island och Norge att alltjämt vara tillämplig i förhållande till medlemsstaterna Danmark och Finland. Enligt de båda utlämningslagarna får svenska medborgare i vissa fall inte utlämnas till andra EU-stater.

I avsnitt 6.4 behandlas frågan om de svenska behörighetsreglernas överensstämmelse med rambeslutet.

4.10 Artikel 11 Utbyte av uppgifter

I *artikel 11* finns bestämmelser om utbyte av uppgifter.

I *punkt 1* föreskrivs att för utbyte av uppgifter om de brott som avses i artiklarna 2–5 skall medlemsstaterna, med iakttagande av bestämmelser om dataskydd, säkerställa att de använder det befintliga nät med operativa kontaktpunkter som kan nås dygnet runt alla dagar i veckan.

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

Frågan om hur bestämmelserna om utbyte av uppgifter förhåller sig till svensk rätt behandlas i avsnitt 6.5.

4.11 Artikel 12 Genomförande

Artikel 12 anger när rambeslutet skall vara genomfört i nationell rätt och hur genomförandet skall följas upp.

Enligt *punkt 1* skall medlemsstaterna senast två år efter det att rambeslutet har trätt i kraft vidta de åtgärder som är nödvändiga för att följa bestämmelserna i rambeslutet.

Punkt 2 föreskriver att medlemsstaterna senast vid samma tidpunkt till rådets generalsekretariat och kommissionen skall överlämna texten till bestämmelser genom vilka skyldigheterna enligt rambeslutet införlivas med deras nationella lagstiftning. Vidare föreskrivs att rådet senast 30 månader efter rambeslutets ikraftträdande, på grundval av en rapport som skall utarbetas utifrån information och en skriftlig rapport från kommissionen, skall bedöma i vilken utsträckning medlemsstaterna har följt bestämmelserna i rambeslutet.

4.12 Artikel 13 Ikraftträdande

Enligt *artikel 13* träder rambeslutet i kraft samma dag som det offentliggörs i Europeiska unionens officiella tidning.

4.13 Uttalande

I samband med att rambeslutet antas skall ett uttalande från kommissionen tas till rådets protokoll. I utkastet till uttalandet beklagar kommissionen att artikeln om påföljder (artikel 6 punkt 2) saknar föreskrift om ett minimistraff för olagligt intrång i informationssystem (artikel 2).

5 Antagande av rambeslutet

Regeringens förslag: Riksdagen godkänner det inom Europeiska unionen upprättade utkastet till rambeslut om angrepp mot informationssystem.

Skälen för regeringens förslag

Angrepp mot informationssystem

Dagens samhälle präglas av att informationsteknik genomsyrar i stort sett alla sektorer. Det innebär samtidigt att samhället är sårbart för olika former av angrepp som riktar sig mot informationssystem, såsom olovliga intrång i systemen och störningar av systemen och av data i systemen.

Datavirus och andra sabotageprogram förstör eller ändrar uppgifter och kan avbryta eller hindra driften av informationssystem men kan också förvanska innehållet på t.ex. webbplatser och webbsidor. Vissa program orsakar skador på själva datorn medan andra i stället utnyttjar datorn för att angripa andra apparater i samma nät. En del program – ofta kallade logiska bomber – kan ligga inaktiva tills de aktiveras genom en viss händelse, t.ex. att ett visst datum infaller, och då förstöra eller modifiera uppgifter. Andra program utlöser angrepp när de öppnas. Dessa kallas ofta trojanska hästar. Ytterligare en typ av program, s.k. datamaskar, kopierar sig själva. Kopiorna skapar sedan ännu fler kopior, vilket leder till att systemet till sist översvämmas av kopiorna. Ett vanligt sätt att sprida datavirus och andra sabotageprogram är i bilagor till elektronisk post eller på webbplatser.

Det förekommer även s.k. tillgänglighetsattacker eller på engelska Denial of Service-attacker (DoS-attacker). Sådana attacker kan innebära att informationssystem blockeras eller att funktionen hos systemen kraftigt sätts ned genom automatiskt genererade meddelanden. Sådana överbelastningar kan liknas vid fall där faxar blockeras av långa och upprepade meddelanden. Program som skickar stora mängder elektronisk post kan avbryta eller allvarligt hindra driften hos informationssystem. Detsamma kan gälla manuella sändningar i stor skala av elektronisk post. Andra typer av attacker innefattar t.ex. störningar av servrar som hanterar domännamnssystemet (DNS).

Det förekommer också kombinationer av de nu nämnda formerna av attacker. Som exempel kan nämnas datavirus som sprids i bilagor till elektronisk post. När viruset infekterar en dator öppnas samtidigt en hemlig s.k. bakdörr till datorn som gör att datorn senare tillfälligt kan användas för att genomföra tillgänglighetsattacker.

Under senare år synes angrepp mot informationssystem ha blivit allt vanligare. Som exempel kan nämnas dataviruset Loveletter och masken Sobig.f., som båda snabbt spred sig över hela världen. I öppna nät, som exempelvis Internet, är det möjligt att relativt enkelt sprida t.ex. nyskapade datavirus. Spridningen följer ibland vissa mönster bl.a. beroende av operativsystem, språk som används i ett elektroniskt brev eller brister i program och datorutrustning. Vissa attacker kan genomföras snabbt men vara svåra att använda för att nå precisa mål. Datavirus kan få en snabb men okontrollerad spridning. Tillgänglighetsattacker har i flera fall haft tydliga mål. Att kartlägga och undersöka system för att få t.ex. ökad precision eller effekt i attacker kan dock vara kostsamt och ta lång tid. Det ökar också risken för att bli upptäckt. Tillgänglighetsattacker har riktats mot nätoperatörer och Internetleverantörer. Det finns en risk att IT-system inom t.ex. industrin, sjukvården eller myndigheter kan utsättas för allvarliga tillgänglighetsattacker över öppna nät eller mer avancerade intrång och attacker i systemen. Även andra kan utsättas. Angreppen kan orsaka betydande kostnader och ekonomiska förluster eller annars få allvarliga konsekvenser. De riskerar också att göra informationssystemen dyrare och därmed mindre överkomliga för användarna. Förtroendet för den nya tekniken och elektroniska tjänster som t.ex. 24-timmarsmyndigheter kan också skadas.

Angreppen utförs ofta av enskilda individer som handlar på eget initiativ. Utvecklingen går emellertid i den riktningen att den organiserade brottsligheten i allt högre utsträckning angriper informationssystem i olagliga syften. Det finns exempelvis organiserade grupper som förstör webbplatser och sedan erbjuder de drabbade ”hjälp” med att återställa webbplatserna mot ersättning. Det finns också en stigande oro i världen för att terroristattacker skall riktas mot informationssystem, främst sådana system som ingår i staters samhällsviktiga infrastruktur. Hur omfattande och allvarlig brottsligheten är i Sverige råder det delade meningar om (se BRÅ-rapport 2002:2 s. 49 och SOU 2000:25 s. 178 och 208). Däremot råder det enighet om att den måste tas på allvar.

Behovet av EU-gemensamma regler

Angreppen mot informationssystem utgör ett hot mot skapandet av ett säkert informationssamhälle och ett område med frihet, säkerhet och rättvisa. Redan i Fördraget om Europeiska unionen, artikel 29, anges att unionens mål inom detta område skall uppnås genom straffrättsligt samarbete och polissamarbete. Bland den brottslighet som särskilt nämns där finns terrorism. Av fördragets artikel 34.2 b följer att tillnärmning av medlemsstaternas lagstiftning skall ske genom rambeslut. I ett antal olika sammanhang inom unionen har betonats att ett effektivt svar på hoten mot informationssystemen kräver en samlad syn på informationssäkerhet och gemensamma regler om högteknologisk brottslighet.

Det finns ett mervärde i att på EU-nivå utforma gemensamma beskrivningar av vilka handlingar som skall anses utgöra straffbara angrepp mot informationssystem och vilka påföljder dessa brott skall kunna leda till. Därigenom skapas ett gemensamt rättsområde som underlättar det rättsliga och polisiära samarbetet för att förebygga och bekämpa sådan brotts-

lighet. Syftet är också att förbättra möjligheterna att bekämpa den organiserade brottsligheten och terrorism. Det upprättade utkastet till rambeslut om angrepp mot informationssystem tillnärmar medlemsstaternas straffrättsliga lagstiftning på detta sätt. Rambeslutet skall också ses som ett komplement till rambeslutet om bekämpande av terrorism (EGT L 164, 22.6.2002, s. 3). Rambeslutet om bekämpande av terrorism innehåller bl.a. bestämmelser om straffbara terroristhandlingar som orsakar omfattande förstörelse av infrastruktur, däribland informationssystem, och som kan utsätta människoliv för fara eller förorsaka betydande ekonomiska skador. Den betydelse som rambeslutet om angrepp mot informationssystem anses ha för kampen mot terrorism har också kommit till uttryck i Europeiska rådets deklaration den 25 och 26 mars 2004 om bekämpande av terrorism där det slås fast att rambeslutet skall antas i juni 2004.

Också inom Europarådet har behovet av gemensamma regler om IT-relaterade brott uppmärksammats. Europarådets konvention om IT-relaterad brottslighet, som presenterats närmare i avsnitt 3.3, innehåller bl.a. bestämmelser om vilka handlingar som skall vara straffbara som IT-relaterade brott. Sverige har undertecknat konventionen och frågan om att ratificera den bereds för närvarande inom Justitiedepartementet.

Sverige intar en framträdande position som IT-nation och det är naturligt att som en del i ett säkert informationssamhälle ha en straffrättslig lagstiftning som ger ett skydd mot direkta angrepp mot och missbruk av tekniken. Sverige stödjer vidare kampen mot terrorism, som bl.a. förs genom en harmonisering av straffrätten på olika områden i EU:s medlemsstater. Sverige har också deltagit aktivt i EU och annat internationellt samarbete som syftar till att förhindra och bekämpa angrepp mot informationssystem och terrorism. Mot denna bakgrund måste det anses vara av yttersta vikt att åstadkomma en ny, förbättrad EU-gemensam lagstiftning mot angrepp mot informationssystem.

Sverige bör anta rambeslutet

Som redogörs för i avsnitt 6 nedan innehåller rambeslutet bestämmelser som, om rambeslutet antas, föranleder vissa ändringar av svensk lag. Ändringarna rör vilka handlingar som skall vara straffbelagda och innebär att det straffbara området i vissa avseenden utvidgas. Dessa handlingar avser förfaranden som även från svensk utgångspunkt måste anses straffvärda. Ändringarna får därmed anses behövliga. Ändringarna torde också kunna genomföras i svensk rätt med bibehållande av den nuvarande systematiken. Utformningen av lagändringarna kräver dock noggranna överväganden. Ett beredningsunderlag grundat på en utförlig och omsorgsfull analys av relevanta frågeställningar måste hämtas in. Det vore givetvis önskvärt att den lagstiftning som rambeslutet föranleder presenteras samtidigt som rambeslutet läggs fram för riksdagens godkännande. I den ovan nämnda deklarationen mot terrorism anges att antagandet skall ske i juni 2004. Att avvakta med ett godkännande till dess att ett beredningsunderlag har hämtats in och förslag till lagstiftning kan presenteras skulle emellertid innebära en avsevärd försening av antagandet av rambeslutet. Sverige bör mot bakgrund av deklarationen och för att visa sitt fortsatta stöd för unionens gemensamma arbete på detta område

verka för att rambeslutet antas snarast möjligt. Eftersom rambeslutet enligt artikel 34.2 b i Fördraget om Europeiska unionen är bindande för medlemsstaterna och då det innehåller bestämmelser som kräver lagändringar, krävs – som redan framgått – riksdagens godkännande innan Sverige röstar för ett antagande av rambeslutet i ministerrådet (10 kap. 2 § regeringsformen). Regeringen föreslår därför att riksdagen godkänner det upprättade utkastet till rambeslut om angrepp mot informationssystem.

6 Behovet av lagändringar

6.1 Handlingar som skall vara straffbelagda

Regeringens bedömning: Svensk rätt uppfyller till övervägande del rambeslutets krav på vilka handlingar som skall vara straffbelagda. De svenska bestämmelserna torde dock inte fullt ut motsvara rambeslutets krav när det gäller att avbryta eller allvarligt hindra ett informationssystems drift och att hindra flödet av datorbehandlingsbara uppgifter eller göra sådana uppgifter oåtkomliga. I dessa avseenden torde alltså krävas lagändringar.

Skälen för regeringens bedömning

Allmänt om rambeslutets straffbestämmelser

Rambeslutet innehåller bestämmelser om att olagliga intrång i informationssystem, olagliga systemstörningar och olagliga datastörningar skall vara straffbelagda. Det får dock göras undantag för ringa fall. Vidare följer av artikel 47 i Fördraget om Europeiska unionen att rambeslutet inte påverkar Europeiska gemenskapernas behörighet. Detta innebär i praktiken att instrument som antagits på det område som regleras i första pelaren – till skillnad mot rambeslutet som behandlas inom ramen för tredje pelaren – inte påverkas och att nationell svensk lagstiftning med anledning av sådana instrument därmed kan lämnas opåverkad. Detta gäller t.ex. direktiv om intrång i immateriella rättigheter i en digital miljö.

Olagligt intrång i informationssystem

Enligt *artikel 2* i rambeslutet skall uppsåtligt orättmätigt intrång i ett informationssystem som helhet eller en del av ett sådant system vara straffbart, åtminstone i fall som inte är ringa.

Den svenska dataintrångsbestämmelsen straffbelägger uppsåtlig olovlig tillgång till upptagning för automatisk databehandling. Såväl rambeslutets bestämmelse som dataintrångsbestämmelsen förutsätter alltså för det första att gärningen begås med uppsåt. Vidare krävs enligt rambeslutet att gärningen utförs orättmätigt och enligt bestämmelsen om dataintrång att gärningen är olovlig. Till begreppet orättmätigt anknyter ingresskäl 13 där det bl.a. sägs att det finns ett behov av att undvika att krimi-

nalisera rättighetshavare och behöriga personer. Kravet på orättmätighet innebär alltså att handlingar som i och för sig uppfyller övriga krav för straffbarhet enligt rambeslutet men som utförs av eller med tillstånd från ägare eller annars behöriga personer i ett företag eller liknande i enlighet med behörigheten inte omfattas av det straffbara området. Huruvida en person intar en sådan ställning får avgöras på samma sätt som gäller i andra sammanhang. När det gäller offentliga webbplatser bör vidare den som tillhandahåller webbplatsen anses ha lämnat tillstånd i rambeslutets mening. Allmänheten kan därmed besöka webbplatsen utan att anses göra sig skyldig till orättmätigt intrång. Ibland ställer en innehavare upp vissa regler, som krav på betalning eller annat, för att en webbplats skall få besökas. Den som iakttar uppställda regler kan inte anses ha orättmätigt berett sig tillgång till webbplatsen. Detsamma gäller den som använder normala tekniker, t.ex. länkar, för att få tillgång till en webbplats. Utanför det straffbara området faller vidare handlingar som medges i nationell lagstiftning. Det kan här vara fråga om brottsbekämpande åtgärder som exempelvis hemlig teleövervakning. Den innebörd av begreppet orättmätigt som nu beskrivits måste anses motsvara vad som enligt dataintrångsbestämmelsen bör förstås med olovligt.

Rambeslutets krav på att handlingen skall bestå i ett intrång motsvarar dataintrångsbestämmelsens krav på att det skall vara fråga om att bereda sig tillgång. Det svenska brottet rubriceras för övrigt data*intrång*. Intrånget skall vidare enligt rambeslutet ha skett i ett informationssystem. Definitionen av vad som utgör ett sådant system innebär att det straffbara området omfattar intrång i datorutrustning, t.ex. persondatorer, fickdatorer och mobiltelefoner som har vissa databehandlingsfunktioner såsom WAP. Vidare omfattas datorbehandlingsbara uppgifter för drift, användning, skydd och underhåll. Det svenska begreppet upptagning för automatisk databehandling måste anses täcka det som i rambeslutet avses med informationssystem.

Dataintrångsbestämmelsen torde följaktligen redan i dag straffbelägga det område som enligt artikel 2 i rambeslutet skall vara kriminaliserat som olagligt intrång i informationssystem. Enligt rambeslutet är det dessutom möjligt för en medlemsstat att som ytterligare krav för straffbarhet föreskriva att gärningen skall begås genom intrång i en säkerhetsåtgärd för att vara straffbar. Dataintrångsbestämmelsen förutsätter inte att en säkerhetsåtgärd kringgås.

Sammanfattningsvis gör alltså regeringen bedömningen att svensk rätt torde uppfylla rambeslutets krav på att olagligt intrång i informationssystem skall vara straffbelagt.

Olaglig systemstörning

Enligt *artikel 3* skall det vara straffbart att uppsåtligen och orättmätigt allvarligt hindra eller avbryta driften av ett informationssystem genom att mata in, överföra, skada, radera, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter, åtminstone i fall som inte är ringa.

Rekvisiten ”mata in” och ”överföra” är av särskild relevans när det gäller s.k. tillgänglighetsattacker. Övriga rekvisit avser särskilt problemet

med datavirus och andra former av sabotageprogram som förstör eller modifierar uppgifter. Angående vad som avses med dessa olika former av attacker, se avsnitt 5.

I svensk rätt straffbeläggs som dataintrång att olovligen ändra eller utplåna en upptagning för automatisk databehandling eller att föra in en sådan upptagning i register. Bestämmelsen förutsätter uppsåt och motsvarar därvidlag rambeslutets bestämmelse. Vidare innehåller båda bestämmelserna krav på att handlingen skall utföras olovligen respektive orättmätigt. Innebörden av dessa två begrepp måste anses vara densamma. I denna fråga hänvisas till vad som sagts i föregående avsnitt om olagligt intrång i informationssystem. Här bör dock tilläggas att sedvanliga åtgärder såsom att testa säkerheten hos ett system eller att installera nya program, som vidtas av behöriga personer i enlighet med behörigheten, inte utgör olagliga störningar av informationssystem även om driften hos systemet allvarligt hindras eller avbryts genom åtgärderna.

Enligt rambeslutet skall handlingen riktas mot ett informationssystem. Definitionen av vad som utgör ett sådant system innebär att det som avses är dels apparater som automatiskt behandlar datorbehandlingsbara uppgifter, dels datorbehandlingsbara uppgifter för drift, användning, skydd och underhåll av apparaterna. Samtidigt är det så att angreppet sker genom användning av eller påverkan på datorbehandlingsbara uppgifter i allmänhet. Det svenska upptagningsbegreppet i dataintrångsbestämmelsen måste, som redan konstaterats i avsnittet om olagligt intrång ovan, anses omfatta det som avses med informationssystem i rambeslutet.

Den handling som skall vara straffbelagd enligt rambeslutet består i att allvarligt hindra eller att avbryta driften av ett informationssystem. Hur dessa störningar kan åstadkommas anges, som redan framgått, genom en uppräkning. Störningarna kan sålunda orsakas genom att någon matar in, överför, skadar, raderar, försämrar, ändrar, hindrar flödet av eller gör det omöjligt att komma åt datorbehandlingsbara uppgifter. Det svenska dataintrångsbrottet förutsätter att någon ändrar eller utplånar en upptagning för automatisk databehandling eller att någon för in en sådan upptagning i ett register.

Att ändra eller utplåna måste anses motsvara de handlingar i rambeslutet som benämns att skada, radera, försämra och ändra. Också rambeslutets handlingar att hindra flödet av och göra det omöjligt att komma åt datorbehandlingsbara uppgifter torde i vissa fall kunna åstadkommas genom en ändring i eller ett utplånande av en upptagning eller möjligen rentav genom ett införande i ett register enligt dataintrångsbestämmelsen. Dessutom är det straffbart att olovligen bereda sig tillgång till en upptagning, också när det sker som ett led i ett handlande som går ut på att göra uppgifter otillgängliga. Emellertid torde inte dataintrångsbrottet täcka samtliga de situationer där datorbehandlingsbara uppgifter hindras eller görs oåtkomliga. Exempelvis torde det vara tveksamt om bestämmelsen gäller i fall där så sker endast temporärt. Uppgifterna kan då knappast anses utplånade eller ändrade. I denna del torde en lagändring bli nödvändig, om inte andra svenska straffbestämmelser omfattar dessa situationer.

Innan dessa bestämmelser diskuteras skall också beröras rambeslutets krav på att inmatningar och överföringar skall straffbeläggas. I många

fall torde dessa handlingar utgöra dataintrång, eftersom de samtidigt medför att ursprungliga upptagningar ändras eller utplånas. Dessutom är det straffbart som dataintrång att göra införingar i register. Registerbegreppet torde dock vara snävare än begreppet upptagning för automatisk databehandling. Vidare är åtgärder som samtidigt innebär att någon olovligen bereder sig tillgång till en upptagning straffbara som dataintrång. Däremot torde dataintrångsbestämmelsen inte omfatta övriga införingar i eller överföringar till upptagningar för automatisk databehandling. Rambeslutet innebär emellertid att samtliga inmatningar och överföringar skall vara straffbara förutsatt att de avbryter eller allvarligt hindrar ett informationssystems drift. Det skall t.ex. vara straffbart att genom automatiskt genererade meddelanden kontakta eller försöka kontakta ett informationssystem så att systemet blockeras. Lagändringar torde därför vara nödvändiga i dessa avseenden för såvitt inte andra gällande straffbestämmelser uppfyller rambeslutets krav i dessa delar.

De straffbestämmelser som främst aktualiseras är reglerna om skadegörelse- och sabotagebrott. Dessa förutsätter som regel att gärningen medför en skada av inte endast tillfällig natur. För att ansvar skall komma i fråga förutsätts också att ett beteende som att skriva in ett kommando på ett tangentbord för att kontakta en dator kan betraktas som en skadegörande handling. Det finns inte någon rättspraxis som belyser den senare frågeställningen. Straffansvaret för skadegörelse och sabotage torde inte heller omfatta vissa av de situationer som enligt rambeslutet skall vara straffbelagda som systemstörning, t.ex. då skadan endast är tillfällig eller då det överhuvudtaget inte uppstår skada. Straffbestämmelsen om egenmäktigt förfarande (8 kap. 8 § brottsbalken), som omfattar bl.a. det fallet att någon olovligen rubbar annans besittning, kan vara tillämplig i dessa situationer om gärningen riktas mot en fysisk databärare men knappast i andra fall, eftersom brottet torde kräva en rumslig besittningsrubbning. Försök till egenmäktigt förfarande är för övrigt inte straffbelagt, vilket rambeslutet förutsätter att försök till olagliga systemstörningar skall vara.

Enligt svensk rätt är det vidare straffbart som undertryckande av urkund att förstöra, göra obrukbar eller undanskaffa en urkund över vilken vederbörande inte får förfoga på detta sätt, om åtgärden innebär fara i bevishänseende (14 kap. 4 § brottsbalken). Det kan diskuteras om denna bestämmelse kan tillämpas på de situationer som i rambeslutet beskrivs som att flödet av uppgifter hindras och att uppgifter görs oåtkomliga. Tillräcklig praxis i detta avseende liksom huruvida vissa andra liknande straffbestämmelser omfattar elektroniska rutiner saknas dock. Rättsläget får därmed anses som oklart. Det kan i detta sammanhang nämnas att en utredning som skall få till uppgift att se över vissa bestämmelser i 14 och 15 kap. brottsbalken planeras att tillsättas.

Av det redovisade framgår att det, utöver dataintrångsbestämmelsen, i första hand är bestämmelserna om skadegörelsebrott och sabotagebrott som är av intresse i sammanhanget. Dessa bestämmelser torde dock inte heller vara tillräckliga för att uppfylla åtagandena enligt rambeslutet i de delar som inte omfattas av dataintrångsbestämmelsen. Lagändringar torde därför vara nödvändiga för att fullt ut uppfylla rambeslutets krav på att det skall vara straffbart att avbryta eller annars allvarligt hindra ett informationssystems drift.

Regeringen gör sammanfattningsvis bedömningen att det torde krävas lagändringar för att generellt kriminalisera att någon avbryter eller annars allvarligt hindrar ett informationssystems drift.

Olaglig datastörning

Enligt *artikel 4* i rambeslutet skall det vara straffbart som olaglig datastörning att uppsåtligt radera, skada, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter i ett informationssystem, om gärningen utförs orättmätigt, åtminstone i fall som inte är ringa. Enligt definitionen i artikel 1 b avses med datorbehandlingsbara uppgifter framställning av fakta, information eller begrepp i en form som lämpar sig för behandling i ett informationssystem, inklusive program som lämpar sig för att få ett informationssystem att utföra en viss uppgift. Det straffbara området omfattar alltså uppsåtligt och orättmätigt raderande etc. av uppgifter av detta slag som finns i ett informationssystem, dvs. – enligt definitionen i artikel 1 a – i princip i apparater som automatiskt behandlar sådana uppgifter.

Olagliga datastörningar kan utgöras av datavirusangrepp riktade mot innehållet i t.ex. en persondator och annan förvanskning av t.ex. webbplatser, jfr vad som sagts om sabotageprogram i avsnitt 5.

Enligt den svenska dataintrångsbestämmelsen är det, som framgått ovan, straffbelagt att olovligen ändra eller utplåna en upptagning för automatisk databehandling eller att föra in en sådan upptagning i ett register. För ansvar enligt bestämmelsen krävs liksom enligt rambeslutets bestämmelse uppsåt. Båda bestämmelserna förutsätter vidare att handlingen utförs olovligen respektive orättmätigt. Dessa krav måste anses ha samma innebörd. I denna del hänvisas till vad som tidigare sagts i avsnitten om olagligt intrång i informationssystem och olaglig systemstörning.

Den straffbara handlingen enligt rambeslutet riktar sig generellt mot datorbehandlingsbara uppgifter som finns i informationssystem. Den avser både innehåll i vanlig bemärkelse och andra uppgifter. De uppgifter som avses i rambeslutet omfattas av begreppet upptagning för automatisk databehandling i dataintrångsbestämmelsen.

Datastörningen kan bestå i att någon raderar, skadar, försämrar eller ändrar de datorbehandlingsbara uppgifterna. Dessa handlingar måste anses motsvara vad som enligt dataintrångsbestämmelsen är straffbelagt som att ändra eller utplåna. Enligt artikeln skall det vidare vara straffbart att hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter. Som angetts i föregående avsnitt om olaglig systemstörning kan i vissa fall sådana datastörningar åstadkommas utan att uppgifterna ändras eller utplånas eller förs in i register eller utan att någon olovligen bereder sig tillgång till en upptagning. I dessa situationer torde dataintrångsbrottet inte motsvara vad som krävs enligt rambeslutet. Som vidare konstaterats i det avsnittet torde inte heller andra svenska straffbestämmelser, främst om skadegörelse- och sabotagebrott, vara tillräckliga för att uppfylla rambeslutets krav i dessa delar. För att helt uppfylla rambeslutets krav på att det skall vara straffbart att hindra flödet av och göra det omöjligt att komma åt datorbehandlingsbara uppgifter torde enligt regeringens bedömning därför krävas lagändring.

Enligt *artikel 5* i rambeslutet skall anstiftan av och medhjälp till olagligt intrång i informationssystem, olaglig systemstörning och olaglig datastörning vara straffbelagt. I svensk rätt är medverkan till dataintrång, skadegörelse, grov skadegörelse samt sabotage och grovt sabotage redan kriminaliserat.

Vidare skall försök till olagligt intrång, olaglig systemstörning och olaglig datastörning vara straffbart. När det gäller intrång får dock en medlemsstat besluta att försök inte skall straffbeläggas. I svensk rätt är försök till dataintrång straffbart under förutsättning att intrånget inte skulle ha varit att anse som ringa om det fullbordats. Rambeslutet kräver dock inte att ringa fall av fullbordade brott straffbeläggs. Därmed bör rambeslutet inte heller anses kräva att försök straffbeläggs i de fall det fullbordade brottet skulle ha varit ringa, även om den fullbordade gärningen i och för sig kriminaliseras i nationell rätt. När det gäller skadegörelse, grov skadegörelse, sabotage och grovt sabotage är försök till dessa brott straffbelagda.

Sammanfattningsvis gör alltså regeringen bedömningen att svensk rätt uppfyller rambeslutets krav om kriminalisering av anstiftan, medhjälp och försök i fråga om de handlingar som täcks av straffbestämmelserna om dataintrång, skadegörelse, grov skadegörelse, sabotage och grovt sabotage.

Närmare om hur lagändringarna bör utformas

Av de föregående avsnitten har framgått att svensk rätt till övervägande del uppfyller de krav som ställs i rambeslutet. Kraven på vilka handlingar som skall vara straffbelagda motsvaras dock inte fullt ut av svenska straffbestämmelser. Enligt rambeslutet skall det vara straffbart att hindra flödet av och göra det omöjligt att komma åt datorbehandlingsbara uppgifter. Det skall också vara straffbart att avbryta eller allvarligt hindra driften av ett informationssystem, bl.a. när det sker genom inmatningar eller överföringar av datorbehandlingsbara uppgifter. Dessutom skall anstiftan av och medhjälp till samt försök till dessa i dag straffria handlingar vara straffbart. I dessa avseenden krävs alltså svenska lagändringar.

Dataintrångsbestämmelsens skyddsobjekt – upptagning för automatisk databehandling – motsvarar rambeslutets skyddsobjekt. Bestämmelsen är också uppbyggd med krav på uppsåt och olovlighet på ett sätt som överensstämmer med rambeslutet. Det framstår därför som naturligt att de nödvändiga lagändringarna görs i dataintrångsbestämmelsen. Bestämmelsen bör så långt det är möjligt behållas i sin nuvarande utformning och endast kompletteras med de tillägg som är påkallade till följd av rambeslutet. Eftersom försök till dataintrång är kriminaliserat, krävs inga särskilda lagstiftningsåtgärder om utvidgningen av det straffbara området sker i den bestämmelsen. Brottsbalkens bestämmelser om medverkan (23 kap. 4 §) innebär att anstiftan av och medhjälp till sådana gärningar kommer att vara kriminaliserade.

När det straffbara området skall utformas är det angeläget att överväga detta i förhållande till handlingar som utgör opinionsyttringar eller liknande, t.ex. sändande av elektronisk post med visst åsiktsinnehåll till en myndighet i syfte att myndigheten skall ta del av och låta sig påverkas av innehållet. Dessutom måste frågor av teknisk natur övervägas. Utvidgningen av det kriminaliserade området kräver sålunda ytterligare analys. Det är därför inte möjligt att nu redovisa den exakta avgränsningen av det straffbara området.

6.2 Påföljder och försvårande omständigheter

Regeringens bedömning: Svensk rätt uppfyller rambeslutets bestämmelser om påföljder och försvårande omständigheter.

Skälen för regeringens bedömning: Straffskalan för dataintrång är böter eller fängelse i högst två år. För skadegörelse och grov skadegörelse är straffskalorna böter eller fängelse i högst ett år respektive fängelse i högst fyra år. Straffskalorna för sabotage och grovt sabotage är fängelse i högst fyra år respektive fängelse i lägst två år och högst tio år eller på livstid.

Enligt *artikel 6 punkt 1* i rambeslutet skall samtliga de handlingar som enligt rambeslutet skall vara straffbara vara belagda med effektiva, proportionella och avskräckande straffrättsliga påföljder. Denna bestämmelse kräver inte någon lagstiftningsåtgärd.

Artikel 6 punkt 2 föreskriver att de brott som avses i artiklarna 3 och 4, dvs. olagliga systemstörningar och olagliga datastörningar men däremot inte olagliga intrång i informationssystem enligt artikel 2 och medverkan och försök enligt artikel 5, skall vara belagda med straffrättsliga påföljder som innebär ett maximistraff på minst ett till tre års fängelse. Detta innebär ett krav på att fängelse i åtminstone ett år skall finnas i straffskalan. Straffskalorna för dataintrång, skadegörelse, grov skadegörelse liksom för sabotagebrott uppfyller detta krav. Följaktligen kräver rambeslutet inte någon lagändring i denna del.

Enligt svensk rätt skall vidare såsom försvårande omständighet vid bedömningen av ett brotts straffvärde särskilt beaktas om brottet utgjort ett led i en brottslig verksamhet som varit särskilt noggrant planlagd eller bedrivits i stor omfattning och i vilken den tilltalade spelat en betydande roll (29 kap. 2 § 6 brottsbalken).

I *artikel 7 punkt 1* i rambeslutet föreskrivs att det skall ses som en försvårande omständighet att brott begås inom ramen för en sådan kriminell organisation som avses i gemensam åtgärd 98/733/RIF av den 21 december 1998 om att göra deltagande i en kriminell organisation i Europeiska unionens medlemsstater till ett brott. Den svenska bestämmelsen måste anses motsvara detta åtagande enligt rambeslutet.

När en sådan försvårande omständighet föreligger skall enligt rambeslutet de gärningar som avses i artikel 2.2 och artiklarna 3 och 4 vara belagda med straffrättsliga påföljder som innebär ett maximistraff på minst två till fem års fängelse. Det innebär att olagliga intrång som begås genom intrång i en säkerhetsåtgärd, olagliga systemstörningar och olagliga datastörningar skall ha straffskalor som innehåller åtminstone två års

fängelse. De tidigare redovisade straffskalorna för dataintrång, grov skadegörelse, sabotage och grovt sabotage uppfyller också detta krav. Det gör däremot inte straffskalan för skadegörelse av normalgraden. I fråga om gradindelade brott är det dock tillräckligt att den grövsta formen – i detta fall grov skadegörelse – motsvarar vad som krävs enligt rambeslutet. Inte heller i denna del kräver rambeslutet därför någon lagändring.

Enligt *artikel 7 punkt 2* får en medlemsstat även vidta de åtgärder som avses i punkt 1, när gärningen har orsakat allvarliga skador eller påverkat väsentliga intressen. Bestämmelsen är fakultativ och kräver därför inte någon lagändring. Emellertid kan enligt gällande svensk rätt sådana omständigheter motivera att brotten bedöms som grov skadegörelse, sabotage eller grov sabotage. Straffskalorna för dessa brott motsvarar den fängelsenivå i punkt 1 som punkt 2 anvisar.

6.3 Ansvar och påföljder för juridiska personer

Regeringens bedömning: Svensk rätt uppfyller de krav som rambeslutet ställer i fråga om ansvar och påföljder för juridiska personer.

Skälen för regeringens bedömning: Rambeslutet innehåller bestämmelser om ansvar och påföljder för juridiska personer. Med juridisk person avses enligt artikel 1 c enhet som har sådan status enligt tillämplig lagstiftning, med undantag av stater eller andra offentliga organ vid utövandet av de befogenheter som de har i egenskap av statsmakter samt internationella offentliga organisationer. Denna definition förekommer i andra redan antagna rambeslut, t.ex. rambeslutet om bekämpning av bedrägeri och förfalskning som rör andra betalningsmedel än kontanter (EGT L 149, 2.6.2001, s. 1). Definitionen är alltså vedertagen.

Bestämmelserna om ansvar och påföljder för juridiska personer i *artiklarna 8 och 9* innebär att påföljder i form av bötesstraff eller administrativa avgifter under vissa förutsättningar skall kunna åläggas juridiska personer när brott har begåtts till deras förmån. Vidare får vissa påföljder införas. Något krav på att införa straffrättsligt ansvar finns alltså inte.

Bestämmelserna utgör standardbestämmelser som återkommer i flera andra antagna rambeslut inom ramen för samarbetet i rättsliga och inrikes frågor. Motsvarande bestämmelser finns bl.a. i EU:s rambeslut om förstärkning av skyddet mot förfalskning i samband med införandet av euron (EGT L 140, 14.6.2000, s. 1). I samband med att riksdagen godkände det rambeslutet gjordes den bedömningen att de svenska reglerna om företagsbot (36 kap. 7–10 §§ brottsbalken) motsvarar de krav som ställs i rambeslutet (prop. 1999/2000:85, bet. 1999/2000:JuU20, rskr. 1999/2000:217). Samma bedömning gjordes i det lagstiftningsärende som behandlade de lagändringar som ansågs nödvändiga till följd av det rambeslutet (prop. 2000/01:40, bet. 2000/01:JuU9, rskr. 2000/01:138). I den rapport som Europeiska kommissionen upprättade avseende medlemsstaternas genomförande av rambeslutet (KOM [2002] 771 slutlig) angavs också Sverige som en av åtta medlemsstater som har lagstiftning varigenom juridiska personer kan ställas till rättsligt ansvar för de brott som omfattas av rambeslutet. Även i fråga om förevarande rambeslut får

reglerna om företagsbot anses uppfylla de krav som uppställs vad gäller ansvar och påföljder för juridiska personer.

6.4 Behörighet

Regeringens bedömning: Rambeslutets krav på behörighet (domsrätt) motsvarar i princip svenska bestämmelser på området. Sverige bör emellertid i den ordning som föreskrivs i rambeslutet lämna underrättelse om att Sverige inte kommer att tillämpa bestämmelsen om behörighet i artikel 10 punkt 1 c i de fall brott har begåtts utanför Sveriges territorium.

Skälen för regeringens bedömning: Svenska regler om straffrättslig behörighet (domsrätt) finns i huvudsak i 2 kap. brottsbalken. För brott som begåtts här i riket döms efter svensk lag vid svensk domstol (1 §). Detsamma gäller om det är ovisst var ett brott förövats men det finns skäl att anta att det har begåtts inom riket. Ett brott anses begånget där den brottsliga handlingen företogs, så ock där brottet fullbordades eller, vid försök, där brottet skulle ha fullbordats (4 §). Så snart någon del av den brottsliga handlingen har ägt rum här i riket är alltså handlingen i sin helhet att anse som begången i Sverige och inte bara den del som faller inom landets gränser.

Artikel 10 punkt 1 a i rambeslutet föreskriver att en medlemsstat skall ha behörighet i fråga om brott enligt rambeslutet som har ägt rum helt eller delvis på medlemsstatens territorium. Enligt *punkt 2* skall i detta fall behörigheten innefatta situationer där a) brottslingen är fysiskt närvarande på medlemsstatens territorium när brottet begås, oavsett om brottet riktar sig mot ett informationssystem på denna medlemsstats territorium eller inte, eller b) brottet riktar sig mot ett informationssystem på medlemsstatens territorium, oavsett om brottslingen är fysiskt närvarande på detta territorium när brottet begås eller inte.

De svenska bestämmelserna om domsrätt över brott som begåtts här i riket och var ett brott skall anses begånget torde i praktiken ge svenska domstolar behörighet att döma över brott i dessa fall. Bestämmelserna måste därför anses uppfylla de angivna kraven i rambeslutet. Därmed krävs inte någon lagändring i denna del.

Enligt 2 kap. brottsbalken döms vidare för brott som begåtts utom riket efter svensk lag vid svensk domstol bl.a. om brottet har begåtts av en svensk medborgare (2 §).

Genom denna bestämmelse uppfylls åtagandet i *punkt 1 b* att varje medlemsstat skall fastställa behörighet beträffande brott enligt rambeslutet som har begåtts av en av medlemsstatens medborgare. Detsamma gäller åtagandet i *punkt 3* om att en medlemsstat, som enligt sin lagstiftning ännu inte utlämnar eller överlämnar sina egna medborgare, skall fastställa sin behörighet i fråga om och, när det är lämpligt, väcka åtal för brotten enligt rambeslutet när de har begåtts av en av landets medborgare utanför landets territorium.

Bestämmelsen i *punkt 1 c* att en medlemsstat skall ha behörighet att döma över brott enligt rambeslutet som har begåtts till förmån för en juridisk person som har sitt huvudkontor på medlemsstatens territorium saknar motsvarighet i svensk rätt. Svenska domstolar har emellertid en

långtgående behörighet att döma över brott. Som framgått ovan har svenska domstolar alltid behörighet att döma över brott som helt eller delvis har begåtts i Sverige. Dessutom har domstolarna en vidsträckt behörighet att döma över brott som begåtts utom riket (se främst 2 och 3 §§). Bestämmelsen i rambeslutet motsvaras dock, som redan sagts, inte av en likalydande behörighetsregel i svensk rätt. Sverige bör därför utnyttja den möjlighet som föreskrivs i *punkt 5* att inte tillämpa denna behörighetsbestämmelse i rambeslutet när brottet har begåtts utanför Sveriges territorium. Enligt *punkt 6* skall rådets generalsekretariat och kommissionen underrättas om detta. Det bör ske genom regeringens försorg.

Slutligen reglerar *punkt 4* fall där flera medlemsstater har behörighet att döma över samma brott. Bestämmelsen innebär att staterna skall samarbeta för att avgöra behörighetsfrågan och att de i det syftet kan anlita de organ eller mekanismer som har inrättats inom Europeiska unionen och att vissa omständigheter därvid kan beaktas. Bestämmelsen innebär alltså en samrådsskyldighet. Formerna för samrådet är emellertid fakultativa. Sådant samråd torde i dag i förekommande fall äga rum formlöst. Någon särskild reglering av frågan kan inte anses nödvändig. Det skall i sammanhanget nämnas att rambeslutet om bekämpande av terrorism (EGT L 164, 22.6.2002, s. 3) innehåller en liknande bestämmelse som, trots att den är av mer obligatorisk karaktär, inte har lett till lagstiftningsåtgärder (jfr prop. 2001/02:135 och 2002/03:38).

Sammanfattningsvis gör regeringen bedömningen att svensk domsrätt föreligger i samtliga fall där medlemsstaterna ovillkorligen skall kunna utöva domsrätt.

6.5 Utbyte av uppgifter

Regeringens bedömning: Bestämmelserna i rambeslutet om utbyte av uppgifter kräver inte lagstiftningsåtgärder. Sverige bör lämna underrättelse om sin kontaktpunkt för utbytet av uppgifter.

Skälen för regeringens bedömning: Enligt *artikel 11* i rambeslutet skall medlemsstaterna för utbyte av uppgifter om de brott som avses i rambeslutet säkerställa att de använder det befintliga nät med operativa kontaktpunkter som kan nås dygnet runt alla dagar i veckan. Detta skall ske med iakttagande av bestämmelser om dataskydd. Det nät som åsyftas är – vilket framgår uttryckligen av ingresskäl 16 – det nät som omnämns i rådets rekommendation av den 25 juni 2001 om kontaktpunkter som upprätthåller ett öppethållande dygnet runt för bekämpning av högteknologisk brottslighet (EGT C 187, 3.7.2001, s. 5). Vidare skall varje medlemsstat underrätta rådets generalsekretariat och kommissionen om sin utsedda kontaktpunkt.

Bestämmelsen innebär sålunda inte ett nytt åtagande att inrätta ett nät med kontaktpunkter. I stället skall det redan befintliga nätet användas för informationsutbyte. Rikskriminalpolisens IT-brottsrotel har en beredskap dygnet runt som innebär att man alltid kan nå en IT-brottsspecialist. På icke kontorstid går kontakten via Rikskommunikationscentralen. Grunden för detta beredskapsåtagande är ett nätverk som skapades i G8 och som Sverige deltagit i sedan 1999. I den nämnda rådsrekommendationen

från 2001 uppmanades de medlemsstater som ännu inte anslutit sig till G8-nätverket att göra det. Inom Rikspolisstyrelsen har tillskapats en funktion för samordning av IT-relaterade brott och incidenter. Funktionen är gemensam för Säkerhetspolisen och Rikskriminalpolisen. På sikt kan denna funktion utgöra en ännu starkare kontaktpunkt än dagens beredskapsmodell.

Det finns alltså redan en kontaktpunkt rörande högteknologisk brottslighet. Artikel 11 innebär att denna befintliga punkt skall användas för utbyte av uppgifter om brotten enligt rambeslutet. I detta måste självklart anses ligga att informationsutbytet också skall ske i de former som sker i dag, dvs. med iakttagande av gällande bestämmelser om dataskydd, vilket framgår uttryckligen av rambeslutet, och gällande sekretessregler. Någon ny reglering för att uppfylla detta åtagande behövs följaktligen inte. Sverige bör genom regeringens försorg underrätta rådets generalsekretariat och kommissionen om denna kontaktpunkt.

I sammanhanget skall också nämnas att Krisberedskapsmyndigheten har ett sammanhållande myndighetsansvar för samhällets informationssäkerhet. I det arbetet ingår bl.a. att analysera förhållanden som rör informationssäkerhet i samhället. Dessutom genomför och sammanställer myndigheten risk- och sårbarhetsanalyser, som tillsammans med erhållet underrättelseunderlag utgör grund för en årlig samlad bedömning till regeringen.

Utöver det arbete som sker med att utbyta uppgifter om IT-brott har regeringen gett Post- och telestyrelsen i uppdrag att inrätta en rikscentral för IT-incidentrapportering. Sedan den 1 januari 2003 är Sveriges IT-incidentcentrum (Sitic) i drift. Sitic har som främsta uppgift att stödja samhället i arbetet med skydd mot IT-incidenter genom att inrätta ett system för informationsutbyte om IT-incidenter mellan samhällets organisationer och Sitic. Sitic skall snabbt kunna sprida information i samhället om nya problem som kan störa IT-system. Att lämna information och råd om förebyggande åtgärder ingår också i uppdraget. Slutligen skall Sitic sammanställa och ge ut statistik som underlag för kontinuerliga förbättringar i det förebyggande arbetet.

7 Ekonomiska konsekvenser

Rambeslutet om angrepp mot informationssystem kan föranleda vissa utvidgningar av det straffbelagda området. Dessa torde emellertid komma att vara av begränsad omfattning och torde endast komma att medföra marginella kostnadsökningar för rättsväsendet. Eventuella merkostnader skall finansieras inom befintliga anslag.

Rambeslutet om angrepp mot informationssystem

RÅDETS RAMBESLUT

av den

om angrepp mot informationssystem

EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA RAMBESLUT

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

med beaktande av kommissionens förslag[1],

med beaktande av Europaparlamentets yttrande[2], och

av följande skäl:

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

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

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

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

(5) Stora klyftor och skillnader i medlemsstaternas lagstiftning på detta område kan försvåra kampen mot organiserad brottslighet och terrorism

[1] EGT C 203 E, 27.8.2002, s. 109.
[2] Yttrandet avgivet den 22 oktober 2002 (EUT C 300 E, 11.12.2003, s. 16).

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

(6) Rådets och kommissionens handlingsplan för att på bästa sätt genomföra bestämmelserna i Amsterdamfördraget om upprättande av ett område med frihet, säkerhet och rättvisa[3], Europeiska rådet i Tammerfors den 15–16 oktober 1999, Europeiska rådet i Santa Maria da Feira den 19–20 juni 2000, kommissionen i "resultattavlan" och Europaparlamentet i sin resolution av den 19 maj 2000 anger eller uppmanar till lagstiftningsåtgärder mot högteknologisk brottslighet, inklusive gemensamma definitioner, kriminaliseringar och påföljder.

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

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

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

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

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

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

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

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

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

(15) Det är lämpligt att föreskriva strängare påföljder när ett angrepp mot ett informationssystem sker inom ramen för en sådan kriminell organisation som avses i gemensam åtgärd 98/733/RIF av den 21 december 1998 om att göra deltagande i en kriminell organisation i Europeiska unionens medlemsstater till ett brott[4]. Det är också lämpligt att föreskriva strängare påföljder när ett sådant angrepp har orsakat allvarliga skador eller har påverkat väsentliga intressen.

(16) Åtgärder bör även förutses för samarbete mellan medlemsstaterna, i syfte att säkra effektiva insatser mot angrepp mot informationssystem. Medlemsstaterna bör därför för utbyte av uppgifter använda sig av det befintliga nät med operativa kontaktpunkter som omnämns i rådets rekommendation av den 25 juni 2001 om kontaktpunkter som upprätthåller ett öppethållande dygnet runt för bekämpning av högteknologisk brottslighet[5].

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

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

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

Artikel 1

Definitioner

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

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

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

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

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

Artikel 2

Olagligt intrång i informationssystem

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

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

Artikel 3

Olaglig systemstörning

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

Artikel 4

Olaglig datastörning

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

Artikel 5

Anstiftan, medhjälp och försök

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

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

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

Artikel 6

Påföljder

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

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

Artikel 7

Försvårande omständigheter

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

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

Artikel 8

Juridiska personers ansvar

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

a) befogenhet att företräda den juridiska personen, eller

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

c) befogenhet att utöva kontroll inom den juridiska personen.

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

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

Artikel 9

Påföljder för juridiska personer

1. Varje medlemsstat skall vidta de åtgärder som är nödvändiga för att se till att en juridisk person som har fällts till ansvar i enlighet med arti-

kel 8.1 kan bli föremål för effektiva, proportionella och avskräckande påföljder, som skall innefatta bötesstraff eller administrativa avgifter och som får innefatta andra påföljder, som

a) fråntagande av rätt till offentliga förmåner eller stöd,

b) tillfälligt eller permanent näringsförbud,

c) rättslig övervakning, eller

d) rättsligt beslut om upplösning av verksamheten.

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

Artikel 10

Behörighet

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

a) helt eller delvis på dess territorium, eller

b) av en av dess medborgare, eller

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

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

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

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

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

4. När ett brott faller under fler än en medlemsstats behörighet och vilken som helst av dessa stater kan lagföra brottet på grundval av samma

omständigheter, skall de berörda medlemsstaterna samarbeta för att avgöra vilken av dem som skall lagföra brottslingarna, för att, om möjligt, centralisera lagföringen till en enda medlemsstat. I detta syfte kan medlemsstaterna anlita de organ eller mekanismer som inrättats inom Europeiska unionen för att underlätta samarbetet mellan deras rättsliga myndigheter och samordningen av deras verksamhet. Följande omständigheter får beaktas i successiv ordning:

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

– Medlemsstaten skall vara den i vilken gärningsmannen är medborgare.

– Medlemsstaten skall vara den på vars territorium gärningsmannen påträffats.

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

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

Artikel 11

Utbyte av uppgifter

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

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

Artikel 12

Genomförande

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

* Två år efter det att detta rambeslut har trätt i kraft.

2. Senast vid samma tidpunkt skall medlemsstaterna till rådets generalsekretariat och kommissionen överlämna texten till bestämmelser genom vilka de skyldigheter som ålagts dem enligt detta rambeslut införlivas med deras nationella lagstiftning. Senast den ...* skall rådet, på grundval av en rapport som skall utarbetas utifrån information och en skriftlig rapport från kommissionen, bedöma i vilken utsträckning medlemsstaterna har följt bestämmelserna i detta rambeslut.

Artikel 13

Ikraftträdande

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

Utfärdat i Bryssel den

På rådets vägnar
Ordförande

_____

* 30 månader efter det att detta rambeslut har trätt i kraft.

Uttalande från kommissionen

Uttalande till rådets protokoll då rambeslutet antas.

Uttalande från kommissionen

Kommissionen beklagar att det i artikel 6.2 i rambeslutet inte föreskrivs ett minimistraff för olagligt intrång enligt artikel 2.

Justitiedepartementet

Utdrag ur protokoll vid regeringssammanträde den 27 maj 2004

Närvarande: statsministern Persson, ordförande, och statsråden Sahlin, Pagrotsky, Östros, Messing, Engqvist, Lövdén, Ringholm, Bodström, Sommestad, Karlsson, Nykvist, Andnor, Nuder, Johansson, Björklund, Holmberg, Jämtin

Föredragande: statsrådet Bodström

Regeringen beslutar proposition 2003/04:164 Sveriges antagande av rambeslut om angrepp mot informationssystem