Innehåll

1 Sammanfattning

I promemorian övervägs behovet av lagändringar för att genomföra EU:s rambeslut om angrepp mot informationssystem. Rambeslutet innehåller bestämmelser om vilka handlingar som skall vara straffbelagda som sådana angrepp. Dessutom finns bestämmelser om bl.a. påföljder för brotten, ansvar och påföljder för juridiska personer, behörighet och utbyte av uppgifter. För att rambeslutet fullt ut skall uppfyllas krävs i två avseenden ett utvidgat straffansvar. Utvidgningarna föreslås ske i dataintrångsbestämmelsen i brottsbalken.

Dataintrångsbestämmelsen utvidgas till att avse undertryckande av en upptagning för databehandling. Vidare utvidgas ansvaret för dataintrång till att omfatta annat allvarligt hindrande av användningen av en sådan upptagning. Kriminaliseringen innebär exempelvis att s.k. tillgänglighetsattacker blir straffbara.

Genom att dessa gärningar straffbeläggs blir försök och förberedelse till gärningarna straffbara enligt bestämmelserna om försök och förberedelse till dataintrång. Dessutom blir brottsbalkens generella bestämmelser om medverkan tillämpliga.

Vidare klargörs att dataintrångsbestämmelsen omfattar alla uppgifter som befordras och som är avsedda för databehandling. Dessutom moderniseras bestämmelsen genom att begreppet automatisk databehandling ersätts med automatiserad databehandling.

I promemorian görs bedömningen att gällande svensk rätt uppfyller rambeslutets bestämmelser i övrigt. Sverige bör utnyttja en möjlighet att inte tillämpa en viss behörighetsregel och lämna underrättelse om detta. Sverige bör vidare ange en svensk

kontaktpunkt för utbyte av uppgifter om brotten enligt rambeslutet.

Ändringarna föreslås träda i kraft den 1 januari 2007.

2 Promemorians författningsförslag

Förslag till lag om ändring i brottsbalken

Härigenom föreskrivs att 4 kap. 9 c § brottsbalken skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	4 kap.
	9 c §[1]
Den som i annat fall än som sägs i 8 och 9 §§ olovligen bereder sig tillgång till upptagning för *automatisk* databehandling eller olovligen ändrar eller utplånar eller i register för in sådan upptagning döms för *dataintrång* till böter eller fängelse i högst två år. Med upptagning avses *härvid* även uppgifter som *är under befordran* via *elektroniskt eller annat liknande hjälpmedel för att användas* för *automatisk* databehandling.	Den som i annat fall än som sägs i 8 och 9 §§ olovligen bereder sig tillgång till *en* upptagning för *automatiserad* databehandling eller olovligen ändrar eller utplånar eller i register för in *en* sådan upptagning döms för *dataintrång* till böter eller fängelse i högst två år. *Detsamma gäller den som olovligen undertrycker eller på annat sätt allvarligt hindrar användningen av en sådan upptagning.* Med upptagning avses även uppgifter som *befordras* via *elektromagnetiska vågor och*

[1] Senaste lydelse 1998:206.

som är avsedda för *automatiserad* databehandling.

Denna lag träder i kraft den 1 januari 2007.

3 Angrepp mot informationssystem

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

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. Program som skickar stora mängder elektronisk post kan avbryta eller allvarligt hindra driften hos ett 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.

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 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 eller brister i program och datorutrustning. Tillgänglighetsattacker har i flera fall haft tydliga mål som nätoperatörer och Internetleverantörer. Det finns en risk för att också t.ex. industrin, sjukvården eller myndigheter utsätts för allvarliga tillgänglighetsattacker över öppna nät eller mer avancerade intrång och attacker i systemen. Även andra kan utsättas för angrepp. Angreppen kan orsaka betydande kostnader och ekonomiska förluster eller annars få allvarliga konsekvenser. De riskerar också att göra informationssystemen dyrare och därmed mindre tillgängliga för envar. Förtroendet för tekniken, t.ex. elektroniska tjänster som 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 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.

4 EU:s rambeslut om angrepp mot informationssystem

4.1 Rambeslutets tillkomst

Våren 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 inom Regeringskansliet och överlämnades till riksdagen (2001/02:FPM110).

Europaparlamentet yttrade sig över förslaget den 22 oktober 2002 (EUT C 300 E, 11.12.2003, s. 26).

Förslaget till rambeslut behandlades vid fem tillfällen i rådets arbetsgrupp för materiell straffrätt samt i januari och 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 ministerrådet för rättsliga och inrikes frågor en politisk överenskommelse om innehållet i rambeslutet vid ett 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 den 28 februari 2003 (RD 2002/03:2952, EUJu2003/311/EU).

Vid Europeiska rådets möte den 25 och den 26 mars 2004 antogs, mot bakgrund av terroristattackerna i Madrid den 11 samma månad, en deklaration om bekämpande av terrorism. I deklarationen slogs fast att ett antal rambeslut beträffande vilka det

förelåg politiska överenskommelser, däribland rambeslutet om angrepp mot informationssystem, skulle antas senast i juni 2004.

Riksdagen godkände rambeslutet den 27 oktober 2004 (prop. 2003/04:164, bet. 2004/05:JuU4, rskr. 2004/05:6). Rambeslutet har ännu inte antagits men det kan förutsättas att det kommer att antas inom en nära framtid.

Rambeslutet i svensk version är fogat till denna promemoria som *bilaga 1*. I *bilaga 2* finns ett uttalande av kommissionen som skall tas till rådets protokoll i samband med att rambeslutet antas.

4.2 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 den 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 den 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 EU när det gäller angrepp mot informationssystem. Det sistnämnda meddelandet följdes upp med rådets resolution av den 28 januari 2002 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.

I ett meddelande 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. Våren 2002 presenterade kommissionen förslaget till rambeslut om angrepp mot informationssystem.

Angrepp mot informationssystem anses utgöra ett hot mot skapandet av ett säkert informationssamhälle och ett område med frihet, säkerhet och rättvisa i EU. Genom EU-gemensamma beskrivningar av vilka handlingar som skall anses utgöra straffbara angrepp mot informationssystem skapas ett gemensamt rättsområde som underlättar det rättsliga och polisiära samarbetet för att förebygga och bekämpa sådana angrepp. Rambeslutet skall ses som ett komplement till rambeslutet om bekämpande av terrorism (EGT L 164, 22.6.2002, s. 3). Den betydelse som rambeslutet anses ha för kampen mot terrorism har kommit till uttryck i Europeiska rådets deklaration från mars 2004 om bekämpande av terrorism.

4.3 Rambeslutets innehåll

4.3.1 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), 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 i sammanhanget 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.

4.3.2 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 systemen 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.

4.3.3 Artikel 1 Definitioner

I *artikel 1* definieras vissa begrepp som används i rambeslutet. Punkterna a och b innehåller definitioner av begreppen 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.

4.3.4 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.

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.

4.3.5 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, när gärningen utförs orättmätigt, åtminstone i fall som inte är ringa.

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.

4.3.6 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, när gärningen utförs orättmätigt, åtminstone i fall som inte är ringa.

4.3.7 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, dvs. olagligt intrång i informationssystem, olaglig systemstörning och olaglig datastörning, 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.

4.3.8 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 de

brotten, 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.

4.3.9 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.

4.3.10 Artiklarna 8 och 9 Ansvar och påföljder för juridiska personer

Artiklarna 8 och 9 innehåller bestämmelser om ansvar och påföljder för juridiska personer.

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 de 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.

4.3.11 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 medlemsstater-

na 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.

4.3.12 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.

4.3.13 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.

Av *punkt 2* följer 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.

4.3.14 Artikel 13 Ikraftträdande

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

4.3.15 Uttalande

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

5 Europarådets konvention om IT-relaterad brottslighet

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

Konventionen, som trädde i kraft den 1 juli 2004, 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, även om det finns vissa avvikelser. Därutöver innehåller konventionen ytterligare straffbestämmelser om IT-relaterade brott. Konventionen innehåller också ett flertal straffprocessuella bestämmelser och bestämmelser om internationellt samarbete.

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

Frågan om Sverige skall ratificera konventionen och protokollet behandlas i departementspromemorian Brott och brottsutredning i IT-miljö (Ds 2005:6). I promemorian framhålls att åtagandena att kriminalisera olagligt intrång i datorsystem, datastörning och störning av datorsystem enligt konventionen kommer att uppfyllas om de förändringar som föreslås i denna promemoria genomförs. I promemorian om konventionen be-

handlas därför bara de ytterligare förändringar som krävs för genomförandet av konventionen.

Rambeslutets bestämmelser har, som nämnts, tagit sin utgångspunkt i konventionens motsvarande bestämmelser. Rambeslutet bör emellertid behandlas fristående från frågan om ratificering av konventionen. Konventionen innehåller nämligen bestämmelser som saknar motsvarigheter i rambeslutet och som rör helt andra områden och den kräver därför till stor del andra överväganden än de som rambeslutet föranleder.

6 Gällande svensk rätt och behovet av lagändringar

6.1 Gällande svensk rätt

6.1.1 Inledning

I avsnitt 6.1.2 och 6.1.3 lämnas en redogörelse för de svenska straffbestämmelser som närmast torde motsvara rambeslutets regler om straffbara handlingar. Där beskrivs bestämmelserna om dataintrång, skadegörelse och grov skadegörelse. Också bestämmelserna om sabotage och grovt sabotage är av intresse och redovisas därför. 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 den lagen.

I avsnitt 6.1.3 berörs också vissa andra straffbestämmelser som har ett samband med bestämmelsen om dataintrång, nämligen reglerna om brytande av post- eller telehemlighet, intrång i förvar, olovlig avlyssning samt förberedelse till brytande av telehemlighet och till olovlig avlyssning. Dataintrångsbestämmelsen är subsidiär i förhållande till bestämmelserna om brytande av post- eller telehemlighet och intrång i förvar.

I avsnitt 6.1.4 redogörs för de svenska reglerna om ansvar för anstiftan, medhjälp och försök. Därefter följer i avsnitt 6.1.5–6.1.8 en beskrivning av gällande svenska bestämmelser om påföljder, försvårande omständigheter, ansvar och påföljder för juridiska personer samt straffrättslig behörighet för domstolar.

6.1.2 Ansvarsbestämmelsen om dataintrång

För *dataintrång* döms den som olovligen bereder sig tillgång till en upptagning för automatisk databehandling eller olovligen ändrar eller utplånar eller i register för in en 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).

Dataintrångsbestämmelsen infördes i brottsbalken 1998 då datalagen (1973:289) ersattes av personuppgiftslagen (1998:204) och datalagens bestämmelse om dataintrång i 21 § överfördes till brottsbalken. Någon ändring i sak gjordes inte.

Datalagen tillkom i början av 1970-talet samtidigt som begreppet upptagning för automatisk databehandling infördes i bestämmelserna om allmänna handlingars offentlighet i 2 kap. tryckfrihetsförordningen (TF). I propositionen uttalades 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. I begreppet ligger också att informationen är läsbar endast med ADB-teknik (prop. 1973:33 s. 75). Efter en lagändring i 21 § datalagen 1986 avses med upptagning för automatisk databehandling även uppgifter som är under befordran via ett elektroniskt eller liknande hjälpmedel för att användas för automatisk databehandling. Tillägget avser uppgifter som ännu inte fixerats på ett datamedium (prop. 1985/86:65 s. 30 ff.).

Dataintrångsbestämmelsen ger genom sitt samlade upptagningsbegrepp ett skydd för uppgifter för automatisk databehandling, även uppgifter som befordras oavsett om de är fixerade på datamedium eller inte. När det gäller uppgifter som befordras har den tekniska utvecklingen inneburit att befordran numera i stor omfattning sker i nät, både ledningsbundna nät och radionät. Det kan därför diskuteras om dataintrångsbestämmelsen i dag omfattar alla uppgifter som överförs.

Ansvar för dataintrång förutsätter uppsåt (1 kap. 2 § brottsbalken). Det krävs också att gärningen utförs olovligen. En gärning anses inte olovlig om den sker med samtycke av den som

förfogar över upptagningen eller i överensstämmelse med gällande rätt, t.ex. regler om tvångsmedel.

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

Vidare straffbeläggs att ändra eller utplåna en upptagning. En ändring kan direkt 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 bestämmelsen tillkom efter påpekande av Justitiekanslern (JK) under remissbehandlingen av det betänkande som låg till grund för propositionen om datalagen (SOU 1972:47). JK ansåg att tolkningen av betänkandets förslag till straffbestämmelse kunde bli föremål för tvekan med hänsyn till att ingenting sades om obehöriga införingar (prop. 1973:33 s. 68). Någon närmare diskussion om kriminaliseringen fördes inte i propositionen.

Införingar av upptagningar i register är alltså straffbelagda. Registerbegreppet måste anses vara snävare än begreppet upptagning för automatisk databehandling. Införingar som sker i sådana upptagningar för automatisk databehandling som inte samtidigt kan betecknas som register kan medföra att upptagningarna ändras eller utplånas. Dessutom kan införingar ske i samband med intrång. I dessa fall omfattas införingarna av de delar av dataintrångsbestämmelsen som straffbelägger ändring eller utplånande av samt intrång i upptagningar.

6.1.3 Ansvarsbestämmelser om skadegörelse m.m.

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, döms för *grovt sabotage* (13 kap. 5 § brottsbalken).

För *brytande av post- eller telehemlighet* döms den som olovligen bereder sig tillgång till ett meddelande, som ett post- eller telebefordringsföretag förmedlar som postförsändelse eller telemeddelande (4 kap. 8 § brottsbalken). För ansvar krävs att det är fråga om ett meddelande som är under befordran från en avsändare till en mottagare och som förmedlas av ett post- eller telebefordringsföretag. Meddelandet skall vara en postförsändelse eller ett telemeddelande. Med telemeddelande avses ljud, text, bild, data eller information i övrigt (Holmqvist m.fl., Brottsbalken En kommentar Kap. 1–12, s. 4:35–4:36). Ett telemeddelande kan förmedlas genom en särskilt anordnad ledare eller med hjälp av radio. Den brottsliga gärningen består i att bereda sig tillgång till meddelandet. Det innebär inte något krav på att gärningsmannen tar del av innehållet. För ansvar förutsätts uppsåt och att

handlingen vidtas olovligen. Olovlighetskravet utesluter avlyssning av telemeddelanden som förmedlas via radio, om det inte är förbjudet att lyssna på meddelanden i radio. I kravet på olovlighet ligger vidare att gärningen skall utföras utan samtycke av den som äger förfoga över meddelandet och utan stöd av lagstiftning, t.ex. tvångsmedelslagstiftning.

Den som, utan att det är fråga om brytande av post- eller telehemlighet, olovligen bryter brev eller telegram eller annars bereder sig tillgång till något som förvaras förseglat eller under lås eller annars tillslutet, döms för *intrång i förvar* (4 kap. 9 § brottsbalken). Denna bestämmelse skyddar brev, telegram och ”något” förutsatt att det är tillslutet. Den brottsliga handlingen består i att bereda sig tillgång till brevet etc. För ansvar krävs att gärningen begås olovligen och med uppsåt.

För *olovlig avlyssning* döms den som i annat fall än som sägs i bestämmelsen om brytande av post- eller telehemlighet olovligen medelst tekniskt hjälpmedel för återgivning av ljud i hemlighet avlyssnar eller upptar tal i enrum, samtal mellan andra eller förhandlingar vid sammanträde eller annan sammankomst, vartill allmänheten inte har tillträde och som han eller hon själv inte deltar i eller obehörigen har berett sig tillträde till (4 kap. 9 a § brottsbalken).

Den som anbringar tekniskt hjälpmedel med uppsåt att bryta telehemlighet eller olovligen avlyssna, döms för *förberedelse till brytande av telehemlighet* respektive *förberedelse till olovlig avlyssning*, om han eller hon inte skall dömas till ansvar för fullbordat sådant brott (4 kap. 9 b § brottsbalken).

6.1.4 Ansvarsbestämmelser om anstiftan, medhjälp och försök

Enligt de allmänna medverkansbestämmelserna (23 kap. 4 § brottsbalken) 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 fysis-

ka 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 medverkansbestämmelserna har uttrycket getts en vidare betydelse och kan innefatta även medverkan som inte utgjort någon förutsättning för brottet. Det innebär att medverkansansvar kan komma i fråga för den som endast obetydligt har 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. Varje medverkande är självständigt ansvarig, dvs. ansvarig oberoende av om det är möjligt att straffa någon annan medverkande. Ansvaret är dock beroende av att en straffbelagd gärning har utförts. Varje medverkande bedöms efter det uppsåt eller den oaktsamhet som ligger honom eller henne till last.

Bestämmelserna om anstiftan och medhjälp gäller enligt huvudregeln vid alla brottsbalksbrott samt brott i specialstraffrätten för vilka fängelse är föreskrivet.

Anstiftan av och medhjälp till dataintrång, skadegörelse, grov skadegörelse, sabotage och grovt sabotage är alltså straffbart.

Försök och förberedelse till brott är straffbart i de fall det finns ett särskilt stadgande om det (23 kap. 1 och 2 §§ brottsbalken). Den som påbörjat utförandet av ett visst brott utan att det 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. För förberedelse kan bl.a. dömas en person som tagit befattning med något som är ägnat att användas som hjälpmedel vid brott.

Försök och förberedelse 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 straffbart (12 kap. 5 § och 13 kap. 12 § brottsbalken). Detsamma gäller förberedelse till de tre sistnämnda brotten.

6.1.5 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 och får inte sättas under fängelse om lägsta straff för det fullbordade brottet är fängelse i två år eller däröver (23 kap. 1 § brottsbalken).

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

6.1.6 Försvårande omständigheter

I svensk rätt finns bestämmelser om att försvårande omständigheter skall beaktas vid bedömningen av ett brotts straffvärde (29 kap. 2 § brottsbalken). Exempelvis skall som en försvårande omständighet 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).

6.1.7 Ansvar och påföljder för juridiska personer

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

brottsligheten. Det gäller dock inte om brottsligheten har varit riktad mot näringsidkaren eller om det annars skulle vara uppenbart oskäligt att ålägga företagsbot.

Företagsbot skall fastställas till lägst tio tusen kronor och högst tre miljoner kronor. När storleken av boten fastställs skall särskild hänsyn tas till brottslighetens art, omfattning och förhållande till näringsverksamheten. En företagsbot kan efterges eller jämkas under särskilda förutsättningar.

6.1.8 Behörighet

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 har förövats men det finns skäl att anta att det har begåtts inom riket. Ett brott anses begånget där den brottsliga handlingen företogs, 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 §). Svensk behörighet för utomlands begångna brott gäller också i vissa särskilt angivna fall andra utlänningar, exempelvis utlänning som efter brottet blivit svensk medborgare. Detsamma gäller utlänning som vistas i Sverige, om brottet kan medföra fängelse i mer än sex månader. Dessa behörighetsregler förutsätter att gärningen inte är fri från ansvar enligt lagen på gärningsorten. Därutöver har svenska domstolar en 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).

Enligt lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder får överlämnande av en person

som eftersöks för lagföring inte vägras enbart på den grunden att personen är medborgare i den anmodade staten. Lagen, som bygger på ett rambeslut, tillämpas i förhållande till andra EU-stater. Dock kommer övergångsvis bestämmelser i lagen (1957:668) om utlämning för brott att vara tillämpliga i förhållande till medlemsstater som inte hunnit genomföra rambeslutet i tid. På samma sätt kommer lagen (1959:254) om utlämning för brott till Danmark, Finland, Island och Norge att vara tillämplig i förhållande till Danmark och Finland. Enligt dessa utlämningslagar får svenska medborgare i vissa fall inte utlämnas till andra EU-stater.

6.2 Handlingar som skall vara straffbelagda

6.2.1 Utgångspunkter för bedömningen av straffbelagda handlingar

Rambeslutet innehåller bestämmelser om att olagliga intrång i informationssystem, olagliga systemstörningar och olagliga datastörningar skall vara straffbelagda. Av artikel 47 i Fördraget om Europeiska unionen följer att rambeslutet inte påverkar Europeiska gemenskapernas behörighet. Det innebär att instrument som antagits på det område som regleras i EU:s första pelare – till skillnad mot rambeslutet som antagits inom ramen för tredje pelaren – inte påverkas. Det gäller t.ex. direktiv om intrång i immateriella rättigheter i en digital miljö.

I avsnitt 6.1.2–6.1.4 har lämnats en redogörelse för gällande svenska straffbestämmelser, däribland dataintrångsbestämmelsen och reglerna om brytande av telehemlighet och intrång i förvar. Redan vid en översiktlig jämförelse mellan dessa svenska bestämmelser och rambeslutets regler om straffbara gärningar framgår att det straffbara området enligt dataintrångsbestämmelsen i stor utsträckning motsvarar rambeslutets regler. Syftet är i båda fallen att ge ett skydd för automatisk databehandling. Bestämmelserna om brytande av telehemlighet och intrång i förvar däremot har som primärt syfte att skydda post, telegram och

andra meddelanden. Vidare omfattar bestämmelsen om brytande av telehemlighet endast meddelanden som är under pågående befordran och som befordras mellan en avsändare och en mottagare. Rambeslutets bestämmelser förutsätter däremot inte att datorbehandlingsbara uppgifter skall vara avsedda för någon annan än den som står bakom dem. Rambeslutet torde dessutom inte avse sådana uppgifter när de överförs i nät, jfr avsnitt 6.2.2–6.2.4.

Det måste därför anses ligga närmast till hands att utgå direkt från dataintrångsbestämmelsen i analysen av hur svensk straffrätt förhåller sig till rambeslutets krav på straffbara handlingar trots att den är subsidiär i förhållande till de andra nämnda bestämmelserna. Dataintrångsbestämmelsen kommer alltså att tas till utgångspunkt i bedömningen av behovet av lagändringar.

6.2.2 Olagligt intrång i informationssystem

Bedömning: Dataintrångsbestämmelsen uppfyller rambeslutets krav på vad som skall vara straffbelagt som olagligt intrång i informationssystem.

Skälen för bedömningen: Enligt *artikel 2* 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 artikel 2 som dataintrångsbestämmelsen förutsätter alltså för det första att gärningen begås med uppsåt.

Vidare krävs enligt artikel 2 att gärningen utförs orättmätigt och enligt bestämmelsen om dataintrång att gärningen är olovlig. Begreppet orättmätigt definieras i artikel 1 d bl.a. som att gärningen sker utan tillstånd av ägaren eller annan rättighetshavare till systemet eller del av systemet. Kravet på orättmätighet innebär alltså att handlingar som i och för sig uppfyller övriga krav för straffbarhet 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 område som skall vara straffbelagt. Denna innebörd av begreppet orättmätigt motsvarar vad som måste anses gälla i fråga om olovlighetskravet i dataintrångsbestämmelsen. I t.ex. den närbesläktade bestämmelsen om brytande av telehemlighet anses vid tillämpningen av olovlighetsrekvisitet en gärning inte som olovlig när den utförs med samtycke av den som äger förfoga över telemeddelandet.

Kravet på orättmätighet enligt artikel 2 innebär vidare enligt definitionen i artikel 1 d att handlingar som medges i nationell lagstiftning faller utanför det straffbara området. Olovlighetskravet i dataintrångsbestämmelsen innebär liksom motsvarande krav i t.ex. bestämmelsen om brytande av telehemlighet att gärningar som utförs med stöd av lagstiftning utesluts från straffansvar. Det kan t.ex. vara fråga om brottsbekämpande åtgärder. Rekvisiten orättmätighet och olovlighet överensstämmer följaktligen även i detta hänseende.

Enligt artikel 2 skall handlingen bestå i ett intrång i ett informationssystem. I artikel 1 a definieras informationssystem som en apparat eller flera sammanhängande apparater som 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. En fråga är om de uppgifter som avses skall finnas i apparaterna eller om artikeln också omfattar intrång i sådana uppgifter när de befordras i nät. Det framgår inte av rambeslutets ingress att avsikten varit att generellt bereda ett skydd för uppgifter som överförs i nät. Tvärtom kan noteras att definitionen av informationssystem inte omfattar nät. I kommissionens ursprungliga förslag till rambeslutet ingick däremot nät i definitionen. Då avsåg den uppgifter som lagras, behandlas, hämtas eller överförs med hjälp av *datorer eller nät* för att *dessa* skall kunna drivas etc. Datorer definierades i sin tur som apparater för automatisk databehandling. Frågan om nät skulle omfattas av begreppet informationssystem var föremål för diskussioner under förhandlingarna om rambeslutet.

Det hävdades att det straffbara området skulle kunna bli alltför långtgående om nät inkluderades. Det hänvisades också till att Europarådets konvention om IT-relaterad brottslighet, som presenterats i avsnitt 5, innehåller en bestämmelse om olagligt intrång i datorsystem (artikel 2) som inte omfattar nät. Slutligen enades man om att inte ta med nät i definitionen. Det gjordes dock inte någon ändring av definitionen i den del den angav att uppgifter hämtas, överförs m.m.

Vidare skall beaktas att artikel 4 om olaglig datastörning kriminaliserar störningar av datorbehandlingsbara uppgifter *i ett informationssystem.* Den bestämmelsen, som avser fler uppgifter än de som omfattas av artikel 2 och flera olika sorters angrepp förutom just intrång enligt artikel 2, förutsätter alltså att uppgifterna finns i ett informationssystem, som ju definieras med uteslutande av nät. Bestämmelsen kan alltså inte anses omfatta angrepp på uppgifter när de befordras i nät. Artikel 2 kan knappast ha ett vidare tillämpningsområde i detta avseende.

Mot den nu beskrivna bakgrunden måste rambeslutets begrepp informationssystem förstås så att det inte omfattar uppgifter som överförs i nät. Artikel 2 avser därmed intrång i apparater för automatisk databehandling och intrång i uppgifter som finns i sådana apparater för drift, användning, skydd och underhåll av dessa.

Dataintrångsbestämmelsen straffbelägger den som bereder sig tillgång till upptagning för automatisk databehandling. Skyddsobjektet är alltså uppgifter avsedda för automatisk databehandling. Det är dock tillräckligt att någon *bereder sig tillgång* till sådana uppgifter, dvs. att personen *kan få del* av dem. Det krävs inte att han eller hon verkligen *tar del* av uppgifterna. Det är därför en rimlig tolkning av bestämmelsen att den kan vara tillämplig så snart någon olovligen tagit sig in en apparat eller ett program som används för att behandla sådana uppgifter. Genom tillträdet till apparaten eller programmet har personen skaffat sig möjlighet att ta del av de uppgifter som finns däri och alltså berett sig tillträde till dessa. Dataintrångsbestämmelsens kriminalisering måste följaktligen i praktiken anses täcka det som enligt

artikel 2 skall vara straffbart som intrång i apparater för databehandling och uppgifter för drift, användning, skydd och underhåll.

Sammanfattningsvis görs alltså bedömningen att dataintrångsbestämmelsen redan i dag uppfyller rambeslutets krav på vad som skall vara straffbelagt som olagligt intrång i informationssystem.

6.2.3 Olaglig systemstörning

Bedömning: Svensk rätt, främst dataintrångsbestämmelsen, uppfyller till övervägande del rambeslutets krav att det skall vara straffbelagt som olaglig systemstörning att avbryta eller allvarligt hindra ett informationssystems drift. Det krävs dock lagändring för att rambeslutet fullt ut skall uppfyllas i denna del.

Skälen för bedömningen: 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.

I dataintrångsbestämmelsen straffbeläggs att olovligen ändra eller utplåna en upptagning för automatisk databehandling eller att föra in en sådan upptagning i register. Intrång i en upptagning är också straffbelagt.

Dataintrångsbestämmelsen förutsätter uppsåt och motsvarar därvidlag artikel 3. Båda bestämmelserna förutsätter vidare att handlingen utförs olovligen respektive orättmätigt. Innebörden av dessa begrepp måste anses vara densamma. I denna fråga hänvisas till vad som sagts i avsnitt 6.2.2 om olagligt intrång i informationssystem.

Enligt artikel 3 skall handlingen riktas mot driften av ett informationssystem. Begreppet informationssystem definieras i artikel 1 a. Den handling som skall vara straffbelagd består i att

allvarligt hindra eller att avbryta driften av systemet. Hur denna störning kan åstadkommas anges genom en uppräkning av olika åtgärder med datorbehandlingsbara uppgifter enligt definitionen i artikel 1 b. Sedvanliga åtgärder som att testa säkerheten hos ett system eller att installera nya program, som vidtas av behöriga personer i enlighet med behörigheten, utgör inte olagliga störningar av informationssystem.

Dataintrångsbestämmelsen kriminaliserar inte direkt ett avbrytande eller annat allvarligt hindrande av driften av apparater för automatisk databehandling eller uppgifter för drift, användning, skydd och underhåll. Däremot straffbeläggs vissa förfaranden med upptagningar. I den mån dessa förfaranden motsvarar de uppräknade åtgärderna med datorbehandlingsbara uppgifter måste bestämmelsen anses uppfylla det krav på kriminalisering som artikel 3 innebär, eftersom bestämmelsen då straffbelägger dessa åtgärder i sig utan krav på att driften av informationssystemet påverkas. I avsnitt 7.2 föreslås ett klargörande av vad upptagningsbegreppet omfattar.

Att ändra eller utplåna upptagningar måste anses motsvara de handlingar i artikel 3 som benämns att skada, radera, försämra och ändra datorbehandlingsbara uppgifter. Begreppet datorbehandlingsbara uppgifter motsvaras i stort av det svenska upptagningsbegreppet, som omfattar uppgifter som är fixerade på datamedium eller som befordras för att användas för automatisk databehandling. Dessutom omfattar dataintrångsbestämmelsen t.ex. en ändring av ett program som styr databehandlingen av en viss upptagning. Detsamma måste gälla ett utplånande i motsvarande fall. Därmed kan dataintrångsbrottet sägas omfatta att skada, radera, försämra och ändra datorbehandlingsbara uppgifter enligt artikel 3.

Artikelns handlingar att hindra flödet av och göra det omöjligt att komma åt datorbehandlingsbara uppgifter kan i vissa fall åstadkommas genom en ändring eller ett utplånande direkt av en upptagning eller av andra uppgifter som styr databehandlingen av en upptagning. Handlingarna kan också vara straffbara enligt dataintrångsbestämmelsen i övrigt. Emellertid torde inte be-

stämmelsen omfatta samtliga situationer av hindrande eller otillgängliggörande av datorbehandlingsbara uppgifter, t.ex. när åtgärderna medför endast tillfälliga effekter.

I artikel 3 anges slutligen inmatningar och överföringar av datorbehandlingsbara uppgifter. Sådana åtgärder torde också i många fall utgöra dataintrång, eftersom de samtidigt kan medföra att upptagningar ändras eller utplånas. Dessutom är det straffbart som dataintrång att göra införingar i register. Även åtgärder som samtidigt innebär att någon olovligen bereder sig tillgång till en upptagning är straffbara. Det kan dock finnas fall som inte omfattas av dataintrångsbestämmelsen, t.ex. situationer där någon genom automatiskt genererade meddelanden kontaktar eller försöker kontakta ett informationssystem (tillgänglighetsattacker).

Frågan är då om andra svenska straffbestämmelser uppfyller åtagandet i artikel 3, särskilt i de delar som dataintrångsbestämmelsen är otillräcklig. De bestämmelser som främst är av intresse är reglerna om skadegörelse- och sabotagebrott. Bestämmelserna avser angrepp på egendom som medför att egendomen förstörs eller skadas. Normalt förutsätts att skadan är av inte endast tillfällig natur. Sabotagebrottet omfattar dessutom andra åtgärder som allvarligt stör eller hindrar användningen av viss egendom. Dessa straffbestämmelser kan omfatta de situationer som skall vara straffbara enligt artikel 3 som avbrytande eller hindrande av ett informationssystems drift. De torde t.ex. kunna tillämpas när apparater för automatisk databehandling eller program skadas. Bestämmelserna torde dock inte täcka alla situationer som skall vara straffbelagda, t.ex. fall när skadan endast är tillfällig. De omfattar alltså inte heller de situationer som faller utanför dataintrångsbestämmelsens tillämpningsområde.

Straffbestämmelsen om egenmäktigt förfarande (8 kap. 8 § brottsbalken) kan vara tillämplig när besittningen till en fysisk databärare olovligen rubbas men knappast i andra fall, eftersom brottet torde kräva en rumslig besittningsrubbning. Det är vidare straffbart som undertryckande av urkund att under vissa förutsättningar förstöra, göra obrukbar eller undanskaffa en urkund

(14 kap. 4 § brottsbalken). Det saknas dock praxis huruvida denna och vissa andra liknande straffbestämmelser omfattar elektroniska rutiner. Det planeras därför en utredning som skall få i uppdrag att se över dessa bestämmelser ur ett IT-perspektiv.

Av det redovisade framgår att dataintrångsbestämmelsen men också andra straffbestämmelser, i första hand de om skadegörelse- och sabotagebrott, till övervägande del uppfyller rambeslutets krav att det skall vara straffbart som olaglig systemstörning att avbryta eller allvarligt hindra driften av ett informationssystem. De är dock inte tillräckliga för att helt uppfylla åtagandena i artikeln. Det krävs därmed lagändring för att rambeslutet fullt ut skall uppfyllas i denna del.

6.2.4 Olaglig datastörning

Bedömning: Svensk rätt, främst dataintrångsbestämmelsen, uppfyller till övervägande del rambeslutets krav på vilka handlingar som skall vara straffbelagda som olaglig datastörning. De svenska bestämmelserna motsvarar dock inte fullt ut kraven att det skall vara straffbart att hindra flödet av datorbehandlingsbara uppgifter i ett informationssystem eller göra sådana uppgifter oåtkomliga. I dessa avseenden krävs lagändring för att rambeslutet helt skall uppfyllas i denna del.

Skälen för bedömningen: Enligt *artikel 4* 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, när gärningen utförs orättmätigt, åtminstone i fall som inte är ringa.

Enligt dataintrångsbestämmelsen är det straffbelagt att olovligen ändra eller utplåna en upptagning för automatisk databehandling eller att föra in en sådan upptagning i ett register. Det är också straffbelagt att göra intrång i en upptagning.

För ansvar enligt dataintrångsbestämmelsen krävs liksom enligt artikel 4 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 sagts i avsnitt 6.2.2 om olagligt intrång.

Den straffbara handlingen enligt artikel 4 riktar sig mot datorbehandlingsbara uppgifter i ett informationssystem. Den avser alltså inte uppgifterna när de befordras i nät. Detta har utvecklats i avsnittet om olagligt intrång och det hänvisas till resonemanget där. Begreppet datorbehandlingsbara uppgifter definieras i artikel 1 b.

Datastörningen skall bestå i att radera, skada, försämra eller ändra datorbehandlingsbara uppgifter. Som angetts i avsnitt 6.2.3 om olaglig systemstörning måste dessa handlingar anses motsvara vad som enligt dataintrångsbestämmelsen är straffbelagt som att ändra eller utplåna upptagningar.

Enligt artikel 4 skall det vidare vara straffbart att hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter. Som också angetts i avsnittet om systemstörning kan sådana störningar redan vara straffbelagda enligt dataintrångsbestämmelsen. I vissa fall kan dock störningarna åstadkommas utan att de är straffbara som dataintrång.

Som vidare konstaterats i det avsnittet kan andra svenska straffbestämmelser, främst om skadegörelse- och sabotagebrott, omfatta de situationer som skall vara straffbelagda enligt artikel 4. De motsvarar dock inte heller fullt ut åtagandet i artikeln att det skall vara straffbart att hindra flödet av och göra det omöjligt att komma åt uppgifter. I dessa avseenden krävs alltså lagändring för att rambeslutet helt skall uppfyllas i denna del.

6.2.5 Anstiftan av, medhjälp till och försök till brott

Bedömning: Svensk rätt uppfyller rambeslutets krav om kriminalisering av anstiftan, medhjälp och försök i fråga om de straffbara gärningar enligt rambeslutet som täcks av straffbestämmelserna om dataintrång, skadegörelse, grov skadegörelse, sabotage och grovt sabotage.

Skälen för bedömningen: Enligt *artikel 5* skall anstiftan av och medhjälp till olagligt intrång, olaglig systemstörning och olaglig datastörning vara straffbelagt. I svensk rätt är medverkan till dataintrång, skadegörelse, grov skadegörelse samt sabotage och grovt sabotage kriminaliserat.

Vidare skall försök till olagligt intrång, olaglig systemstörning och olaglig datastörning vara straffbart. När det gäller intrång får dock en medlemsstat besluta att inte straffbelägga försök. I svensk rätt är försök till dataintrång straffbart. Det gäller dock inte om intrånget skulle ha varit att anse som ringa om det hade fullbordats. Eftersom rambeslutet inte kräver att ringa fall av fullbordade brott straffbeläggs, bör inte heller krävas att försök straffbeläggs i de fall det fullbordade brottet skulle ha varit ringa, även om den fullbordade gärningen i och för sig är kriminaliserad. Den svenska kriminaliseringen av försök till dataintrång måste alltså anses förenlig med rambeslutets försöksbestämmelse. När det gäller skadegörelse, grov skadegörelse, sabotage och grovt sabotage är försök till dessa brott straffbelagt.

Svensk rätt uppfyller följaktligen rambeslutets krav om kriminalisering av anstiftan, medhjälp och försök i fråga om de gärningar som skall vara straffbara enligt rambeslutet och som täcks av straffbestämmelserna om dataintrång, skadegörelse, grov skadegörelse, sabotage och grovt sabotage.

6.3 Påföljder och försvårande omständigheter

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

Skälen för bedömningen: Enligt *artikel 6 punkt 1* skall de handlingar som enligt rambeslutet skall vara straffbara vara belagda med effektiva, proportionella och avskräckande straffrättsliga påföljder.

Artikel 6 punkt 2 föreskriver att de brott som avses i artiklarna 3 och 4, dvs. olaglig systemstörning och olaglig datastörning men däremot inte olagligt intrång 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. Det innebär att fängelse i åtminstone ett år skall finnas i straffskalan. 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. Straffskalorna uppfyller alltså artikel 6 punkt 2. Följaktligen krävs inte någon lagändring för att uppfylla åtagandena i artikel 6.

I *artikel 7 punkt 1* föreskrivs att det skall ses som en försvårande omständighet att brott begås inom ramen för en sådan kriminell organisation som avses i den gemensamma åtgärden 98/733/RIF av den 21 december 1998 om att göra deltagande i en kriminell organisation i Europeiska unionens medlemsstater till ett brott. Enligt svensk rätt skall som en 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. Bestämmelsen måste anses motsvara åtagandet i artikel 7 punkt 1.

När en sådan försvårande omständighet som anges i artikeln föreligger skall vidare de gärningar som avses i artikel 2 punkt 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 olagligt intrång som begås genom intrång i en säkerhetsåtgärd, olaglig systemstörning och olaglig datastörning 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 därmed inte någon lagändring. Emellertid kan enligt svensk rätt sådana omständigheter motivera att brottet bedöms som grov skadegörelse, sabotage eller grovt sabotage. Straffskalorna för dessa brott motsvarar den fängelsenivå i punkt 1 som punkt 2 anvisar.

Sammanfattningsvis görs alltså bedömningen att svensk rätt uppfyller rambeslutets bestämmelser om påföljder och försvårande omständigheter.

Avslutningsvis skall kort beröras frågan om det ändå finns anledning att nu föreslå straffskärpningar.

I samband med propositionen om Sveriges antagande av rambeslutet (prop. 2003/04:164) bereddes bl.a. vissa myndigheter tillfälle att lämna synpunkter på ett utkast till propositionen (dnr Ju2004/4752/L5). Myndigheterna instämde i eller invände inte mot regeringens bedömning att rambeslutets bestämmelser i de nu aktuella delarna inte kräver lagändringar. Ett par myndigheter framförde dock att det likväl bör införas en strängare straffskala för dataintrång eller ett grovt dataintrångsbrott.

Dataintrång kan medföra fängelse i upp till två år. Vidare kan en gärning av detta slag vara sådan att den skall bedömas som grov skadegörelse, sabotage eller grovt sabotage. För dessa brott kan ännu längre fängelsestraff följa. Ett sådant brott kan i sin tur vara att bedöma som terroristbrott enligt lagen (2003:148) om straff för terroristbrott, jfr avsnitt 6.1.1. För sådant brott gäller en straffskala från fängelse i lägst två år upp till livstid. Det finns alltså i allvarliga fall ett stort utrymme att ingripa med kraftfulla reaktioner.

En straffhöjning för dataintrång eller ett införande av ett grovt sådant brott skulle dessutom förutsätta, förutom ett behov av en sådan lagändring, överväganden om det behövs motsvarande ändringar i de andra bestämmelser i 4 kap. brottsbalken som har ett samband med dataintrångsbestämmelsen. Dessa har i dag samma straffskala och saknar också en gradindelning av brotten.

Mot denna bakgrund föreslås inte någon ändring av straffskalan för dataintrång eller ett införande av ett grovt sådant brott.

6.4 Ansvar och påföljder för juridiska personer

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

Skälen för bedömningen: I *artiklarna 8 och 9* finns 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 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), och är alltså vedertagen.

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

Bestämmelserna utgör standardbestämmelser som finns i flera andra antagna rambeslut, bl.a. i rambeslutet 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 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 var nödvändiga till följd av rambeslutet (prop. 2000/01:40, bet. 2000/01:JuU9, rskr. 2000/01:138). I den rapport som kommissionen upprättade avseende medlemsstaternas genomförande av rambeslutet (KOM [2002] 771 slutlig) angavs också att Sverige har lagstiftning om

att juridiska personer kan ställas till rättsligt ansvar för de brott som omfattas av rambeslutet.

Även i fråga om rambeslutet om angrepp mot informationssystem får de svenska reglerna om företagsbot anses uppfylla de krav som uppställs vad gäller ansvar och påföljder för juridiska personer.

6.5 Behörighet

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 bedömningen: *Artikel 10 punkt 1 a* 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 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.

Enligt svenska regler om straffrättslig behörighet (domsrätt) döms efter svensk lag vid svensk domstol för brott som begåtts här i riket. Detsamma gäller om det är ovisst var ett brott har förövats men det finns skäl att anta att det har begåtts inom riket. Ett brott anses begånget där den brottsliga handlingen företogs och också där brottet fullbordades eller, vid försök, där brottet skulle ha fullbordats. Så snart någon del av handlingen har ägt rum här i riket är alltså handlingen i sin helhet att anse som begången i Sverige.

Dessa bestämmelser ger i praktiken svenska domstolar behörighet att döma över brott i de fall som avses i punkt 1 a och punkt 2. Bestämmelserna måste därför anses uppfylla rambeslutet i dessa avseenden. Någon lagändring krävs därför inte.

Enligt svensk rätt döms vidare för brott som begåtts utom riket efter svensk lag vid svensk domstol bl.a. om brottet har begåtts av en svensk medborgare.

Härigenom 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.

Enligt *punkt 1 c* skall en medlemsstat vidare ha behörighet att döma över brott enligt rambeslutet som har begåtts till förmån för en juridisk person som har sitt huvudkontor på medlemsstatens territorium. 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. Bestämmelsen i punkt 1 c motsvaras dock inte av en likalydande behörighetsregel i svensk rätt. Sverige bör därför utnyttja den möjlighet som föreskrivs i *punkt 5* att inte tillämpa denna bestämmelse 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 EU samt att vissa omständigheter därvid kan beaktas. Sådant samråd torde i dag i förekommande fall äga rum formlöst. Någon särskild reglering av frågan kan inte anses nöd-

vändig. Det skall i sammanhanget nämnas att EU:s rambeslut om bekämpande av terrorism innehåller en motsvarande bestämmelse som inte har lett till lagstiftningsåtgärder (jfr prop. 2001/02:135 och 2002/03:38).

Sammanfattningsvis görs bedömningen att svensk domsrätt föreligger i samtliga fall där medlemsstaterna ovillkorligen skall kunna utöva domsrätt och att bestämmelsen om samarbete för att avgöra behörighetsfrågor inte kräver någon lagreglering.

6.6 Utbyte av uppgifter

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

Skälen för bedömningen: Enligt *artikel 11* 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 ingressskäl 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). Detta nätverk skapades i G8, som utgörs av åtta ledande industriländer. I rådsrekommendationen från 2001 uppmanas de medlemsstater som ännu inte anslutit sig till G8-nätverket att göra det. Av artikel 11 följer vidare att varje medlemsstat skall underrätta rådets generalsekretariat och kommissionen om sin kontaktpunkt.

Sverige har deltagit i detta nätverk sedan 1999. Rikskriminalpolisens IT-brottsrotel har en beredskap dygnet runt som innebär att en IT-brottsspecialist alltid kan nås. Inom Rikspolisstyrelsen har tillskapats en funktion för samordning av IT-relaterade brott och incidenter. Funktionen är gemensam för Säkerhetspolisen och Rikskriminalpolisen.

Det finns alltså redan en svensk kontaktpunkt rörande högteknologisk brottslighet. Artikel 11 innebär att denna skall användas för utbyte av uppgifter om brotten enligt rambeslutet. I detta måste självklart ligga att informationsutbytet skall ske i de former som gäller i dag, dvs. med iakttagande av gällande bestämmelser om dataskydd och sekretessregler. Det förra framgår uttryckligen av artikeln. Någon reglering för att uppfylla åtagandet i artikeln kan följaktligen inte anses behövlig. Sverige bör genom regeringens försorg underrätta rådets generalsekretariat och kommissionen om sin kontaktpunkt.

I sammanhanget skall nämnas Sveriges IT-incidentcentrum (Sitic). Sitic:s främsta uppgift är att stödja samhället i arbetet med skydd mot IT-incidenter genom ett system för informationsutbyte mellan samhällets organisationer och Sitic. Sitic skall snabbt sprida information i samhället om nya problem som kan störa IT-system. Sitic följer kontinuerligt information om sårbarheter och förändringar i mönstret för Internettrafiken. Att lämna information och råd om förebyggande åtgärder ingår också i uppdraget. Slutligen skall Sitic sammanställa och ge ut statistik som underlag för förbättringar i det förebyggande arbetet.

Vidare skall nämnas att Krisberedskapsmyndigheten har ett sammanhållande myndighetsansvar för samhällets informationssäkerhet. I det arbetet ingår bl.a. att genomföra och sammanställa risk- och sårbarhetsanalyser, som tillsammans med underrättelseunderlag, utgör grunden för en årlig bedömning till regeringen.

7 Ett utvidgat straffansvar för dataintrång

7.1 Utgångspunkter för genomförandet av rambeslutets bestämmelser om straffbara handlingar

Förslag: För att rambeslutets bestämmelser om straffbara handlingar fullt ut skall uppfyllas utvidgas dataintrångsbestämmelsen.

Skälen för förslaget: Av avsnitt 6.2–6.6 har framgått att svensk rätt i stort uppfyller bestämmelserna i rambeslutet om angrepp mot informationssystem. Rambeslutets krav på vilka handlingar som skall vara straffbelagda uppfylls till övervägande del av gällande straffbestämmelser. Det finns dock vissa situationer som skall vara straffbelagda enligt rambeslutet som inte är kriminaliserade i svensk rätt. Det innebär i sin tur att medverkan till och försök till de i dag straffria handlingarna inte är kriminaliserat. Enligt rambeslutet skall emellertid anstiftan av och medhjälp till samt försök till dessa handlingar vara straffbelagt. Eftersom rambeslutet är bindande för Sverige, krävs svenska lagändringar i dessa avseenden för att rambeslutet helt skall uppfyllas. Som regeringen konstaterat i propositionen om Sveriges antagande av rambeslutet (prop. 2003/04:164) avser ändringarna förfaranden som från svensk utgångspunkt måste anses straffvärda.

De handlingar som utgör angrepp mot informationssystem enligt rambeslutet motsvaras i första hand av dataintrångsbestämmelsen. De skäl som har angetts i avsnitt 6.2.1 för att i första hand överväga dataintrångsbestämmelsen i analysen av hur

gällande svensk rätt förhåller sig till rambeslutets regler om straffbara handlingar talar också för att lagändringarna bör göras i den bestämmelsen. Analysen i avsnitt 6.2.2–6.2.4 har vidare visat att dataintrångsbestämmelsens kriminaliseringar av åtgärder med upptagningar för automatisk databehandling måste anses motsvara åtagandena enligt rambeslutet att kriminalisera vissa förfaranden med informationssystem och datorbehandlingsbara uppgifter. Bestämmelsen kriminaliserar dessutom redan i stor utsträckning de åtgärder som skall vara straffbelagda enligt rambeslutet. Den är vidare uppbyggd med krav på uppsåt och olovlighet på ett sätt som överensstämmer med rambeslutet. Det föreslås därför att rambeslutets bestämmelser om straffbara gärningar skall uppfyllas fullt ut genom att dataintrångsbestämmelsen utvidgas.

Av det sagda följer samtidigt att bestämmelsen inte bör omarbetas för att överensstämma med rambeslutets formuleringar av åtgärder som utgör angrepp eller rambeslutets tekniska begrepp som t.ex. informationssystem. Bestämmelsen uppfyller redan till stor del det som skall vara straffbelagt enligt rambeslutet. De utvidgningar av straffansvaret som krävs för att helt uppfylla rambeslutet är begränsade och bör genomföras utan genomgripande förändringar av bestämmelsen. Ett införande av ett nytt eller alternativt skyddsobjekt som t.ex. informationssystem skulle i onödan komplicera bestämmelsen. Det skulle också riskera att utsträcka kriminaliseringen av t.ex. intrång för långt. I sammanhanget skall erinras om att straffbestämmelserna om skadegörelse- och sabotagebrott uppfyller rambeslutet i vissa delar. En större omarbetning av dataintrångsbestämmelsen skulle vidare kunna medföra en vidlyftig lagtext. En fördel med bestämmelsen i dag är att den – liksom svensk straffrättslig reglering i allmänhet – är koncentrerad.

Bestämmelsen föreslås följaktligen så långt möjligt behållas i sin nuvarande utformning när den kompletteras med de tillägg som är nödvändiga till följd av rambeslutet. Det innebär att kraven på uppsåt och olovlighet skall behållas. Det innebär vidare att upptagningar även fortsättningsvis skall vara skyddsobjekt. I

fråga om upptagningsbegreppet föreslås dock några ändringar för att klargöra och modernisera detta, se avsnitt 7.2.

7.2 Upptagningsbegreppet

Förslag: Det klargörs att dataintrångsbestämmelsen omfattar alla uppgifter som befordras via elektromagnetiska vågor och som är avsedda för databehandling. Dessutom moderniseras bestämmelsen genom att uttrycket automatisk databehandling ersätts med automatiserad databehandling.

Skälen för förslaget

Ett klargörande av upptagningsbegreppet

Innan de lagändringar som rambeslutet föranleder i dataintrångsbestämmelsen behandlas bör övervägas om bestämmelsen behöver klargöras i fråga om upptagningsbegreppet. Som framgått tidigare kan det diskuteras om den är tillämplig på alla uppgifter för databehandling som överförs oavsett hur befordran sker.

Bestämmelsen omfattar upptagning för automatisk databehandling. Med sådan upptagning avses uppgift som är fixerad på datamedium och som är läsbar endast med teknik för sådan behandling. Med upptagning jämställs uppgift som är under befordran via elektroniskt eller liknande hjälpmedel för att användas för automatisk databehandling. Med sådan uppgift avses uppgift som ännu inte fixerats på datamedium.

Lagstiftarens syfte har varit att bereda ett skydd för överföringar av både uppgifter som är fixerade och uppgifter som ännu inte är fixerade på datamedium. När lagstiftningen infördes i början av 1970-talet och kompletterades i mitten av 1980-talet skedde uppgiftsöverföringar inte i nät i den omfattning som sker i dag. De uppgifter som överfördes i nät förmedlades i huvudsak i ledningsbundna nät. Det fanns dock redan då även teknik för befordran via radio (jfr prop. 1973:33 s. 15). I dag sker uppgifts-

överföringar i stor utsträckning också via radio. Exempel på ledningsbundna nät är optisk fiberkabel, fasta telefonnät, kabel-TV-nät och elnät. Exempel på nät via radio utgör mobiltelefonnät eller annan trådlös radioaccess, satelliter samt markbundna nät för analog och digital TV och radio. Datakommunikation kan överföras i nationella stomnät, som främst är baserade på optiska fiberkablar men också till viss del radiolänk (prop. 2002/03:110 s. 61 f.). Även exempelvis uppgraderade telefonnät, satellit samt marknätet för digital TV kan användas för sådan kommunikation.

Skyddsbehovet för uppgifter gör sig gällande oavsett på vilket sätt uppgifterna befordras. Lagstiftningen bör därför ge ett heltäckande skydd för uppgifter som överförs.

Dataintrångsbestämmelsens lydelse kan i sig inte anses utesluta att detta skydd finns redan i dag. En försiktighet vid tolkningen kan dock vara påkallad med hänsyn till hur tekniken såg ut när lagstiftningen tillkom men också med hänsyn till grundläggande principer för tolkning av straffrättsliga bestämmelser. En utgångspunkt är att analogiska tolkningar skall undvikas. Å andra sidan har straffbestämmelser inte ett statiskt innehåll. De skall kunna tillämpas också om de tekniska förhållandena ändras. Det kan därför hävdas att dataintrångsbestämmelsen omfattar samtliga överföringar av uppgifter. För en sådan tolkning talar att det straffrättsliga skyddet annars urholkas genom den tekniska utvecklingen. För att det inte skall råda någon tvekan i fråga om tillämpningsområdet för dataintrång bör bestämmelsen förtydligas så att det framgår att den omfattar alla uppgifter som befordras.

Den närmare utformningen av klargörandet

Klargörandet av att dataintrångsbestämmelsen omfattar alla uppgifter för automatisk databehandling som befordras kan ske genom en omformulering av den del av bestämmelsen som anger att med upptagning avses även uppgifter som är under befordran via ett elektroniskt eller annat liknande hjälpmedel för att använ-

das för automatisk databehandling. En fördel med detta är att det ursprungliga upptagningsbegreppet kan lämnas oförändrat.

Ändringen bör ske genom att uttrycket ”elektroniskt eller annat liknande hjälpmedel” ersätts. I yttrandefrihetsgrundlagen (YGL) anges att information överförs med hjälp av *elektromagnetiska vågor* (1 kap. 1 § tredje stycket och 9 § första stycket). I lagen (2003:389) om elektronisk kommunikation talas om överföring i *elektroniska kommunikationsnät* (1 kap. 7 §). Vid övervägande av vilket uttryckssätt som bör införas i dataintrångsbestämmelsen är avgörande att det inte får råda något tvivel om att bestämmelsen omfattar alla uppgifter för databehandling som överförs, även uppgifter som befordras mellan en dator och dess utrustning. Det framstår därför som lämpligast att använda samma terminologi som i YGL. Det uttryckssättet täcker alla former för att överföra uppgifter för databehandling som finns i dag.

Vidare bör orden ”för att användas för” ersättas med ”och som är avsedda för” så att bestämmelsen generellt täcker uppgiftsöverföringar oavsett om uppgifterna har fixerats på datamedium eller inte.

Sammanfattningsvis föreslås ett klargörande av att dataintrångsbestämmelsen omfattar alla uppgifter som befordras via elektromagnetiska vågor och som är avsedda för databehandling.

Särskilt om befordran via radio

Bestämmelsen om brytande av telehemlighet, som dataintrångsbestämmelsen har ett nära samband med, omfattar telemeddelanden oavsett hur de tekniskt förmedlas. Straffansvar inträder dock normalt inte när det är fråga om brytande av meddelanden som befordras via radio. Detta på grund av att olovlighetskravet inte anses uppfyllt med hänsyn till principen om att etern är fri.

Sedan länge gäller både nationellt och internationellt som en grundläggande princip att etern är fri. Det innebär att det i princip är tillåtet att avlyssna meddelanden som befordras via radio (se. tex. prop. 1992/93:200 s. 166 och 2002/03:110 s. 254).

Principen om eterns frihet innebär i dag för straffrättens del att bestämmelsen om brytande av telehemlighet i regel inte är tillämplig på radiobefordrade telemeddelanden. Det anses, som nämnts, följa av att bestämmelsens krav på olovlighet då inte är uppfyllt. Även dataintrångsbestämmelsen, som också ger ett skydd för uppgifter under befordran, förutsätter för straffansvar att en gärning är olovlig. Att dataintrångsbestämmelsen omfattar uppgifter som överförs via radio är alltså inte oförenligt med principen om att etern är fri. Frågan om olovlighetsrekvisitet kan anses uppfyllt eller inte i dessa fall torde främst vara intressant i situationer som rör intrång.

En språklig modernisering av upptagningsbegreppet

Utöver det ovan föreslagna klargörandet av upptagningsbegreppet finns anledning att överväga begreppet i ytterligare ett avseende. Skälet är en ändrad begreppsanvändning i annan svensk lagstiftning som är av relevans i sammanhanget.

Upptagningsbegreppet tillkom ursprungligen i samband med att vissa ändringar gjordes i 2 kap. tryckfrihetsförordningen (TF) om allmänna handlingars offentlighet. I TF har begreppet senare – den 1 januari 2003 – modifierats på det sättet att det i lagtexten i stället för upptagning för *automatisk* databehandling anges upptagning för *automatiserad* databehandling. Ändringen motiverades med att det nya uttrycket bättre överensstämde med gällande terminologi för behandling av uppgifter (prop. 2001/02:70 s. 13 och 23). Det hänvisades också till att det gamla begreppet inte finns i personuppgiftslagen (1998:204), som ersatt datalagen, eller i de registerförfattningar som tillkommit efter att personuppgiftslagen trätt i kraft. Någon saklig skillnad mellan de båda begreppen ansågs inte föreligga.

De skäl som åberopats för moderniseringen av upptagningsbegreppet i TF måste anses motivera motsvarande ändring i dataintrångsbestämmelsen. Det föreslås därför att ”upptagning för automatisk databehandling” ersätts med ”upptagning för *automatiserad* databehandling”. Vidare föreslås att orden ”automatisk

databehandling” i den del av bestämmelsen som jämställer uppgifter under befordran med sådan upptagning ändras till ”*automatiserad* databehandling”. Några ändringar i sak är det inte fråga om.

7.3 Undertryckande och allvarligt hindrande av användningen av en upptagning

Förslag: Den som uppsåtligen och olovligen undertrycker eller på annat sätt allvarligt hindrar användningen av en upptagning för automatiserad databehandling döms för dataintrång.

Skälen för förslaget

Undertryckande av en upptagning

Enligt *artikel 4* skall det vara straffbart att uppsåtligt och orättmätigt hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter i ett informationssystem. Sådana störningar är i dag inte alltid straffbara. Dataintrångsbestämmelsen måste därför kompletteras så att störningarna blir straffbelagda fullt ut.

I avsnitt 7.1 har slagits fast att bestämmelsens skyddsobjekt även fortsättningsvis skall vara upptagning samt att kraven på uppsåt och olovlighet skall behållas. Det handlande som skall straffbeläggas kan förslagsvis uttryckas på det sättet att en upptagning undertrycks. I straffbestämmelsen om undertryckande av urkund används begreppet undertrycka för att beskriva att en urkund görs obrukbar, undanskaffas eller förstörs (se 14 kap. 4 § brottsbalken). Trots att begreppet omfattar också undertryckande av mer permanent natur måste det i allmänhet anses väl uttrycka det handlande som skall kriminaliseras enligt artikel 4. En fördel är också att begreppet anger handlandet på ett koncentrerat sätt.

Det föreslås följaktligen att den som uppsåtligen och olovligen undertrycker en upptagning för automatiserad databehandling skall dömas för dataintrång.

Påpekas skall att upptagningsbegreppet och det klargörande av detta som föreslagits i avsnitt 7.2 innebär att den föreslagna kriminaliseringen blir mer långtgående än vad artikel 4 förutsätter. Exempelvis kommer den att omfatta undertryckande av upptagningar som överförs i ledningsbundna nät. De skäl som anförts för att behålla och klargöra upptagningsbegreppet måste emellertid samtidigt anses utgöra skäl för att kriminaliseringen av undertryckande skall gälla samma skyddsobjekt.

Allvarligt hindrande av användningen av en upptagning

Enligt *artikel 3* skall det vara straffbart som olaglig systemstörning att uppsåtligt och orättmätigt avbryta eller allvarligt hindra driften av ett informationssystem. En sådan störning kan enligt artikeln ske genom inmatning eller överföring av datorbehandlingsbara uppgifter. En störning kan också ske t.ex. genom att sådana uppgifter hindras eller görs oåtkomliga. Systemstörningar är inte straffbelagda fullt ut i dag. Genom att undertryckande av upptagning kriminaliseras straffbeläggs dock en åtgärd som hindrar eller gör uppgifter oåtkomliga. För ansvar krävs då inte att undertryckandet medför ett avbrott eller annat allvarligt hindrande av ett systems drift. Denna ändring kan emellertid inte anses vara tillräcklig för att helt uppfylla kriminaliseringskravet i artikel 3. Exempelvis kan inmatningar av virusprogram eller överföringar av en stor mängd automatiskt genererade uppgifter medföra att en normal användning av upptagningar hindras utan att upptagningarna helt undertrycks.

Dataintrångsbestämmelsen måste alltså utvidgas för att den fullt ut skall motsvara artikeln. En utgångspunkt vid kriminaliseringen är att bestämmelsens uppsåtskrav och olovlighetsrekvisit skall behållas.

Det handlande som skall straffbeläggas bör anges vid sidan av den gärning som består i att undertrycka en upptagning, eftersom den gärningen i sig kan omfatta handlingar som medför systemstörningar.

Handlandet skall enligt artikel 3 bestå i att avbryta eller allvarligt hindra ett informationssystems drift, dvs. driften av apparater för databehandling och sådana uppgifter som finns i apparaterna för drift, användning, skydd och underhåll av dem. Dessa driftsstörningar innebär samtidigt att upptagningar för automatiserad databehandling som finns i informationssystem som störs inte kan användas på ett normalt sätt. Exempelvis överföringar eller införingar av automatiskt genererade meddelanden kan medföra att en myndighets datorer får kraftigt nedsatt funktion. Därmed hindras en normal användning av myndighetens upptagningar. Den kriminalisering som krävs för att systemstörningar fullt ut skall vara straffbelagda kan alltså åstadkommas genom att ett hindrande av användningen av en upptagning straffbeläggs. I den svenska straffbestämmelsen om sabotage är det på motsvarande sätt kriminaliserat att allvarligt hindra *användningen av* viss egendom. Som slagits fast i avsnitt 7.1 skall vidare upptagningar fortsatt vara skyddsobjekt i dataintrångsbestämmelsen. För övrigt kommer bestämmelsens andra delar att fånga upp större delen av de situationer som anges i artikel 3.

Vidare bör i enlighet med artikel 3 krävas att åtgärden *allvarligt* hindrar användningen av en upptagning. I detta ligger också att en åtgärd som avbryter, dvs. helt hindrar, användningen omfattas. Uttryckssättet motsvarar därmed helt rambeslutets ”avbryta eller allvarligt hindra”. I regel torde dock ansvar för undertryckande komma i fråga om användningen av en upptagning helt hindras.

Sammanfattningsvis föreslås att den som uppsåtligen och olovligen allvarligt hindrar användningen av en upptagning för automatiserad databehandling döms för dataintrång.

I sammanhanget skall anmärkas att upptagningsbegreppet och det förtydligande av detta som föreslås i avsnitt 7.2 innebär att den föreslagna kriminaliseringen kommer att sträcka sig längre

än vad som behövs enligt artikel 3. De skäl som angetts för att kriminaliseringen skall gälla upptagningar liksom de skäl som anförts för att klargöra begreppet måste dock anses innebära att kriminaliseringen är godtagbar.

Opinionsyttringar m.m.

En särskild fråga är hur kriminaliseringsförslagen förhåller sig till opinionsyttringar. Datorer används ibland som medel för att uttrycka åsikter i vissa frågor. Exempelvis kan flera personer enas om att ett visst klockslag en viss dag kontakta en särskild webbsida eller sända elektronisk post (e-post) till en viss adress.

Ytterligare en fråga är hur förslagen förhåller sig till den grundlagsfästa meddelarfriheten, dvs. skyddet för den som till redaktioner eller liknande lämnar uppgifter för offentliggörande i grundlagsskyddade medier.

Utgångspunkten är att det straffbara området enligt dataintrångsbestämmelsen inte skall träffa ett handlande som utgör en ren opinionsyttring. Med det menas här att någon sänder ett meddelande med visst åsiktsinnehåll till en mottagare i syfte att mottagaren skall ta del av innehållet och eventuellt låta sig påverkas av det. Att ett innehåll i sig kan vara straffbart, t.ex. som olaga hot, är en annan sak. Straffansvaret för dataintrång får inte heller omfatta fall där någon genom t.ex. e-post gör bruk av sin meddelarfrihet.

De föreslagna kriminaliseringarna förutsätter både att användningen av en upptagning allvarligt hindras eller att upptagningen undertrycks och att det föreligger uppsåt i förhållande till detta. Därmed faller rena opinionsyttringar utanför det straffbara området. Detsamma gäller fall där någon använder sig av sin meddelarfrihet.

Kriminaliseringen kan däremot träffa t.ex. en situation där en eller flera personer sänder e-post till en viss e-postadress i så stor omfattning att det stör mottagarens e-postsystem och därmed hindrar användningen av upptagningar i systemet. Att ett sådant handlande skall vara straffbelagt kan jämföras med att det t.ex. är

straffbart att genom fysiska angrepp skada ett företags datorer i syfte att uttrycka missnöje med företagets policy i en viss fråga. Därigenom hindras användningen av upptagningar i datorerna. För straffansvar för en störning av det nämnda slaget i exemplet förutsätts dock att den enskilde kan anses uppsåtligen själv eller tillsammans med de andra ha allvarligt hindrat användningen av upptagningen. På grund av detta kvalificerade krav och uppsåtskravet torde vissa situationer som i och för sig inte kan betraktas som rena opinionsyttringar komma att falla utanför det straffbara området. Ett alternativ för att undvika att sådana fall blir straffria skulle kunna vara att slopa kravet på att hindrandet skall vara allvarligt. Det skulle dock innebära en mer långtgående kriminalisering än vad rambeslutet kräver. Dessutom framstår behovet av en så vidsträckt kriminalisering som tveksamt.

Sammanfattningsvis omfattar den föreslagna kriminaliseringen inte rena opinionsyttringar. Den kommer inte heller i konflikt med meddelarfriheten.

7.4 Anstiftan, medhjälp och försök m.m.

Bedömning: Genom att de gärningar som omfattas av kriminaliseringsförslagen i det föregående avsnittet straffbeläggs blir brottsbalkens generella bestämmelser om medverkan och bestämmelsen om försök till dataintrång tillämpliga på anstiftan av, medhjälp till och försök till gärningarna. Det krävs därför inte några särskilda lagstiftningsåtgärder för att straffbelägga medverkan och försök till gärningarna.

Skälen för bedömningen: Enligt *artikel 5* skall anstiftan av och medhjälp till olagligt intrång, olaglig systemstörning och olaglig datastörning vara straffbelagt. Dessutom skall försök till huvudbrotten vara straffbart. Försök till olagligt intrång behöver dock inte kriminaliseras. Dessutom behöver ringa fall av fullbordade brott inte heller kriminaliseras.

I avsnitt 6.2.5 har konstaterats att svensk rätt uppfyller artikelns krav om kriminalisering av anstiftan, medhjälp och försök i

fråga om de gärningar som skall vara straffbelagda enligt rambeslutet och som täcks av straffbestämmelserna om dataintrång, skadegörelse, grov skadegörelse, sabotage och grovt sabotage.

Genom att de gärningar som omfattas av kriminaliseringsförslagen i det föregående avsnittet straffbeläggs blir brottsbalkens generella bestämmelser om medverkan tillämpliga på anstiftan av och medhjälp till gärningarna. Därmed uppfylls fullt ut kravet i artikel 5 att anstiftan av och medhjälp till brotten enligt rambeslutet skall vara straffbelagt.

De föreslagna kriminaliseringarna medför vidare att gällande straffbestämmelse om försök till dataintrång blir tillämplig. Det krävs alltså inte någon särskild lagstiftningsåtgärd för att straffbelägga försök till de gärningar som nykriminaliseras. Åtagandet i artikel 5 att straffbelägga försök till brotten enligt rambeslutet får därigenom motsvarighet i svensk rätt. Det gäller dock inte ringa fall, som i dag är undantagna från den svenska försökskriminaliseringen. Undantaget måste emellertid anses förenligt med rambeslutet. I denna fråga hänvisas till vad som sagts i avsnitt 6.2.5. Rambeslutets krav att försök skall vara kriminaliserat uppfylls följaktligen fullt ut.

Nykriminaliseringarna innebär att bestämmelsen om förberedelse till dataintrång blir tillämplig på de nya straffbara gärningarna. Förberedelse till dataintrång är straffbart förutsatt att brottet inte skulle ha varit att anse som ringa om det fullbordats. En sådan utvidgning av det straffbara området är inte påkallad av rambeslutet. Emellertid måste förberedelse till de gärningar som nu föreslås kriminaliserade anses lika straffvärda som de fall av förberedelse till dataintrång som redan är straffbelagda. Utvidgningen får därför anses motiverad.

8 Ikraftträdande

Förslag: Ändringarna i dataintrångsbestämmelsen träder i kraft den 1 januari 2007.

Skälen för förslaget: Enligt *artikel 12* skall medlemsstaterna vidta de åtgärder som är nödvändiga för att följa bestämmelserna i rambeslutet senast två år efter det att rambeslutet har trätt i kraft. Rambeslutet har ännu inte trätt i kraft men kan förutsättas komma att antas inom en nära framtid. De föreslagna ändringarna i dataintrångsbestämmelsen föreslås därför träda i kraft den 1 januari 2007.

Några särskilda övergångsbestämmelser är inte nödvändiga. Av 5 § brottsbalkens promulgationslag följer att nykriminaliseringarna i dataintrångsbestämmelsen inte får tillämpas på ett sådant sätt att de ges retroaktiv verkan.

9 Kostnader

För att fullt ut uppfylla rambeslutet om angrepp mot informationssystem föreslås vissa utvidgningar av bestämmelsen om dataintrång. Utvidgningarna innebär samtidigt att gällande bestämmelser om försök och förberedelse samt medverkan till brotten blir tillämpliga. Dessutom föreslås att dataintrångsbestämmelsen klargörs i ett avseende och samtidigt moderniseras språkligt sett.

Utvidgningarna av det straffbara området är av begränsad omfattning. De övriga ändringarna påverkar i princip inte det straffbelagda området.

Antalet ärenden och mål om dataintrång hos polis, åklagare och domstolar är i dag förhållandevis begränsat. År 2003 uppgick antalet polisanmälda dataintrång till drygt 700. Enligt preliminära siffror är antalet detsamma för 2004. Under åren 2000–2002 varierade antalet mellan 341 och 407. Utvidgningen av straffansvaret för dataintrång kan inte i sig antas leda till någon påtagligt ökad tillströmning av ärenden eller mål hos de brottsbekämpande myndigheterna. Inte heller kriminalvården kan antas drabbas av någon märkbar kostnadsökning.

Enligt rambeslutet skall det ske ett informationsutbyte i fråga om de brott som omfattas av rambeslutet. Utbytet skall ske inom ramen för ett redan befintligt nät för utbyte av uppgifter om högteknologisk brottslighet och i de former som gäller i dag. I Sverige är detta en uppgift för polisen. Åtagandet kan antas innebära en begränsad ökad arbetsbelastning.

Sammantaget görs bedömningen att genomförandet av rambeslutet torde medföra endast marginella kostnadsökningar för

rättsväsendet. Eventuella merkostnader skall därför finansieras inom befintliga anslag.

10 Författningskommentar

Förslaget till lag om ändring i brottsbalken

4 kap.

9 c §

Paragrafen har delats in i två stycken. Brottsbeskrivningarna finns i första stycket. I andra stycket jämställs vissa uppgifter med en upptagning enligt första stycket.

Bestämmelsen är fortfarande subsidiär i förhållande till bestämmelserna i 4 kap. 8 och 9 §§ brottsbalken om brytande av post- eller telehemlighet och intrång i förvar. Som tidigare gällt får förhållandet mellan dataintrång och övriga brottsbalksbrott avgöras enligt sedvanliga principer för bedömningen av konkurrens mellan överlappande straffstadganden i brottsbalken.

I *första stycket* är den första meningen oförändrad i sak. Meningen har moderniserats språkligt bl.a. genom att begreppet *automatiserad* databehandling används.

Av den nya andra meningen följer att den som undertrycker eller på annat sätt allvarligt hindrar användningen av en sådan upptagning som avses i första meningen döms för dataintrång till böter eller fängelse i högst två år. På samma sätt som gäller handlingarna i första meningen avses inte fysiska angrepp.

En förutsättning för straffansvar är att gärningen begås olovligen. Sedvanliga åtgärder som att testa säkerheten hos system eller att installera nya program, som vidtas av behöriga personer i enlighet med behörigheten, kan inte anses vara olovliga. För straffansvar krävs vidare uppsåt.

Det handlande som straffbeläggs är för det första att undertrycka en upptagning för automatiserad databehandling. Med det avses att upptagningen görs oåtkomlig eller att flödet av uppgifterna hindras. Undertryckandet kan ske genom användning av sabotageprogram eller en upptagning. Om upptagningen förändras eller förstörs, kan ansvar i stället komma i fråga för ändring eller utplånande av upptagningen.

Dessutom straffbeläggs att på annat sätt allvarligt hindra användningen av en upptagning för automatiserad databehandling. Kriminaliseringen omfattar sådana åtgärder som inte kan anses undertrycka en upptagning men som ändå påverkar användningen av upptagningen. Exempelvis kan införingar av virusprogram i en dator och överföringar av automatiskt genererade meddelanden till en dator eller datorsystem medföra att en upptagning i datorn eller systemet inte kan användas på ett normalt sätt. Det bör inte krävas att den som rätteligen förfogar över upptagningen hindras i sin användning i en konkret situation. Med uttrycket ”allvarligt hindra” avses att det skall vara fråga om en betydande störning av inte endast tillfällig natur. I det fallet användningen helt förhindras kan ansvar inträda för undertryckande av upptagning. Om en störning orsakas av flera personer, krävs att den enskilde har uppsåt till störningen för att ansvar skall komma i fråga.

Utanför det straffbara området faller rena opinionsyttringar som innebär att meddelanden med visst åsiktsinnehåll sänds, t.ex. med elektronisk post, till en mottagare för att denne skall ta del av innehållet och eventuellt låta sig påverkas av detta, Kriminaliseringen träffar inte heller fall där någon genom t.ex. elektronisk post gör bruk av sin grundlagsfästa meddelarfrihet. Detsamma gäller reklam i elektronisk post, som regleras i marknadsföringslagen (1995:450). Däremot omfattar kriminaliseringen fall där de handlingar som beskrivs i andra meningen uppsåtligen och olovligen begås just för att väcka opinion eller uttrycka missnöje.

Försök och förberedelse är straffbart enligt 4 kap. 10 § brottsbalken. Vidare är medverkan straffbelagt enligt bestämmelserna i 23 kap. brottsbalken.

Ändringarna har behandlats i avsnitt 7.3.

I *andra stycket* jämställs med upptagning enligt första stycket uppgifter som befordras via elektromagnetiska vågor och som är avsedda för automatiserad databehandling. Genom ändringarna klargörs att dataintrångsbestämmelsen omfattar alla uppgifter som befordras. Bestämmelsen i denna del har dessutom moderniserats språkligt.

Stycket innebär att de uppgifter som anges omfattas av brottsbeskrivningarna i första stycket. Exempelvis omfattas uppgifter som befordras via radio oavsett om uppgifterna har fixerats på datamedium eller inte. När det gäller sådana uppgifter kan kravet på olovlighet utesluta ansvar i enlighet med principen om att etern är fri. Huruvida olovlighetskravet i detta avseende är uppfyllt eller inte får övervägas i varje enskilt fall med hänsyn till samtliga omständigheter i det särskilda fallet. Frågan torde främst vara intressant i intrångssituationer.

Ändringarna i andra stycket har behandlats i avsnitt 7.2.

Rambeslutet om angrepp mot informationssystem

RÅDETS RAMBESLUT 2005/…/RIF

av den

om angrepp mot informationssystem

EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA RAMBESLUT

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

med beaktande av kommissionens förslag,

med beaktande av Europaparlamentets yttrande[1], 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.

[1] EUT C 300 E, 11.12.2003, s.26.

(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 28 januari 2002 om en gemensam inställning och särskilda åtgärder på området för nät och informationssäkerhet[2].

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

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

[2] EGT C 43, 16.2.2002, s. 2.
[3] EGT C 19, 23.1.1999, s. 1.

rådet i Santa Maria da Feira den 19–20 juni 2000, kommissionen i "resultattavlan" och Europaparlamentet i sin resolution av den 19 maj 2000 anger eller uppmanar till lagstiftningsåtgärder mot högteknologisk brottslighet, inklusive gemensamma definitioner, kriminaliseringar och påföljder.

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

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

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

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

(11) Det finns ett behov av att fastställa en gemensam inställning i fråga om brottsrekvisit, genom att gemensamt kriminalisera

olagligt intrång i informationssystem, olaglig systemstörning och olaglig datastörning.

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

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

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

(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].

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

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Definitioner

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

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

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

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

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

Artikel 2

Olagligt intrång i informationssystem

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

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

Artikel 3

Olaglig systemstörning

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

när gärningen utförs orättmätigt, åtminstone i fall som inte är ringa.

Artikel 4

Olaglig datastörning

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

Artikel 5

Anstiftan, medhjälp och försök

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

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

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

Artikel 6

Påföljder

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

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

Artikel 7

Försvårande omständigheter

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

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

Artikel 8

Juridiska personers ansvar

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

a) befogenhet att företräda den juridiska personen, eller

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

c) befogenhet att utöva kontroll inom den juridiska personen.

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

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

Artikel 9

Påföljder för juridiska personer

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

a) fråntagande av rätt till offentliga förmåner eller stöd,

b) tillfälligt eller permanent näringsförbud,

c) rättslig övervakning, eller

d) rättsligt beslut om upplösning av verksamheten.

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

lighet med artikel 8.2 kan bli föremål för effektiva, proportionella och avskräckande påföljder eller åtgärder.

Artikel 10

Behörighet

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

a) helt eller delvis på dess territorium, eller

b) av en av dess medborgare, eller

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

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

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

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

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

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

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

– Medlemsstaten skall vara den i vilken gärningsmannen är medborgare.

– Medlemsstaten skall vara den på vars territorium gärningsmannen påträffats.

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

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

Artikel 11

Utbyte av uppgifter

1. För utbyte av uppgifter om de brott som avses i artiklarna 2, 3, 4 och 5 skall medlemsstaterna, med iakttagande av bestämmelser

om dataskydd, säkerställa att de använder det befintliga nät med operativa kontaktpunkter som kan nås dygnet runt alla dagar i veckan.

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

Artikel 12

Genomförande

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

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

---

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

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

Uttalande från kommissionen

Uttalande till rådets protokoll vid antagande av rambeslutet

Uttalande från kommissionen

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