Regeringens proposition 2006/07:66

Angrepp mot informationssystem

Prop. 2006/07:66

Regeringen överlämnar denna proposition till riksdagen.

Stockholm den 8 mars 2007

Maud Olofsson

Beatrice Ask
(Justitiedepartementet)

Propositionens huvudsakliga innehåll

I propositionen 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, domsrätt och utbyte av uppgifter.

För att Sverige fullt ut skall uppfylla åtagandena enligt rambeslutet krävs ett utvidgat straffansvar i förhållande till gällande rätt på området. Utvidgningen föreslås ske i bestämmelsen om dataintrång i brottsbalken.

Dataintrångsbestämmelsen utvidgas till att omfatta dels den som olovligen blockerar en uppgift som är avsedd för automatiserad behandling, dels den som olovligen allvarligt stör eller hindrar användningen av en sådan uppgift. Även försök och förberedelse till sådana brott straffbeläggs. Medverkan till sådana brott blir också straffbart. Kriminaliseringen innebär exempelvis att s.k. tillgänglighetsattacker blir straffbara.

Vidare förtydligas dataintrångsbestämmelsen och moderniseras språkligt genom att uttrycket ”uppgift som är avsedd för automatiserad behandling” ersätter det tidigare använda upptagningsbegreppet.

I propositionen 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 Rikspolisstyrelsen som svensk kontaktpunkt för utbyte av uppgifter om brotten enligt rambeslutet.

Ändringarna föreslås träda i kraft den 1 juni 2007.

Innehållsförteckning

1 Förslag till riksdagsbeslut

Regeringen föreslår att riksdagen antar regeringens förslag till lag om ändring i brottsbalken.

2 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 uppgift som är avsedd för automatiserad behandling* eller olovligen ändrar*,* utplånar*, blockerar* eller i register för in *en* sådan *uppgift* döms för *dataintrång* till böter eller fängelse i högst två år. *Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift.*

Denna lag träder i kraft den 1 juni 2007.

[1] Senaste lydelse 1998:206.

3 Ärendet och dess beredning

Våren 2002 presenterade Europeiska kommissionen ett förslag till rambeslut om angrepp mot informationssystem (EGT C 203 E, 27.8.2002, s. 109). Syftet med förslaget var att tillnärma medlemsstaternas lagstiftning på området angrepp mot informationssystem. En faktapromemoria upprättades inom Regeringskansliet och överlämnades till riksdagen (2001/02:FPM110).

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

Vid rådet för rättsliga och inrikes frågor den 27–28 februari 2003 nåddes en politisk överenskommelse om innehållet i rambeslutet.

Vid Europeiska rådets möte den 25–26 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). Efter att samtliga parlamentsförbehåll hävts antogs rambeslutet den 24 februari 2005. I samband med antagandet gjorde kommissionen ett uttalande som togs till rådets protokoll. Medlemsstaterna skall genomföra bestämmelserna i rambeslutet senast den 16 mars 2007.

Rambeslutet i svensk version är fogat till denna proposition som *bilaga 1*. Kommissions uttalande finns i *bilaga 2*.

Inom Justitiedepartementet har upprättats en departementspromemoria, Angrepp mot informationssystem (Ds 2005:5). En sammanfattning av promemorian finns i *bilaga 3*. Promemorians författningsförslag finns i *bilaga 4*.

Promemorian har remissbehandlats och en förteckning över remissinstanserna finns i *bilaga 5*. En sammanställning av remissyttrandena finns tillgänglig i Justitiedepartementet (dnr Ju2005/2433/L5).

Lagrådet

Regeringen beslutade den 15 februari 2007 att inhämta Lagrådets yttrande. Lagrådsremissens förslag stämmer överens med propositionens. Lagrådet har lämnat förslaget utan erinran. Yttrandet finns i *bilaga 6*.

4 Bakgrund och allmänna utgångspunkter

4.1 Angrepp mot informationssystem

Dagens samhälle präglas av att informationsteknik genomsyrar i stort sett alla sektorer. Det innebär samtidigt att samhället är sårbart för olika former av angrepp som riktar sig mot tekniken, såsom olovliga intrång i informationssystem samt 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. Vissa program orsakar skador på innehållet (information och program) i själva datorn medan andra i stället utnyttjar datorn och dess innehåll 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 trojaner. 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. Upprepade anrop eller försök till anrop kan avbryta eller allvarligt hindra driften hos ett informationssystem. Detsamma kan gälla program som sänder stora mängder elektronisk post (e-post) eller manuella sändningar i stor skala av sådan post. Andra typer av attacker innefattar t.ex. störningar av servrar som hanterar domännamnssystemet eller andra grundläggande system.

Det förekommer också kombinationer av de nu nämnda formerna av attacker. Som exempel kan nämnas datavirus som sprids i bilagor till e-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 datavirus och datamaskar som spritt sig, ofta snabbt, 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 t.ex. Internetleverantörer. Det finns en risk för att också t.ex. industrin, sjukvården eller myndigheter utsätts för allvarliga tillgänglighetsattacker över allmänt tillgängliga 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. 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 samhällets centrala infrastruktur. Hur omfattande och allvarlig brottsligheten är i Sverige i dag kan inte med säkerhet sägas. Att brottsligheten måste tas på allvar är dock uppenbart.

4.2 Något om det internationella arbetet

4.2.1 Arbete inom Europeiska unionen

Den 3 december 1998 antogs i Wien en handlingsplan för att på bästa sätt genomföra bestämmelserna i Amsterdamfördraget om upprättandet av ett område med frihet, säkerhet och rättvisa. I handlingsplanen angavs 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 15–16 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 19–20 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 2001 (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. Under delar av 2002 och 2003 framförhandlades innehållet i rambeslutet om angrepp mot informationssystem. Vid rådet för rättsliga och inrikes frågor den 27–28 februari 2003 nåddes en politisk överenskommelse om innehållet i rambeslutet. Det antogs sedan den 24 februari 2005. Rambeslutet behandlas närmare i avsnitt 5.

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 hand-

lingar 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.

EG:s direktiv om lagring av trafikuppgifter

Efter bombattentaten i Madrid i mars 2004 fick rådet för rättsliga och inrikes frågor i uppdrag av Europeiska rådet att snarast anta gemensamma åtgärder om lagring av trafikuppgifter. Ett antal länder, däribland Sverige, utarbetade ett förslag som presenterades under sommaren 2004 och som förhandlades under 2004 och 2005. Europaparlamentet och rådet antog den 15 mars 2006 direktiv 2006/24/EG om lagring av trafikuppgifter.

Direktivet reglerar en skyldighet för medlemsstaterna att se till att leverantörer av vissa tjänster (fast och mobil telefoni) och Internet (Internetåtkomst, e-post och Internettelefoni) eller leverantörer av de kommunikationsnät som nämnda tjänster använder, lagrar vissa trafikuppgifter som uppkommer i samband med kommunikationen. Tanken är att se till att trafikuppgifter skall finnas tillgängliga och kunna lämnas ut till de brottsbekämpande myndigheterna för att de skall kunna avslöja, utreda, och åtala för allvarlig brottslighet. Direktivet skall vara genomfört i nationell lagstiftning senast den 15 september 2007 avseende de delar som gäller fast och mobil telefoni och senast den 15 mars 2009 avseende de delar som gäller Internet. I maj 2006 tillsatte den dåvarande regeringen en särskild utredare för genomförandet av direktivet i svensk rätt (dir. 2006:49).

Haagprogrammet m.m.

Europeiska rådet antog den 4–5 november 2004 ett nytt femårigt arbetsprogram för stärkt frihet, säkerhet och rättvisa – det s.k. Haagprogrammet. Programmet, som ersätter det tidigare Tammerforsprogrammet, syftar till att förbättra unionens och dess medlemsstaters gemensamma kapacitet bl.a. när det gäller att bekämpa organiserad gränsöverskridande brottslighet och hålla tillbaka terroristhotet. En handlingsplan för genomförandet av Haagprogrammet antogs av Europeiska rådet den 16–17 juni 2005. Handlingsplanen innefattar bl.a. åtgärder för att förbättra informationsutbytet mellan brottsbekämpande myndigheter, se föregående avsnitt. Vidare berörs också åtgärder för bättre förebyggande av organiserad brottslighet, däribland meddelande om IT-brottslighet och åtgärder för IT-säkerhet.

Under 2006 offentliggjorde kommissionen dels ett meddelande med titeln ”En strategi för ett säkert informationssamhälle” (KOM [2006] 251 slutlig), dels ett meddelande om översynen av EU:s regelverk för elektroniska kommunikationsnät och kommunikationstjänster (KOM [2006] 334 slutlig). I det senare föreslogs nya bestämmelser för att stärka säker-

het och personlig integritet inom området för elektronisk kommunikation. I ett meddelande den 15 november 2006 om skräppost, spionprogram och sabotageprogram (KOM [2006] 688 slutlig) angav kommissionen bl.a. att den i början av 2007 avser att lägga fram en strategi om nätbrottslighet.

I sammanhanget kan även nämnas att inom EU inrättades 2004 Europeiska byrån för nät- och informationssäkerhet (European Network and Information Security Agency, Enisa). Byrån är ett expert- och kompetenscentrum för informationssäkerhetsfrågor med uppgift att öka medlemsstaternas förmåga att förebygga, åtgärda och lösa problem som rör nät- och informationssäkerhet.

4.2.2 Arbete inom Europarådet – 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 EU:s rambeslut 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 bör ratificera konventionen och protokollet behandlas i departementspromemorian Brott och brottsutredning i IT-miljö (Ds 2005:6). I promemorian föreslås att Sverige skall ratificera konventionen och tilläggsprotokollet till denna. Vidare läggs i promemorian fram de förslag till lagändringar som krävs för en anpassning av svensk rätt till konventionen. I fråga om åtagandena enligt konventionen att kriminalisera olagligt intrång i datorsystem, datastörning och störning av datorsystem framhålls i promemorian att dessa kommer att uppfyllas om de förändringar som föreslås i departementspromemorian Angrepp mot informationssystem (Ds 2005:5), som legat till grund för denna proposition, genomförs. I promemorian om konventionen behandlas därför bara de ytterligare förändringar som krävs för att genomföra konventionen. Bland annat föreslås att tillämpningsområdet för dataintrång skall utvidgas till att omfatta även olovlig avlyssning av datorer. Promemorian har remitterats och är föremål för beredning inom Justitiedepartementet.

Frågan om genomförandet av rambeslutet bör samordnas med frågan om ett genomförande av konventionen berörs under avsnitt 7.1.

5 EU:s rambeslut om angrepp mot informationssystem

5.1 Rambeslutets syfte och innehåll

Rambeslutet syftar till att närma medlemsstaternas straffrättsliga lagstiftning till varandra 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.

5.2 Ingressen

I ingressen till rambeslutet anges att rambeslutet antagits 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, samt att det finns 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.

5.3 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.

5.4 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.

5.5 Artikel 3 Olaglig systemstörning

Enligt *artikel 3* skall medlemsstaterna kriminalisera visst handlande som utgör 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.

5.6 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.

5.7 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.

5.8 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.

5.9 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.

5.10 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 den juridiska personen. 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.

5.11 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 medlemsstaterna anlita de organ eller mekanismer som inrättats inom Europeiska unionen för att underlätta samarbetet mellan deras rättsliga myndigheter och samordningen av deras verksamhet. Följande omständigheter får beaktas i successiv ordning.
– Medlemsstaten skall vara den inom vars territorium brottet har begåtts enligt punkt 1 a och punkt 2.
– Medlemsstaten skall vara den i vilken gärningsmannen är medborgare.
– Medlemsstaten skall vara den på vars territorium gärningsmannen påträffats.

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

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

5.12 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.

5.13 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 vidta nödvändiga åtgärder för att följa bestämmelserna i rambeslutet senast den 16 mars 2007.

Enligt *punkt 2* skall medlemsstaterna senast vid samma tidpunkt till rådets generalsekretariat och kommissionen överlämna texten till bestämmelser genom vilka skyldigheterna enligt rambeslutet införlivas med deras nationella lagstiftning. Senast den 16 september 2007 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 rambeslutet.

5.14 Artikel 13 Ikraftträdande

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

5.15 Uttalande

I samband med antagandet av rambeslutet gjorde kommissionen ett uttalande, som togs till rådets protokoll. I uttalandet beklagar kommissionen att det i artikel 6 punkt 2 om påföljder inte föreskrivs ett minimistraff för olagligt intrång enligt artikel 2.

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 motsvarar 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

Bestämmelsen om dataintrång infördes i brottsbalken 1998 (4 kap. 9 c §) i samband med att den tidigare datalagen (1973:289) ersattes med personuppgiftslagen (1998:204). Datalagens bestämmelse om dataintrång (21 §) överfördes då till brottsbalken utan ändring i sak. Datalagen hade tillkommit samtidigt som vissa ändringar gjorts i tryckfrihetsförordningens bestämmelser om allmänna handlingars offentlighet.

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.

Det objekt som skyddas i bestämmelsen anges med begreppet upptagning för automatisk databehandling. Med detta skall enligt förarbetena förstås uppgift som är fixerad på någon form av datamedium och som alltså antingen finns i eller kan matas in i en datamaskin. Vidare ligger i begreppet att informationen är läsbar endast med ADB-teknik (prop. 1973:33 s. 75). Till upptagningsbegreppet måste även datorprogram av olika slag räknas (jfr t.ex. SOU 1992:110 s. 110 och SOU 2005:38 s. 144 samt prop. 1975/76:160 s. 120–121). Sedan en lagändring 1986 anges i dataintrångsbestämmelsen att med upptagning avses också uppgifter som är under befordran via ett elektroniskt eller liknande hjälpmedel för att användas för automatisk databehandling. Genom tillägget gjordes bestämmelsen uttryckligen tillämplig på information som förs över till en dator, även om uppgifterna ännu inte kan anses ha fixerats på ett datamedium (prop. 1985/86:65 s. 30 ff. och 48).

Ansvar för dataintrång förutsätter uppsåt (1 kap. 2 § brottsbalken). För straffansvar krävs vidare att gärningen utförs olovligen. Härmed utesluts från det straffbara området sådant förfarande som sker med samtycke av den som har rätt att förfoga över upptagningen eller i överensstämmelse med gällande rätt, t.ex. regler om tvångsmedel (jfr Holmqvist m.fl., Brottsbalken En kommentar Kap. 1–12, s. 4:36).

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

Vidare straffbeläggs att ändra eller utplåna en upptagning för automatisk databehandling. 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, t.ex. genom radering.

Slutligen är det också straffbelagt som dataintrång att föra in en upptagning för automatisk databehandling i ett register. Denna del av bestämmelsen tillkom efter påpekande av Justitiekanslern under remissbehandlingen av det betänkande som låg till grund för propositionen om datalagen (SOU 1972:47). Justitiekanslern ansåg att tolkningen av betänkandets förslag kunde bli föremål för tvekan med hänsyn till att ingenting sades om obehöriga införingar (prop. 1973:33 s. 68). Någon närmare diskussion om kriminaliseringens innebörd i denna del fördes inte i propositionen.

Införingar av upptagningar i register är alltså straffbelagda. Registerbegreppet medför en begränsning av det straffbara området så till vida att endast sådana införingar som sker i uppgifter strukturerade på visst sätt omfattas. Således omfattar tillämpningsområdet för dataintrångsbestämmelsen i denna del inte alla slag av införingar av upptagningar. Andra införingar kan dock vara straffbara genom att de träffas av de delar av bestämmelsen 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. 4:34–4:35). Ett telemeddelande kan förmed-

las t.ex. 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 anses utesluta 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 gällande rätt, 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 fysiska medel. Enligt normalt språkbruk främjas en gärning när någon har gjort något som underlättar eller i vart fall är ägnat att underlätta gärningens utförande. I 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 vid alla brottsbalksbrott samt de brott i specialstraffrätten för vilka fängelse är föreskrivet eller för vilka särskild föreskrift finns att medverkan skall bestraffas. Bestämmelserna gäller inte, om något annat följer av vad för särskilda fall 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 på viss tid, lägst två 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 särskilt 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 (29 kap. 2 § 6).

6.1.7 Ansvar och påföljder för juridiska personer

I brottsbalken (36 kap. 7–10 a §§) finns bestämmelser om att i vissa fall ålägga näringsidkare företagsbot. Genom ändringar som trätt i kraft den

1 juli 2006 har möjligheterna att ålägga sådan bot utökats (prop. 2005/06:59, bet. 2005/06:JuU13, rskr. 2005/06:169).

För att kunna ålägga någon företagsbot förutsätts dels att brottet har begåtts i utövningen av näringsverksamhet, dels att det för brottet är föreskrivet strängare straff än penningböter. Dessutom förutsätts att näringsidkaren inte har gjort vad som skäligen kunnat krävas för att förebygga brottsligheten eller att brottet har begåtts av en person i ledande ställning grundad på befogenhet att företräda näringsidkaren eller att fatta beslut på dennes vägnar eller av en person som annars haft ett särskilt ansvar för tillsyn eller kontroll i verksamheten. Företagsbot skall dock inte åläggas i anledning av brottslighet som varit riktad mot näringsidkaren.

Företagsbot skall fastställas till lägst fem tusen kronor och högst tio miljoner kronor. När storleken av boten fastställs skall med beaktande av straffskalan för brottet särskild hänsyn tas till den skada eller fara som brottsligheten inneburit samt till brottslighetens omfattning och förhållande till näringsverksamheten. Skälig hänsyn skall också tas till om näringsidkaren tidigare ålagts att betala företagsbot. 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 som huvudregel att gärningen inte är fri från ansvar enligt lagen på gärningsorten. Strängare påföljd än den som är möjlig enligt lagen på gärningsorten får inte heller dömas ut. 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 för 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, som bygger på ett rambeslut, får överlämnande till en EU-stat av en person som eftersöks för lagföring inte vägras enbart på den grunden att personen är medborgare i den anmodade staten.

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.

I avsnitt 6.1.2–6.1.4 har lämnats en redogörelse för gällande svenska straffbestämmelser, däribland dataintrångsbestämmelsen. 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. Dessutom är syftet med bestämmelserna i båda fallen att ytterst ge ett skydd för automatiserad behandling. Vad däremot gäller de i och för sig i förhållande till dataintrångsbestämmelsen primära bestämmelserna om brytande av post- eller telehemlighet och intrång i förvar, har dessa som främsta syfte att skydda post, telegram och andra meddelanden. Vidare omfattar bestämmelsen om brytande av post- eller telehemlighet endast meddelanden som är under pågående befordran och som befordras mellan en avsändare och en mottagare. Rambeslutets bestämmelser förutsätter emellertid inte att de uppgifter som avses skyddas skall vara avsedda för någon annan än den som står bakom dem. Rambeslutet torde dessutom inte omfatta uppgifter under befordran i nät, jfr avsnitt 6.2.2–6.2.4.

Sammantaget finner regeringen därför att det ligger närmast till hands att utgå direkt från dataintrångsbestämmelsen i analysen av hur svensk straffrätt förhåller sig till rambeslutets krav på straffbara handlingar. Dataintrångsbestämmelsen kommer alltså att tas till utgångspunkt i bedömningen av behovet av lagändringar såvitt avser kriminaliseringsåtagandena.

6.2.2 Olagligt intrång i informationssystem

Regeringens bedömning: Svensk rätt uppfyller genom dataintrångsbestämmelsen rambeslutets krav på vad som skall vara straffbelagt som olagligt intrång i informationssystem.

Promemorians bedömning överensstämmer med regeringens bedömning.

Remissinstanserna: Majoriteten av remissinstanserna har inte haft något att erinra mot promemorians bedömning. Några remissinstanser, *Åklagarmyndigheten* och *Rikspolisstyrelsen*, har invänt mot begreppet upptagning för automatisk databehandling och menat att begreppet är för snävt för att i alla delar svara mot de åtaganden som följer av rambeslutet när det gäller vad som skall vara straffbelagt enligt artikel 2 som olagligt intrång i informationssystem. Myndigheterna har närmare bestämt anfört att uppgifter som enbart finns i ett temporärt minne, t.ex. arbetsminnet i en dator, inte omfattas av begreppet men däremot av rambeslutet. Också *Säkerhetspolisen* har uttryckt tveksamhet om sådana uppgifter skyddas av dataintrångsbestämmelsen.

Skälen för regeringens bedömning: 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 bl.a. uppsåtlig olovlig tillgång till upptagning för automatisk databehandling.

Såväl artikel 2 som dataintrångsbestämmelsen förutsätter alltså 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 och innebär i förhållande till artikel 2 intrång som sker utan tillstånd av ägaren eller annan rättighetshavare till systemet eller del av systemet eller som inte medges i nationell lagstiftning. Kravet på orättmätighet innebär alltså att handlingar som i och för sig uppfyller övriga krav för straffbarhet men som utförs antingen av eller med tillstånd från ägare eller annars behöriga personer i t.ex. ett företag i enlighet med behörigheten eller med stöd i gällande rätt inte omfattas av det område som skall vara straffbelagt. Denna innebörd av begreppet får anses motsvaras av vad som enligt dataintrångsbestämmelsen måste förstås med begreppet olovlig (se avsnitt 6.1.2).

Enligt artikel 2 skall handlingen bestå i ett intrång i ett informationssystem. I artikel 1 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. Det senare innebär alltså att endast sådana datorbehandlingsbara uppgifter som är att anse som nödvändiga för att systemet skall kunna fungera omfattas. En fråga i sammanhanget är om uppgifterna skall finnas i apparaterna eller om artikeln också omfattar intrång i sådana uppgifter när de befordras i nät. Definitionen av informationssystem omnämner inte särskilt nät. I kommissionens ursprungliga förslag till rambeslut ingick däremot nät i definitionen. Den avsåg då uppgifter som lagras, behandlas, hämtas eller överförs med hjälp av *datorer eller nät* för att *dessa* skall kunna drivas etc. Frågan om nät skulle omfattas av begreppet informationssystem var föremål för diskussioner under förhandlingarna om rambeslutet. Bland annat hävdades från vissa medlemsstater att det straffbara området skulle kunna bli alltför långtgående om nät inkluderades. Slutligen enades medlemsstaterna 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. Mot den nu beskrivna bakgrunden måste rambeslutets begrepp informationssystem förstås så att det inte omfattar uppgifter som befordras i nät. Artikel 2 avser därmed intrång i apparater för automatisk databehandling och i uppgifter som finns i sådana apparater för drift, användning, skydd och underhåll av dessa.

Dataintrångsbestämmelsen straffbelägger bl.a. den som bereder sig tillgång till upptagning för automatisk databehandling. Som framgått skall med sådan upptagning förstås uppgifter, information eller program av olika slag, som är fixerade på någon form av datamedium och alltså antingen finns i eller kan matas in i en datamaskin eller som är under

befordran på sätt som närmare anges i bestämmelsen. För straffansvar är det 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 i en apparat som används för uppgifter av nämnt slag. Genom tillträdet till apparaten har personen skaffat sig möjlighet att ta del av de uppgifter som finns i apparaten och alltså berett sig tillgång till dessa. Dataintrångsbestämmelsens kriminalisering måste följaktligen anses täcka det som enligt artikel 2 skall vara straffbart som intrång i apparater för automatisk behandling och uppgifter för drift, användning, skydd och underhåll av dessa. Majoriteten av remissinstanserna har instämt i eller inte haft något att erinra mot denna bedömning.

Några remissinstanser, bl.a. *Åklagarmyndigheten* och *Rikspolisstyrelsen*, har dock invänt att begreppet upptagning för automatisk databehandling inte fullt ut motsvarar rambeslutets begrepp informationssystem så till vida att upptagningsbegreppet inte omfattar uppgifter som enbart finns i ett temporärt minne, t.ex. arbetsminnet i en dator, eftersom sådana uppgifter inte är att anse som lagrade eller fixerade och inte heller är under befordran. Regeringen vill i denna del framföra följande. Straffbestämmelsen om dataintrång har tillkommit för att generellt skydda datalagrat material från obehöriga åtgärder. Som framgått skall med sådant material förstås bl.a. uppgift som har fixerats på någon form av datamedium och som alltså antingen finns i eller kan matas in i en datamaskin. Det finns inget i förarbetena som tyder på att avsikten varit att avgränsa upptagningsbegreppet så att endast uppgifter på datamedier av viss karaktär omfattas. Tvärtom framgår att lagstiftaren inte framhållit datamedierna eller minnena som sådana som avgörande för vad som skall anses utgöra en upptagning utan i stället fokuserat på själva informationsinnehållet, dvs. den uppgift som har fixerats på det tekniska mediet (prop. 1973:33 s. 74 f.). Till detta kommer att sedan lagändringen 1986 omfattar upptagningsbegreppet uttryckligen också uppgifter som ännu inte har fixerats på något datamedium, nämligen uppgifter som är under befordran för att användas för automatisk databehandling (se avsnitt 6.1.2). Ett temporärt minne, som t.ex. arbetsminnet i en dator, utgör exempel på ett datamedium som används för bearbetning av program och andra data. På grund härav samt med hänsyn till vad som nyss sagts har regeringen svårt att se varför uppgifter som finns i ett sådant minne inte skulle falla inom beskrivningen av upptagningsbegreppet. Enligt regeringens mening talar i stället starka skäl för att upptagningsbegreppet och det gällande straffansvaret även inbegriper uppgifter som finns i en dators temporära minne. Sådana uppgifter måste dessutom anses lika skyddsvärda som andra uppgifter som skyddas av dataintrångsbestämmelsen. För att bl.a. klarlägga att straffskyddet omfattar också uppgifter av nu nämnt slag föreslås i avsnitt 7.2 en tydligare beskrivning av skyddsobjektet.

Sammanfattningsvis gör regeringen den bedömningen att svensk rätt, genom dataintrångsbestämmelsen, uppfyller rambeslutets krav på vad som skall vara straffbelagt som olagligt intrång i informationssystem.

6.2.3 Olaglig systemstörning

Regeringens bedömning: Svensk rätt uppfyller genom främst dataintrångsbestämmelsen 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.

Promemorians bedömning överensstämmer med regeringens bedömning.

Remissinstanserna: Majoriteten av remissinstanserna har inte haft något att erinra mot promemorians bedömning. *Åklagarmyndigheten* och *Rikspolisstyrelsen* har invänt mot begreppet upptagning för automatisk databehandling och menat att det är för snävt i förhållande till rambeslutets krav på straffbart handlande enligt artikel 3 om olaglig systemstörning. Till exempel omfattar enligt Rikspolisstyrelsen straffansvaret inte den situationen att ett program i en dators arbetsminne angrips och därmed stör systemet, eftersom uppgifter i ett sådant minne inte är att anse som lagrade (fixerade) och inte heller är under befordran. Även *Säkerhetspolisen* har på liknande grunder ifrågasatt upptagningsbegreppets förenlighet med de åtaganden som följer av rambeslutets artikel 3.

Skälen för regeringens bedömning: 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 föregående avsnitt om olagligt intrång i informationssystem.

Enligt artikel 3 riktas handlingen mot driften av ett informationssystem. Vad som utgör ett sådant system definieras i artikel 1 a och har närmare kommenterats i föregående avsnitt. Det som sägs där är tillämpligt också här. Den handling som skall vara straffbelagd består i att allvarligt hindra eller avbryta driften av systemet. Hur denna störning kan åstadkommas anges som framgått genom en uppräkning av olika åtgärder med datorbehandlingsbara uppgifter. Vad som närmare skall förstås med sådana uppgifter finns redovisat i avsnitt 5.3.

Dataintrångsbestämmelsen kriminaliserar inte direkt ett allvarligt hindrande eller avbrytande av driften av ett informationssystem. Däremot straffbeläggs vissa förfaranden med upptagningar. I den mån dessa 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 enlighet med vad regeringen i tidigare avsnitt (6.1.2 och 6.2.2) sagt om innebörden och tolkningen av det svenska upptagningsbegreppet och straffan-

svaret måste begreppet anses motsvara vad som enligt rambeslutet skall förstås med begreppet datorbehandlingsbara uppgifter. I avsnitt 7.2 föreslås en ändrad beskrivning av skyddsobjektet i syfte att bl.a. klargöra vad bestämmelsen skyddar.

De förfaranden som i dataintrångsbestämmelsen beskrivs som ändra eller utplåna måste anses motsvara de åtgärder i artikel 3 som benämns skada, radera, försämra och ändra. Vad därefter gäller artikelns åtgärder i övrigt, dvs. att mata in, överföra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter torde i många fall dessa samtidigt innebära att upptagningar ändras eller utplånas och därmed omfattas av dataintrångsbestämmelsen. Dessutom är det straffbart som dataintrång att föra in en upptagning i ett register. Åtgärderna är även straffbara som dataintrång i de fall de samtidigt innebär att någon olovligen bereder sig tillgång till en upptagning. Trots det nu sagda torde emellertid dataintrångsbestämmelsen inte fullt ut täcka de situationer där datorbehandlingsbara uppgifter matas in, överförs, hindras eller görs oåtkomliga. Det förekommer t.ex. situationer där informationssystem avsiktligt blockeras eller kraftigt överbelastas genom automatiskt genererade meddelanden. Som exempel kan nämnas program som skapar och sänder så stora mängder e-post att mottagarens system blockeras. Sådana angrepp kan även åstadkommas genom manuella sändningar av e-post i stor skala. Det kan också handla om att genom upprepade anrop eller försök till anrop överbelasta eller blockera ett informationssystem för andra användare.

Frågan är då om det finns andra svenska straffbestämmelser som uppfyller åtagandet i artikel 3, särskilt i de delar där 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 vissa av de situationer som skall vara straffbara enligt artikel 3 som hindrande eller avbrytande av ett informationssystems drift. De torde t.ex. kunna tillämpas i vissa fall när handlandet samtidigt innebär att datorer eller program skadas. Bestämmelserna torde dock inte fullt ut täcka de situationer som skall vara straffbelagda enligt artikel 3. Det är t.ex. tveksamt i vilken utsträckning de är tillämpliga vid tillgänglighetsattacker där skadan endast är av tillfällig karaktär. Därtill skall läggas att sabotagebestämmelsen till skillnad från rambeslutet endast tar sikte på viss för samhället särskilt viktig egendom. Sammanfattningsvis svarar alltså inte heller skadegörelse- och sabotagebrotten fullt ut mot det åtagande som följer av artikel 3.

Det kan vidare diskuteras om straffbestämmelsen om egenmäktigt förfarande (8 kap. 8 § brottsbalken) kan vara tillämplig. För sådant brott skall bl.a. den dömas som utan tillgrepp, genom att anbringa eller bryta lås eller annorledes, olovligen rubbar annans besittning. I vilken utsträckning ansvar för egenmäktigt förfarande kan aktualiseras för tillgänglighetsattacker är emellertid oklart. Vägledande praxis saknas.

Vidare kan nämnas att det är 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. En utredning har fått i uppdrag att se över bestämmelserna om förfalsknings- och sanningsbrotten ur ett IT-perspektiv (dir. 2005:68). Uppdraget skall redovisas senast den 29 juni 2007.

Av det redovisade framgår att främst dataintrångsbestämmelsen men också andra straffbestämmelser, bl.a. de om skadegörelse- och sabotagebrott, till övervägande del uppfyller rambeslutets krav i artikel 3 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

Regeringens bedömning: Svensk rätt uppfyller genom främst dataintrångsbestämmelsen 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 att lagstiftningsåtgärder vidtas.

Promemorians bedömning överensstämmer med regeringens bedömning.

Remissinstanserna: Majoriteten av remissinstanserna har inte haft något att erinra mot promemorians bedömning. *Åklagarmyndigheten* och *Rikspolisstyrelsen* har gjort gällande att det svenska begreppet upptagning för automatisk databehandling inte fullt ut motsvarar rambeslutets krav på straffbarhet enligt artikel 4 om olaglig datastörning. Enligt myndigheterna omfattar upptagningsbegreppet inte uppgifter som finns i temporära minnen, t.ex. en dators arbetsminne, eftersom de inte är att anse som lagrade (fixerade) och inte heller är under befordran.

Skälen för regeringens bedömning: 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 i informationssystem.

Den straffbara handlingen enligt artikel 4 riktar sig mot datorbehandlingsbara uppgifter i ett informationssystem. Det innebär att den inte avser sådana uppgifter när de befordras i nät. Detta har närmare ut-

vecklats i avsnitt 6.2.2 varför det i denna del hänvisas till resonemanget som förts där.

Datastörningen skall bl.a. 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. I sammanhanget kan nämnas att det i avsnitt 7.2 föreslås ett förtydligande av vilka uppgifter som bestämmelsen skyddar.

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 olaglig systemstörning kan sådana störningar i viss utsträckning redan omfattas av dataintrångsbestämmelsen. I vissa fall kan dock störningar av angivet slag åstadkommas utan att de är straffbara som dataintrång. Som vidare konstaterats i det avsnittet torde inte heller andra svenska straffbestämmelser, främst om skadegörelse och sabotage, vara tillräckliga för att fullt ut uppfylla rambeslutets krav i dessa delar. Även i denna del hänvisas till vad som anförts i föregående avsnitt.

Sammanfattningsvis krävs alltså att lagstiftningsåtgärder vidtas för att svensk rätt helt skall uppfylla rambeslutets krav på att det skall vara straffbart att hindra flödet av eller göra datorbehandlingsbara uppgifter oåtkomliga.

6.2.5 Anstiftan av, medhjälp till och försök till brott

Regeringens 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.

Promemorians bedömning överensstämmer med regeringens bedömning.

Remissinstanserna har lämnat bedömningen utan erinran.

Skälen för regeringens bedömning: Enligt *artikel 5 punkt 1* skall anstiftan av och medhjälp till olagligt intrång i informationssystem, olaglig systemstörning och olaglig datastörning vara straffbelagt. I svensk rätt är anstiftan av och medhjälp till dataintrång, skadegörelse, grov skadegörelse samt sabotage och grovt sabotage straffbart.

Vidare skall enligt *artikel 5 punkt 2* försök till olagligt intrång i informationssystem, olaglig systemstörning och olaglig datastörning vara straffbart. När det gäller olagligt intrång i informationssystem får dock en medlemsstat enligt *artikel 5 punkt 3* besluta att inte straffbelägga försök till sådant brott. Enligt svensk rätt är försök till dataintrång straffbart under förutsättning att intrånget inte skulle ha varit att anse som ringa om det hade fullbordats. Eftersom rambeslutet inte kräver att ringa fall av de fullbordade brotten i artikel 2, 3 och 4 straffbeläggs, är det enligt regeringens mening en rimlig tolkning att utgå ifrån att så inte heller krävs i fråga om försök i sådana fall även om de fullbordade ringa gärningarna i och för sig kriminaliseras i nationell rätt. När det gäller skadegörelse,

grov skadegörelse, sabotage och grovt sabotage är försök till dessa brott straffbelagda.

Sammanfattningsvis gör regeringen den bedömningen att 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.

6.3 Påföljder och försvårande omständigheter

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

Promemorians bedömning överensstämmer med regeringens bedömning.

Remissinstanserna: Remissinstanserna har inte haft något att erinra mot promemorians bedömning. *Göteborgs tingsrätt* och *Rikspolisstyrelsen* har därutöver ansett att det bör införas en särskild straffskala med fängelse upp till fyra år för grova fall av dataintrång. Även *Säkerhetspolisen* har ansett det angeläget att införa ett grovt dataintrångsbrott eller i vart fall skärpa straffskalan för dataintrång.

Skälen för regeringens bedömning: Enligt *artikel 6 punkt 1* skall samtliga de brott som avses i artiklarna 2, 3, 4 och 5 vara belagda med effektiva, proportionella och avskräckande straffrättsliga påföljder. Vidare skall enligt *artikel 6 punkt 2* de brott som avses i artiklarna 3 och 4, dvs. olaglig systemstörning och olaglig datastörning, vara belagda med 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 på viss tid, lägst två och högst tio år, eller på livstid. Samtliga brott har alltså ett maximistraff om minst ett års fängelse. Följaktligen krävs inte någon lagändring för att uppfylla åtagandena i artikel 6.

I *artikel 7 punkt 1* föreskrivs att brott enligt artiklarna 2 punkt 2, 3 och 4, dvs. olagligt intrång i informationssystem som begås genom intrång i en säkerhetsåtgärd samt olaglig systemstörning och olaglig datastörning, som begås inom ramen för en kriminell organisation, skall vara belagda med ett maximistraff på minst två till fem års fängelse. Det innebär att fängelse i åtminstone två år skall finnas i straffskalan. 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 enligt regeringens mening tillräckligt att den grövsta formen – i detta fall grov skadegörelse – motsvarar vad som krävs enligt rambeslutet. Straffskalorna är alltså förenliga med rambeslutet. Också den omständighet som rambeslutet anger som försvårande måste anses motsvara vad som gäller enligt svensk rätt. Enligt brottsbalken skall nämligen 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. 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 brottet har orsakat allvarliga skador eller påverkat väsentliga intressen. Bestämmelsen är fakultativ och kräver därmed inte någon lagändring. I sammanhanget bör dock framhållas att enligt svensk rätt kan sådana omständigheter motivera att brottet bedöms som t.ex. grov skadegörelse eller grovt sabotage. Straffskalorna för dessa brott motsvarar väl den i punkt 1 föreskrivna fängelsenivån.

Sammanfattningsvis görs alltså bedömningen att svensk rätt uppfyller rambeslutets bestämmelser om påföljder och försvårande omständigheter. Samtliga remissinstanser har instämt i eller inte haft något att erinra mot denna bedömning.

Göteborgs tingsrätt och *Rikspolisstyrelsen* har likväl ansett – särskilt mot bakgrund av den stora ekonomiska skada som kan orsakas kommersiella intressen vid angrepp mot informationssystem – att det bör införas en särskild straffskala med fängelse i högst fyra år för grova fall av dataintrång. Även *Säkerhetspolisen* har av samma skäl ansett det angeläget att införa ett grovt dataintrångsbrott eller i vart fall skärpa straffskalan för dataintrång.

Regeringen vill i denna del framföra följande. Dataintrång kan medföra fängelse i upp till två år. Vidare kan en gärning av sådant slag beroende på omständigheterna i det enskilda fallet vara att bedöma som grov skadegörelse, sabotage eller grovt sabotage. För dessa brott kan enligt vad som ovan redovisats följa ett ännu längre fängelsestraff. 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 det brottet gäller en straffskala från fängelse i lägst två år upp till livstid. Det finns alltså redan enligt dagens lagstiftning utrymme att i allvarliga fall ingripa med kraftfulla reaktioner. Därtill skall läggas att frågan om en straffhöjning för dataintrång eller ett införande av ett grovt sådant brott förutsätter överväganden om motsvarande ändringar behövs i de andra bestämmelser i 4 kap. brottsbalken som har ett nära samband med dataintrångsbestämmelsen. Dessa har i dag samma straffskala. Samtliga saknar vidare gradindelning. Dessutom är dataintrångsbestämmelsen som framgått ett subsidiärt brott till brytande av post- eller telehemlighet och intrång i förvar. Förslaget av remissinstanserna väcker alltså frågor av såväl systematisk som lagteknisk karaktär. Regeringen gör bedömningen att frågorna förutsätter en analys som det saknas beredningsunderlag för och som inte heller är möjlig att göra inom ramen för detta lagstiftningsärende. Mot denna bakgrund föreslår regeringen inte någon ändring av straffskalan för dataintrång eller ett införande av ett grovt sådant brott.

6.4 Ansvar och påföljder för juridiska personer

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

Promemorians bedömning överensstämmer med regeringens bedömning.

Remissinstanserna: I princip samtliga remissinstanser har inte haft något att erinra mot promemorians bedömning. Enligt *Juridiska fakultetsnämnden vid Uppsala universitet* aktualiserar rambeslutets genomförande åter frågan om den svenska regleringen av företagsbot i längden kan anses uppfylla de krav som inom EU ställs på ansvar för juridiska personer.

Skälen för regeringens bedömning: 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 [2001] 771 slutlig) angavs också att Sverige har lagstiftning om att juridiska personer kan ställas till rättsligt ansvar för de brott som omfattas av rambeslutet.

Motsvarande bedömning, dvs. att Sverige uppfyller bestämmelserna om ansvar och påföljder för juridiska personer, har gjorts för andra rambeslut och senast när det gäller EU:s rambeslut om olaglig narkotikahandel (prop. 2005/06:42, bet. 2005/06:JuU10, rskr. 2005/06:147). Därutöver kan nämnas att möjligheterna att ålägga företagsbot utvidgats den 1 juli 2006 (se avsnitt 6.1.7).

Juridiska fakultetsnämnden vid Uppsala universitet har anfört att förevarande rambesluts genomförande åter aktualiserar frågan om den svenska regleringen av företagsbot i längden kan anses uppfylla de krav som inom EU ställs på ansvar för juridiska personer.

Regeringen gör bedömningen att de svenska reglerna om företagsbot även i fråga om rambeslutet om angrepp mot informationssystem får anses motsvara de krav som ställs i rambeslutets artikel 8 och artikel 9 om ansvar och påföljder för juridiska personer.

Regeringens bedömning: Rambeslutets krav på behörighet (domsrätt) motsvarar i princip svenska bestämmelser på området. Sverige bör 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.

Promemorians bedömning överensstämmer med regeringens bedömning.

Remissinstanserna har lämnat bedömningen utan erinran. *Svea hovrätt* har dock väckt frågan om inte underrättelsen också, i enlighet med artikel 10 punkterna 5 och 6, bör ange under vilka omständigheter som Sverige kommer att tillämpa bestämmelsen om behörighet i artikel 10 punkt 1 b i fråga om svenska medborgare som begår brott utom riket, t.ex. med åberopande av krav på dubbel straffbarhet.

Skälen för regeringens bedömning*: 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 men 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 svenska domstolar behörighet att döma över brott i de fall som avses i punkt 1 a och punkt 2. Bestämmelserna uppfyller därför rambeslutet i dessa avseenden. Någon lagändring krävs alltså 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. För att svensk domsrätt skall föreligga för sådana brott krävs dock normalt att gärningen är straffbar där den begicks (krav på dubbel straffbarhet). Vidare får inte dömas till strängare påföljd än den strängaste påföljd som är möjlig enligt lagen på gärningsorten. Med hänsyn till syftet med rambeslutet, dvs. att det i samtliga EU-medlemsstater skall finnas lagstiftning som bygger på de gemensamma bestämmelserna i rambeslutet om vilka handlingar som skall vara straffbara som angrepp mot informationssystem och om påföljder för sådana angrepp, torde emellertid nämnda krav svårligen medföra några tillämpningsproblem.

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. 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 nödvändig. Det skall i sammanhanget nämnas att bl.a. 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

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

Promemorians bedömning överensstämmer med regeringens bedömning.

Remissinstanserna har lämnat bedömningen utan erinran.

Skälen för regeringens bedömning: Enligt *artikel 11* skall medlemsstaterna för utbyte av uppgifter om de brott som avses i rambeslutet, 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. Det nät som åsyftas är – vilket uttryckligen framgår av punkt 16 i ingressen – det 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. Av artikel 11 följer vidare att varje medlemsstat skall underrätta rådets generalsekretariat och kommissionen om sin kontaktpunkt.

Sverige har deltagit i nämnda 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 att Rikspolisstyrelsen skall vara Sveriges kontaktpunkt.

7 Ett utvidgat straffansvar för dataintrång

7.1 Utgångspunkter för genomförandet av rambeslutets bestämmelser om straffbara handlingar

Regeringens förslag: För att rambeslutets bestämmelser om straffbara handlingar fullt ut skall uppfyllas utvidgas straffansvaret för dataintrång.

Promemorians förslag överensstämmer med regeringens förslag.

Remissinstanserna: Majoriteten av remissinstanserna har inte haft något att erinra mot promemorians förslag. *Krisberedskapsmyndigheten* och *Sveriges advokatsamfund* har ifrågasatt den föreslagna lagtekniska lösningen och hänvisat till att huvuddelen av medlemsländerna inom EU och Europarådet infört separata regler för kriminalisering av intrång i system respektive angrepp mot lagrade data. Enligt remissinstanserna har frågan om en motsvarande uppdelning av regelverket behövs i Sverige inte fått tillräcklig genomlysning i promemorian. De har vidare ifrågasatt olovlighetsrekvisitet i dataintrångsbestämmelsen och menat att det är oklart och svårtolkat med hänsyn till de många olikartade företeelser som det avser att omfatta. Enligt myndigheterna försvårar detta bl.a. informationssäkerhetsarbetet för företag och myndigheter. *Svenskt Näringsliv* har framfört att det vore önskvärt av pedagogiska skäl att införa en konstruktion som motsvarar den i rambeslutet. *Sig Security* har uttryckt sig i samma riktning. *Rikspolisstyrelsen* har mot bakgrund av uppfattningen att bl.a. upptagningsbegreppet bör utgå ur dataintrångsbestämmelsen ansett att det vore lämpligt att också ändra skyddsobjektet i den. Enligt myndigheten vore ett alternativ att använda de begrepp som definieras och används i rambeslutet, dvs. informationssystem och datorbehandlingsbara uppgifter. – *Svea hovrätt* har ansett att promemorians och departementspromemorians Brott och brottsutredning i IT-miljö (Ds

2005:6) förslag till ändringar i dataintrångsbestämmelsen i det fortsatta lagstiftningsarbetet bör samordnas i fråga om föreslagna utvidgningar av det kriminaliserade området och förslag till definition av upptagningsbegreppet. Även *Krisberedskapsmyndigheten* har ansett att det finns behov av en sådan samordning.

Skälen för regeringens förslag: Av avsnitten 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 svenska straffbestämmelser. Det finns dock vissa handlingar som skall vara straffbelagda enligt rambeslutet som inte är kriminaliserade i svensk rätt. De gärningar som åtminstone i vissa fall inte är kriminaliserade är när någon allvarligt hindrar eller avbryter driften av ett informationssystem genom bl.a. inmatningar eller överföringar av datorbehandlingsbara uppgifter eller hindrar flödet av eller gör det omöjligt att komma åt datorbehandlingsbara uppgifter i ett informationssystem. Anstiftan av och medhjälp till samt försök till dessa är följaktligen inte heller straffbelagt. 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 har konstaterat i propositionen om Sveriges antagande av rambeslutet (prop. 2003/04:164) avser ändringarna förfaranden som från svensk utgångspunkt måste anses vara straffvärda.

En särskild fråga är då i vilken straffbestämmelse lagändringarna lämpligen bör genomföras. Regeringen gör i denna del följande bedömning. De skäl som regeringen åberopat i avsnitt 6.2.1 för att i första hand välja dataintrångsbestämmelsen i analysen av hur gällande svensk straffrätt förhåller sig till rambeslutets regler om straffbara handlingar gör sig också gällande med avseende på den nu aktuella frågan. Därutöver har analysen i avsnitten 6.2.2–6.2.4 visat att dataintrångsbestämmelsens kriminalisering av åtgärder med upptagningar för automatisk databehandling måste anses motsvara åtagandena enligt rambeslutet att kriminalisera vissa förfaranden med informationssystem och datorbehandlingsbara uppgifter. Dataintrångsbestämmelsen är vidare uppbyggd med krav på uppsåt och olovlighet på ett sätt som överensstämmer med den reglering som följer av rambeslutet. Sammantaget talar enligt regeringen såväl systematiska som sakliga skäl för att lagändringarna bör göras i dataintrångsbestämmelsen. För att fullt ut uppfylla rambeslutets krav på kriminalisering bör således straffansvaret för dataintrång utvidgas.

Majoriteten av remissinstanserna har inte haft något att erinra mot en sådan lagteknisk lösning. Från några håll har dock kritiska synpunkter förts fram. *Krisberedskapsmyndigheten* och *Sveriges advokatsamfund* har med hänvisning till att andra medlemsländer inom EU och Europarådet infört separata regler för kriminalisering av intrång i system respektive angrepp mot data efterfrågat en närmare analys i fråga om behovet av en motsvarande uppdelning i svensk rätt. I denna del vill regeringen framföra följande. Som framgått uppfyller dataintrångsbestämmelsen redan med sin nuvarande uppbyggnad och utformning till stor del det som skall vara straffbelagt enligt rambeslutet. Den utvidgning av straffansvaret som krävs för att helt uppfylla rambeslutet är av endast begränsad omfattning

och kan enligt vad som närmare framgår av avsnitt 7.3 genomföras utan genomgripande förändringar av dataintrångsbestämmelsen. En lagteknisk lösning motsvarande den som remissinstanserna fört fram och som alltså i sig inte är nödvändig för att genomföra rambeslutet skulle emellertid förutsätta en betydligt större omarbetning av befintligt regelverk. En sådan lösning väcker dessutom ett antal frågor av systematisk karaktär. Även vissa gränsdragningsproblem kan förutses med en sådan lösning. Enligt regeringen kräver frågorna överväganden som inte låter sig göra inom ramen för detta lagstiftningsärende.

Vad därefter gäller frågan om att, såsom *Rikspolisstyrelsen* gett uttryck för, ändra skyddsobjektet i dataintrångsbestämmelsen genom att föra in ett nytt och alternativt sådant som t.ex. informationssystem anser regeringen att en sådan omarbetning, som för övrigt inte är någon förutsättning för att uppfylla åtagandena enligt rambeslutet, i onödan skulle komplicera bestämmelsen. En sådan omarbetning ger också upphov till frågor av systematisk natur. Den skulle dessutom riskera att medföra en vidlyftig lagtext. En fördel med den nuvarande konstruktionen är i stället att bestämmelsen – liksom svensk straffrättslig reglering i allmänhet – är koncentrerad. Någon förändring av skyddsobjektet i det nu angivna avseendet bör således inte komma till stånd. I fråga om upptagningsbegreppet föreslår dock regeringen vissa ändringar för att förtydliga och modernisera detta, se avsnitt 7.2.

Avslutningsvis har *Krisberedskapsmyndigheten* och *Sveriges advokatsamfund* varit kritiska även i fråga om den närmare utformningen av dataintrångsbestämmelsen. Sålunda har remissinstanserna ansett att olovlighetsrekvisitet är oklart och svårtolkat, eftersom det döljer många olikartade företeelser och därmed försvårar bl.a. informationssäkerhetsarbetet för företag och myndigheter. De har som exempel tagit upp frågan huruvida en arbetsgivare gör sig skyldig till brott genom att kontrollera anställdas e-post. Regeringen, som i och för sig kan ha viss förståelse för den kritik som remissinstanserna fört fram, vill peka på att motsvarande rekvisit även används i de till dataintrångsbestämmelsen primära bestämmelserna om brytande av post- eller telehemlighet och intrång i förvar. Rekvisitet är inte heller nytt. En fördel med att behålla rekvisitet är att de förarbetsuttalanden och den praxis som finns om detta, både vad avser dataintrångsbestämmelsen och liknande straffbestämmelser där samma rekvisit förekommer, fortsatt kan ha tillämplighet och därmed ge vägledning. Därtill kommer att avsikten med rekvisitet just är att kunna fånga upp gärningar av skiftande slag. Att i lagtext i detalj försöka räkna upp samtliga dessa är enligt regeringens mening inte lämpligt och inte heller möjligt. Den närmare avgränsningen får i stället överlämnas åt rättstillämpningen att avgöra med ledning av samtliga omständigheter i varje enskilt fall, däribland vilka arbetsrättsliga rättigheter och skyldigheter en arbetsgivare kan ha. I sammanhanget kan nämnas att en särskild utredare fått i uppdrag att lämna förslag till lagreglering av skydd för den personliga integriteten i arbetslivet (dir. 2006:55). Föreslagen lagreglering skall klargöra både när viss kontroll av arbetstagare och arbetssökande får ske samt hur den information sådan kontroll genererar får behandlas. I uppdraget ingår t.ex. att lämna förslag till reglering av kontroll av privat användning av e-post och Internet. Uppdraget skall redovisas den 15 januari 2008. Det bör slutligen tilläggas att frågan om tillämp-

ningen av olovlighetsrekvisitet oftast inte torde vålla några större svårigheter. De flesta remissinstanserna har inte heller framfört att de sett några sådana problem. Någon ändring i fråga om rekvisitet bör alltså inte genomföras.

Sammanfattningsvis föreslås alltså att straffansvaret för dataintrång utvidgas. Det föreslås också i avsnitt 7.2 vissa förtydliganden och en språklig modernisering av bestämmelsen. Utgångspunkten för genomförandet av rambeslutets bestämmelser om straffbara handlingar skall vara att så långt möjligt behålla den nuvarande uppbyggnaden och utformningen av dataintrångsbestämmelsen och endast komplettera den med de tillägg som är nödvändiga till följd av rambeslutet. Av det sagda följer således att bestämmelsen inte skall omarbetas för att helt överensstämma med rambeslutets formuleringar av åtgärder som utgör angrepp eller rambeslutets tekniska begrepp.

Ett par remissinstanser, bl.a. *Svea hovrätt*, har ansett att promemorians och departementspromemorians Brott och brottsutredning i IT-miljö (Ds 2005:6) förslag till ändringar i dataintrångsbestämmelsen i det fortsatta lagstiftningsarbetet bör samordnas i fråga om bl.a. föreslagna utvidgningar av det kriminaliserade området. Regeringen gör i detta avseende följande bedömning. Rambeslutets bestämmelser om straffbara handlingar har visserligen, som nämnts i avsnitt 4.2.2, tagit sin utgångspunkt i Europarådets konvention om IT-relaterad brottslighet motsvarande bestämmelser. Konventionens genomförande behandlas i den nämnda departementspromemorian. Enligt regeringens uppfattning bör emellertid genomförandet av rambeslutet behandlas fristående från frågan om ett genomförande av konventionen. Konventionen innehåller nämligen ett flertal bestämmelser som saknar motsvarighet i rambeslutet och som rör helt andra områden. Det kan därför förutsättas att ett genomförande av konventionens bestämmelser till stor del kräver andra överväganden än de som genomförandet av rambeslutets bestämmelser föranleder. Någon samordning med frågan om genomförande av Europarådets konvention om IT-relaterad brottslighet bör därmed inte ske.

7.2 Upptagningsbegreppet

Regeringens förslag: Dataintrångsbestämmelsen förtydligas och moderniseras språkligt genom att begreppet upptagning för automatisk databehandling, som även inbegriper uppgifter som är under befordran via elektroniskt eller annat liknande hjälpmedel, i sin helhet ersätts med uttrycket ”uppgift som är avsedd för automatiserad behandling”.

Promemorians förslag: Överensstämmer till viss del med regeringens förslag. I promemorian har föreslagits en något annorlunda lagteknisk lösning och utformning av lagtexten. Enligt promemorians förslag förtydligas enbart den del av bestämmelsen som avser uppgifter som är under befordran – bl.a. genom att uttrycket elektromagnetiska vågor används – medan det ursprungliga upptagningsbegreppet i princip behålls intakt. I promemorian har vidare föreslagits en modernisering av bestämmelsen genom att uttrycket automatisk databehandling ersätts med automatiserad databehandling.

Remissinstanserna: *Åklagarmyndigheten* har – mot bakgrund av uppfattningen att upptagningsbegreppet inte omfattar uppgifter som finns i en dators temporära minne då uppgifterna inte är att anse som fixerade eller under befordran – ansett att begreppet bör utmönstras ur lagstiftningen och ersättas med ett annat rekvisit som tar sikte på att skydda alla uppgifter som behandlas inom ramen för automatisk databehandling, oavsett om de har fixerats eller inte. Även *Rikspolisstyrelsen* har på samma grund förespråkat att upptagningsbegreppet bör utgå ur lagstiftningen. Ett alternativ enligt myndigheten vore att använda de begrepp som definieras och används i rambeslutet, dvs. ”informationssystem” och ”datorbehandlingsbara uppgifter”. Också *Säkerhetspolisen* har pekat på detta alternativ. *Helsingborgs tingsrätt* har ansett att den föreslagna utvidgningen av dataintrångsbestämmelsen, som i grunden kommer att bestå av tre olika typer av brottsförfaranden – olagligt intrång, olaglig systemstörning och olaglig datastörning – gjort bestämmelsen svårtillgänglig. Några remissinstanser, bl.a. *Säkerhetspolisen*, *Försvarsmakten* och *SIG Security*, har förordat att begreppet elektromagnetiska vågor ersätts med begreppet elektroniska kommunikationsnät som finns definierat i lagen (2003:389) om elektronisk kommunikation. Enligt Försvarsmakten täcker det senare bättre in alla former av överföringar av uppgifter för databehandling. Även *Åklagarmyndigheten* har ansett att det finns skäl att närmare undersöka om begreppet elektromagnetiska vågor verkligen omfattar all datakommunikation oavsett överföringsteknik. *Statskontoret* och *SIG Security* har förordat begreppet automatiserad behandling, som är den numera dominerande terminologin. *Krisberedskapsmyndigheten* och *Sveriges advokatsamfund* har pekat på frågan huruvida en arbetsgivare gör sig skyldig till brott genom att avlyssna kommunikation som sker via etern.

Skälen för regeringens förslag

Upptagningsbegreppet förtydligas

Innan de lagändringar som rambeslutet föranleder behandlas kan det finnas anledning att överväga om dataintrångsbestämmelsen behöver förtydligas i fråga om upptagningsbegreppet.

Som framgått av den tidigare redogörelsen i avsnitt 6.1.2 avses med begreppet upptagning för automatisk databehandling uppgift som är fixerad på någon form av datamedium och som alltså antingen finns i eller kan matas in i en dator samt 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 det senare avses också uppgift som ännu inte har fixerats på något datamedium.

Regeringen har i avsnitt 6.2.2 ansett att begreppet upptagning för automatisk databehandling och det gällande straffskyddet bör förstås så att det omfattar även uppgifter som finns i en dators temporära minne. Vissa remissinstanser, bl.a. *Åklagarmyndigheten* och *Rikspolisstyrelsen*, har dock ifrågasatt en sådan tolkning. Enligt myndigheterna är det tveksamt om uppgifterna i ett sådant fall kan sägas ha varit fixerade på ett datamedium. De kan – har myndigheterna menat – inte heller sägas vara under befordran i den mening som avses i dataintrångsbestämmelsen.

En utgångspunkt är givetvis att lagstiftningen skall vara så klar och tydlig som möjligt. Detta gör sig särskilt gällande i fråga om rekvisit som är av avgörande betydelse för tillämpningen av en straffbestämmelse. Upptagningsbegreppet utgör ett sådant rekvisit. En oklarhet i fråga om den närmare innebörden av begreppet riskerar att medföra att vissa straffvärda förfaranden faller utanför det straffbara området.

Syftet med dataintrångsbestämmelsen har, som framgått, varit att ge ett skydd för allt datalagrat material. I bestämmelsen har detta kommit till uttryck bl.a. genom användningen av begreppet upptagning för automatisk databehandling. Det temporära minnet i en dator, t.ex. arbetsminnet, utgör i dag en viktig grundkomponent där program och andra uppgifter kontinuerligt lagras medan bearbetning pågår. Uppgifter av sådant slag är att anse som lika skyddsvärda som de uppgifter som odiskutabelt omfattas av dataintrångsbestämmelsen. Enligt regeringen är det angeläget att kunna ingripa även mot angrepp som riktar sig mot sådana uppgifter. Det får därför inte råda någon tvekan om vad som straffrättsligt bör gälla i fråga om sådana fall. Mot denna bakgrund anser regeringen att det framstår som motiverat att förtydliga dataintrångsbestämmelsen så att det tydligare än i dag framgår att det straffbara området också omfattar sådana uppgifter som finns i en dators temporära minne.

Dataintrångsbestämmelsen kan emellertid diskuteras även i ett annat avseende, nämligen i fråga om vad som närmare gäller för uppgifter som befordras. En särskild fråga i det sammanhanget är om bestämmelsen enligt sin nuvarande utformning är tillämplig på sådana uppgifter alldeles oavsett på vilket sätt de befordras.

Lagstiftarens syfte har i detta avseende varit att bereda ett skydd för överföringar av både uppgifter som är fixerade och uppgifter som ännu inte har fixerats på något datamedium. När dataintrångsbestämmelsen infördes i början av 1970-talet och kompletterades i mitten av 1980-talet skedde visserligen uppgiftsöverföringar i nät men inte i den omfattning som sker i dag. De uppgifter som överfördes i nät torde ofta ha förmedlats i ledningsbundna nät, men det fanns också teknik för befordran via radio (jfr prop. 1973:33 s. 15). Den tekniska utvecklingen har medfört att uppgiftsöverföringar i dag sker i ett antal olika nät.

Skyddsbehovet för uppgifter som befordras gör sig enligt regeringens mening gällande alldeles oavsett på vilket sätt de befordras. Lagstiftningen bör därför ge ett heltäckande skydd för uppgifter som överförs. Enligt regeringen kan dataintrångsbestämmelsens lydelse i sig inte anses utesluta att detta skydd finns redan i dag. En viss 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. Mot denna bakgrund och då det inte heller i detta avseende får råda någon tvekan i fråga om vad som närmare skall gälla anser regeringen att skäl föreligger att förtydliga att dataintrångsbestämmelsen omfattar alla uppgifter som befordras.

Den närmare utformningen av förtydligandet

Vad därefter gäller frågan om förtydligandets närmare utformning gör regeringen en delvis annorlunda bedömning än den som görs i promemorian. Regeringen har i stället ansett att det i två avseenden finns behov av

att förtydliga dataintrångsbestämmelsen, dels i fråga om det ursprungliga begreppet upptagning för automatisk databehandling, dels i fråga om det tillägg till begreppet som infördes 1986 om att med upptagning avses även uppgifter som är under befordran via ett elektroniskt eller annat liknande hjälpmedel för att användas för automatisk databehandling. Enligt regeringens mening finns det två alternativa lösningar att laborera med när det gäller frågan på vilket sätt förtydligandet lämpligen bör genomföras. Det första alternativet är att som grund behålla de nuvarande formuleringarna men justera dessa så att de tydligare än i dag ger uttryck för alla de uppgifter som dataintrångsbestämmelsen avser att skydda. Det andra alternativet går ut på att sammanföra och ersätta de nuvarande formuleringarna med ett nytt och gemensamt uttryck som på ett mer koncentrerat och tydligare sätt beskriver och fångar upp de angivna uppgifterna. Vad som talar för det förra alternativet är att den nuvarande uppbyggnaden av upptagningsbegreppet då i princip kan behållas oförändrad. Å andra sidan riskerar en sådan lösning samtidigt att göra lagtexten vidlyftig och ytterligare komplicera bestämmelsen. En fördel med det senare alternativet är att lagtexten förenklas och görs mer lättillgänglig. Det skapar också bättre förutsättningar att modernisera och framtidsanpassa begreppsapparaten i bestämmelsen. Till detta skall läggas vad bl.a. *Åklagarmyndigheten*, *Rikspolisstyrelsen* och *Helsingborgs tingsrätt* anfört om behovet av att i olika avseenden förtydliga och göra dataintrångsbestämmelsen mer begriplig. Därutöver kan även nämnas att ett flertal remissinstanser, bl.a. *Säkerhetspolisen*, *Försvarsmakten* och *SIG Security*, haft invändningar mot det förslag till förtydligande som lades fram i promemorian och efterfrågat ytterligare klargörande. Även det nu sagda menar regeringen ger stöd för att det är det senare alternativet som bör vinna företräde. Sammanfattningsvis anser således regeringen att övervägande skäl talar för att upptagningsbegreppet i sin helhet nu bör bytas ut.

Vad därefter gäller frågan om vilket uttryck som bör ersätta ifrågavarande begrepp föreslår regeringen som lämpligt sådant ”uppgift som är avsedd för automatiserad behandling”. Fördelen med att välja det uttrycket framför t.ex. det av bl.a. *Rikspolisstyrelsen* förordade begreppet ”datorbehandlingsbara uppgifter”, som återfinns i rambeslutet, är att det i större utsträckning svarar mot det uttryckssätt som ofta används i förarbetena för att beskriva vad som avses med uttrycket upptagning för automatisk databehandling, inklusive uppgifter som befordras. Uttrycket ansluter vidare till den mer moderna terminologi som redan utvecklats i annan angränsande lagstiftning där det just talas om att uppgifter behandlas automatiserat (prop. 2001/02:70 s. 23). Därutöver har begreppet ”uppgift som är avsedd för automatiserad behandling” även den fördelen att det är ett mer teknikneutralt uttryck. Det senare menar regeringen är särskilt viktigt för att kunna tillförsäkra en rättstillämpning som inte urholkar straffskyddet även om de tekniska förhållandena ändras.

Regeringen föreslår alltså att dataintrångsbestämmelsen förtydligas och moderniseras språkligt genom att upptagningsbegreppet i sin helhet ersätts med uttrycket ”uppgift som är avsedd för automatiserad behandling”. Avsikten med det valda begreppet är att fånga in alla uppgifter som uttrycks i en för en automatiserad behandling anpassad och läsbar form. Det innebär att även program av olika slag omfattas av begreppet. Det är

för tillämpningen av begreppet utan betydelse var någonstans de nämnda uppgifterna finns eller förvaras i systemet. Därmed lämnas inte längre något utrymme för diskussioner om uppgifterna är att anse som ”fixerade” eller inte, på vilket datamedium de förvaras eller med vilken teknik de överförs. Regeringen återkommer i författningskommentaren med en närmare redogörelse för begreppets innebörd.

Särskilt om befordran via radio

Sedan länge har ansetts gälla både nationellt och internationellt som en grundläggande princip att etern är fri. Den har ansetts innebära att det i princip är tillåtet för var och en att fritt avlyssna såväl sådan radiokommunikation som är riktad till allmänheten som annan typ av radiokommunikation (se t.ex. prop. 1992/93:200 s. 166 och 2002/03:110 s. 254). En annan sak är att den som via en radiomottagare avlyssnat eller på annat sätt med användande av sådan mottagare fått tillgång till ett meddelande som regel inte får föra det vidare (jfr 6 kap. 23 § lagen [2003:389] om elektronisk kommunikation).

Straffbestämmelsen om brytande av telehemlighet, som dataintrångsbestämmelsen har ett nära samband med, omfattar intrång i telemeddelanden oavsett på vilket sätt de tekniskt förmedlas. Enligt den nyss nämnda principen om att etern är fri anses dock intrång i radiobefordrade sådana i princip falla utanför bestämmelsens tillämpningsområde. Det följer av att olovlighetsrekvisitet i ett sådant fall inte anses uppfyllt.

Principen om eterns frihet anses alltså i dag för straffrättens del innebära att bestämmelsen om brytande av telehemlighet i princip inte är tillämplig på intrång i 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 oavsett på vilket sätt de tekniskt befordras, förutsätter för straffansvar att gärningen är olovlig. På samma grund som beträffande bestämmelsen om brytande av telehemlighet kan därmed i regel inte heller dataintrångsbestämmelsen anses vara tillämplig på intrång i radiobefordrade uppgifter. Vad däremot gäller andra angrepp som t.ex. manipulation i form av ändring eller radering av uppgifter som befordras kan dataintrångsbestämmelsen vara tillämplig även på uppgifter som befordras via radio. Att dataintrångsbestämmelsen omfattar även radiobefordrade uppgifter är alltså inte oförenligt med den nämnda principen.

7.3 Blockering av en uppgift för automatiserad behandling m.m.

Regeringens förslag: Dataintrångsbestämmelsen utvidgas till att omfatta dels den som olovligen blockerar en uppgift som är avsedd för automatiserad behandling, dels den som olovligen allvarligt stör eller hindrar användningen av en sådan uppgift.

Promemorians förslag: Överensstämmer i stort med regeringens förslag, men med en något annorlunda utformning av lagtexten. Enligt pro-

memorians förslag skall dataintrångsbestämmelsen utvidgas till att omfatta den som olovligen undertrycker eller allvarligt hindrar användningen av en upptagning för automatiserad databehandling.

Remissinstanserna: Merparten av remissinstanserna har inte haft något att erinra mot promemorians förslag. *Justitiekanslern* har ifrågasatt om det inte går att hitta ett modernare och mer adekvat ord än undertrycka, som i lexikon anges vara synonymt med tvinga till lydnad, underkuva, göra våld på, mörklägga m.m. Några remissinstanser, bl.a. *Krisberedskapsmyndigheten*, *Sveriges advokatsamfund* och *Helsingborgs tingsrätt*, har ansett att det finns vissa otydligheter i fråga om den föreslagna kriminaliseringen och menat att de kan leda till problem med att avgränsa det straffbara området. Enligt Krisberedskapsmyndigheten och Advokatsamfundet förefaller förslaget innebära att hindrande åtgärder som ses som nödvändiga av säkerhetsskäl – såsom t.ex. att störa ut mobiltelefoni i fängelser – inte kan vidtas utan särskild författningsreglering som tillåter åtgärden, dvs. gör den ”lovlig”. Helsingborgs tingsrätt har ansett att begreppet ”allvarligt hindra” ger föga ledning för rättstillämpningen vid tillgänglighetsattacker som görs i opinionssyfte. Enligt *Svenskt Näringsliv* ter det sig inte helt logiskt att med dataintrång skall förstås även undertryckande och annat allvarligt hindrande av användningen av en upptagning. – *Rikspolisstyrelsen* har ansett att det s.k. registerbegreppet bör utgå ur dataintrångsbestämmelsen, eftersom det saknas skäl att låta uppgifter som är ordnade i register åtnjuta ett större skydd än andra uppgifter som inte är systematiserade på ett sådant sätt.

Skälen för regeringens förslag

Blockering av en uppgift som är avsedd för automatiserad behandling

Som framgått innebär rambeslutets *artikel 4* ett åtagande att kriminalisera bl.a. sådant handlande som består i att uppsåtligen 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. I enlighet med bedömningen i avsnitt 6.2.4 erfordras därför vissa lagstiftningsåtgärder för att uppfylla åtagandet. Lagtekniskt bör detta, som framgått, åstadkommas genom att straffansvaret för dataintrång utvidgas. Utgångspunkterna för en sådan kriminalisering har angetts i avsnitt 7.1.

Det handlande som skall straffbeläggas skall alltså bestå i att hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter. Närmast torde avses hindrande eller spärrande åtgärder av olika slag. Det torde t.ex. kunna röra sig om sådant förfarande som att föra in eller sprida olika typer av sabotageprogram (t.ex. datavirus, trojaner eller logiska bomber).

I promemorians förslag till lagtext uttrycktes det straffbara handlandet på det sättet att en upptagning för automatiserad databehandling *undertrycks*. Begreppet är hämtat från straffbestämmelsen om undertryckande av urkund där det används för att beskriva att en urkund görs obrukbar, undanskaffas eller förstörs (14 kap. 4 § brottsbalken). *Justitiekanslern* har invänt mot det föreslagna begreppet och ifrågasatt om det inte går att hitta ett modernare och mer adekvat ord. Han har därvid särskilt pekat på att undertrycka i lexikon anges vara synonymt med tvinga till lydnad,

underkuva, göra våld på, mörklägga m.m. Regeringen delar den tveksamhet som Justitiekanslern gett uttryck för i fråga om begreppet undertrycka. För att på ett bättre och mer träffande sätt fånga upp de förfaranden som den nu aktuella kriminaliseringen avser att omfatta föreslår regeringen i stället det modernare begreppet ”blockerar”. Begreppet får dessutom anses bättre överensstämma med den terminologi som redan utvecklats på området (jfr t.ex. 3 § personuppgiftslagen [1998:204]). I författningskommentaren redogörs för begreppets närmare innebörd i nu aktuellt avseende.

Enligt vad som tidigare redovisats är åtagandet i artikel 4 begränsat till att träffa datorbehandlingsbara uppgifter *i* ett informationssystem och avser alltså inte sådana uppgifter när de befordras i nät. I promemorian har inte föreslagits någon motsvarande begränsning av det straffbara området. Enligt regeringen skulle en sådan leda till att uppgifter på ett mindre lämpligt sätt skyddas olika beroende på var i systemet de befinner sig. En begränsning skulle dessutom innebära att uppgifter skyddas olika beroende på vilken typ av straffbelagd åtgärd som vidtas med uppgifterna (se även avsnitt 7.2). Mot bakgrund härav finner regeringen att skäl saknas att föreslå en annan avgränsning i detta hänseende än den i promemorian förespråkade. Den föreslagna kriminaliseringen bör alltså på samma sätt som beträffande dataintrångsbestämmelsen i övrigt vara tillämplig på alla uppgifter avsedda för automatiserad behandling oberoende av var uppgifterna finns eller förvaras i systemet. Kriminaliseringen bör vidare, i enlighet med rambeslutet och vad som sagts i avsnitt 7.1, träffa endast sådant handlande som sker olovligen.

Sammanfattningsvis föreslår regeringen sålunda att dataintrångsbestämmelsen utvidgas till att omfatta även den som olovligen blockerar en uppgift som är avsedd för automatiserad behandling. En utvidgad dataintrångsbestämmelse föreslås vidare utformas så att den omfattar den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, *blockerar* eller i register för in en sådan uppgift. Regeringen återkommer i författningskommentaren till den föreslagna kriminaliseringens innebörd. Nedan behandlas dessutom den gällande kriminaliseringen av införing i register.

Allvarligt störande eller hindrande av användningen av en uppgift som är avsedd för automatiserad behandling

Enligt *artikel 3* i rambeslutet skall det vara straffbart som olaglig systemstörning att uppsåtligt och orättmätigt allvarligt hindra eller avbryta driften av ett informationssystem. En sådan störning skall enligt artikeln ske bl.a. genom inmatning eller överföring av datorbehandlingsbara uppgifter eller genom att sådana uppgifter hindras från att flöda eller görs oåtkomliga. Som framgått av avsnitt 6.2.3 är systemstörningar av det angivna slaget inte straffbelagda fullt ut i dag. Genom att som ovan föreslagits utvidga dataintrångsbestämmelsen till att omfatta även den som blockerar en uppgift som är avsedd för automatiserad behandling straffbeläggs dock i sig sådana åtgärder som hindrar flödet av uppgifter eller som gör uppgifter oåtkomliga. För straffansvar krävs då inte att blockeringen samtidigt medför ett avbrott eller annat allvarligt hindrande av systemets drift. Vad som nu sagts kan emellertid inte anses tillräckligt för att helt

uppfylla kriminaliseringsåtagandet i artikel 3. Exempelvis kan det förekomma situationer där inmatning av virusprogram eller överföring av en stor mängd automatiskt genererade meddelanden kraftigt påverkar driften av ett system och därmed också användningen av de uppgifter som finns i systemet utan att uppgifterna helt blockeras. Dataintrångsbestämmelsen måste därför utvidgas ytterligare för att fullt ut motsvara åtagandet. Utgångspunkterna för en utvidgad kriminalisering framgår av avsnitt 7.1.

Det straffbara handlandet skall enligt vad som framgått bestå i att allvarligt hindra eller avbryta driften av ett informationssystem, dvs. driften av apparater för automatisk databehandling samt uppgifter som finns i sådana apparater för att de skall kunna drivas, användas, skyddas och underhållas. I promemorian jämställs en sådan driftsstörning med att de uppgifter som finns i ett informationssystem som störs inte kan användas på ett normalt sätt. Som exempel nämns att överföringar eller införingar av automatiskt genererade meddelanden som medför att en myndighets datorer får kraftigt nedsatt funktion samtidigt hindrar en normal användning av myndighetens uppgifter. Enligt promemorians förslag bör därför den kriminalisering som krävs för att fullt ut straffbelägga systemstörningar åstadkommas genom att det görs straffbart att hindra användningen av en sådan uppgift. I princip samtliga remissinstanser har godtagit eller har inte haft något att erinra mot promemorians förslag. Mot bakgrund härav samt med hänsyn till vad regeringen i tidigare avsnitt slagit fast om att uppgifter avsedda för automatiserad behandling även fortsättningsvis skall gälla som skyddsobjekt i dataintrångsbestämmelsen anser regeringen att skäl föreligger för en kriminalisering på det sätt som promemorian föreslagit. Vad gäller frågan om vilket uttryckssätt som närmare bör användas för att beskriva det straffbara handlandet har några remissinstanser efterlyst vissa förtydliganden. För att den åsyftade kriminaliseringen skall komma till klarare uttryck och också för att uppnå en bättre överensstämmelse med rambeslutet anser regeringen att uttryckssättet ”allvarligt stör eller hindrar användningen av en uppgift som är avsedd för automatiserad behandling” bör väljas. För straffansvar förutsätts alltså att det är frågan om betydande störningar. I begreppet ligger också att en åtgärd som avbryter, dvs. helt hindrar, användningen av en uppgift avsedd för automatiserad behandling omfattas. I det senare fallet torde dock som regel ansvar för blockering komma i fråga. Regeringen återkommer i författningskommentaren med en mer utförlig redogörelse för begreppets innebörd.

Vad därefter gäller frågan om det för straffansvar bör fordras att gärningsmannen har använt sig av vissa särskilt angivna åtgärder för att begå den straffbara handlingen gör regeringen följande bedömning. Som framgått tidigare är åtagandet enligt rambeslutets artikel 3 begränsat till att träffa sådana åtgärder som består i att mata in, överföra, skada, radera, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter. Även om de nu uppräknade åtgärderna får anses väl täcka de förfaranden som i dag används i de sammanhang som här avses bör enligt regeringens mening straffansvaret inte begränsas till enbart dessa åtgärder. Starka skäl talar i stället för att låta både dessa och även andra jämförbara åtgärder kunna omfattas av det straffbara området. Detta inte minst för att kunna tillförsäkra en rättstillämpning även om de tekniska förutsättningarna ändras. Förslagsvis kan detta

komma till uttryck i lagtexten genom att det där anges att användningen störs eller hindras genom en åtgärd som liknar de övriga i bestämmelsen uppräknade, i första hand ändrar, utplånar eller i register för in.

Straffansvaret bör vidare med stöd av åtagandet i artikel 3 och i enlighet med utgångspunkterna i avsnitt 7.1 avgränsas så att det träffar endast sådant handlande som sker olovligen. Det bör vidare på samma grunder som angetts i föregående avsnitt omfatta alla uppgifter som är avsedda för automatiserad behandling oavsett var de finns eller förvaras i systemet.

Krisberedskapsmyndigheten och *Sveriges advokatsamfund* har ansett att den i promemorian föreslagna kriminaliseringen är otydlig och kan leda till problem med att avgränsa det straffbara området. Enligt Krisberedskapsmyndigheten och Advokatsamfundet förefaller förslaget innebära att hindrande åtgärder som ses som nödvändiga av säkerhetsskäl – såsom t.ex. att störa ut mobiltelefoni i fängelser – inte kan vidtas utan särskild författningsreglering som tillåter åtgärden, dvs. gör den lovlig. Regeringen vill i sammanhanget framföra följande. Till exempel en myndighet som har stöd i författning att vidta en sådan åtgärd som remissinstanserna beskrivit kommer givetvis inte att träffas av den nya kriminaliseringen. Avsikten med den är inte heller att straffbelägga sådant förfarande som en för ändamålet behörig person i enlighet med behörigheten vidtar för att testa ett systems säkerhet eller skydd. Detta följer av att gärningen för att vara straffbar skall ha begåtts olovligen. Regeringen har tidigare gjort bedömningen att någon ändring av olovlighetsrekvisitet inte bör komma i fråga. Skälen för detta är närmare utvecklade i avsnitt 7.1. Vad remissinstanserna nu anfört föranleder inte någon annan bedömning av frågan.

Sammanfattningsvis föreslår regeringen sålunda att dataintrångsbestämmelsen utvidgas till att omfatta även den som olovligen genom en åtgärd som liknar de övriga åtgärder som straffbeläggs i bestämmelsen allvarligt stör eller hindrar användningen av en uppgift som är avsedd för automatiserad behandling. Av systematiska hänsyn föreslås att kriminaliseringen anges efter de övriga i dataintrångsbestämmelsen straffbelagda åtgärderna. Bestämmelsen kan redan i de delarna träffa flera av de situationer som anges i artikel 3.

Slutligen har *Svenskt Näringsliv* ansett att det inte ter sig helt logiskt att med dataintrång skall förstås även det av regeringen nu föreslagna straffbara handlandet. Enligt regeringens mening finns det dock ett flertal kopplingar mellan nu aktuellt handlande och vad som i dag avses med dataintrång. Till exempel torde som framgått det föreslagna straffbelagda handlandet inte sällan samtidigt innebära att uppgifter avsedda för automatiserad behandling ändras eller utplånas eller att någon olovligen bereder sig tillgång till sådana uppgifter. Sammantaget anser regeringen därför att skäl föreligger att låta även det nu aktuella handlandet benämnas som dataintrång.

Opinionsyttringar m.m.

En särskild fråga är hur kriminaliseringsförslagen förhåller sig till opinionsyttringar. Datorer används inte sällan som medel för att uttrycka åsikter i vissa frågor. Det förekommer ibland att flera personer i ett sådant

syfte enas om att ett visst klockslag en viss dag kontakta en särskild webbsida eller sända 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 skall inte heller omfatta fall där någon genom t.ex. e-post gör bruk av sin meddelarfrihet.

De föreslagna kriminaliseringarna förutsätter både effekten att användningen av en uppgift allvarligt störs eller hindras eller att uppgiften blockeras och att det föreligger uppsåt i förhållande till detta. Även om alla uppsåtsformer i och för sig är tillämpliga innebär det nu sagda att rena opinionsyttringar faller utanför det straffbara området. Detsamma gäller för 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 också användningen av uppgifter i systemet. Att ett sådant handlande bör vara straffbelagt förutsatt att uppsåt föreligger 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. För straffansvar för en störning av det nämnda slaget i exemplet förutsätts dock att den enskilde kan anses olovligen och uppsåtligen själv eller tillsammans med de andra ha allvarligt stört eller hindrat användningen av uppgiften. Å andra sidan torde på grund av nämnda kvalificerade krav samt kravet på uppsåt 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 det skall vara fråga om allvarligt störande eller hindrande. Det skulle dock innebära en mer långtgående kriminalisering än vad rambeslutet kräver. Dessutom framstår behovet av en så vidsträckt kriminalisering som tveksamt. I sammanhanget bör dock tilläggas, som framgått ovan, att det för straffansvar inte förutsätts att gärningsmannen handlar med ett direkt uppsåt att åstadkomma ovan angivna effekter utan sedvanliga uppsåtsregler är tillämpliga.

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

Särskilt om införing i register

Enligt dataintrångsbestämmelsen är det straffbart att i ett register föra in en upptagning för automatisk databehandling. Med regeringens förslag ovan blir det straffbart att föra in en uppgift som är avsedd för automatiserad behandling i ett register. Registerbegreppet har kommenterats i avsnitt 6.1.2.

Rikspolisstyrelsen har ifrågasatt den angivna kriminaliseringen och ansett att registerbegreppet bör utgå. Enligt Rikspolisstyrelsen medför begreppet att det straffbara området blir för snävt då informationen för att omfattas måste vara strukturerad på ett visst sätt. Genom att slopa orden ”i register” skulle enligt Rikspolisstyrelsen bestämmelsen bli tydligare och diskussioner om vilket skydd uppgifter ordnade i register skall åtnjuta i förhållande till andra uppgifter inte behöva uppkomma.

Enligt regeringens uppfattning är det emellertid, såsom Rikspolisstyrelsen också själv varit inne på, svårt att föreställa sig en situation där en införing görs i något som inte är ett register och där införingen inte heller i övrigt omfattas av nuvarande eller föreslagen kriminalisering i dataintrångsbestämmelsen eller förberedelse- eller försökskriminaliseringen. Någon direkt kritik mot bestämmelsen med hänsyn till tillämpningen i praxis har inte heller framförts. Till detta kommer att ett slopande av registerbegreppet enligt regeringens mening riskerar att medföra en alltför vidsträckt kriminalisering. Inte minst väcks frågor om förhållandet till sådana rena opinionsyttringar som regeringen diskuterat ovan. Behovet av att, som Rikspolisstyrelsen föreslagit, utvidga dataintrångsbestämmelsen till att omfatta alla införingar framstår således av flera skäl som tveksamt. En sådan ändring bör därför inte genomföras.

7.4 Anstiftan, medhjälp och försök m.m.

Regeringens bedömning: Genom att de gärningar som omfattas av kriminaliseringsförslagen straffbeläggs blir brottsbalkens generella bestämmelser om medverkan och bestämmelserna om försök och förberedelse till dataintrång tillämpliga på anstiftan av, medhjälp till, försök till och förberedelse till gärningarna. Det krävs därför inte några särskilda lagstiftningsåtgärder för att straffbelägga medverkan, försök och förberedelse till gärningarna.

Promemorians bedömning överensstämmer med regeringens bedömning.

Remissinstanserna har delat eller inte haft någon erinran mot bedömningen.

Skälen för regeringens bedömning: Enligt *artikel 5* skall anstiftan av och medhjälp till olagligt intrång i informationssystem, olaglig systemstörning och olaglig datastörning vara straffbelagt. Dessutom skall försök till de angivna brotten vara straffbart. Beträffande olagligt intrång i informationssystem får dock en medlemsstat besluta att inte straffbelägga försök till sådant brott. Enligt rambeslutet krävs inte heller att ringa fall av fullbordade brott straffbeläggs.

Av avsnitt 6.2.5 har framgått 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 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 nu föreslås kriminaliseras och som regeringen bedömer som straffvärda. Åtagandet i artikel 5 att straffbelägga försök till brotten får därigenom motsvarighet i svensk rätt. Det gäller dock inte ringa fall, som i dag är undantagna från den svenska försöksbestämmelsen. 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.

Förutom vad som nu sagts innebär de föreslagna kriminaliseringarna även att bestämmelsen om förberedelse till dataintrång blir tillämplig. Förberedelse till dataintrång är straffbart förutsatt att brottet inte skulle ha varit att anse som ringa om det hade fullbordats. En sådan utvidgning av det straffbara området är inte påkallad av rambeslutet. Emellertid måste förberedelse till de gärningar som nu föreslås bli kriminaliserade anses lika straffvärda som de fall av förberedelse till dataintrång som är straffbelagda redan i dag. Utvidgningen får därför anses motiverad.

8 Ikraftträdande

Regeringens förslag: Ändringarna i dataintrångsbestämmelsen träder i kraft den 1 juni 2007.

Promemorians förslag: I promemorian har föreslagits att lagändringarna skall träda i kraft den 1 januari 2007.

Remissinstanserna: Majoriteten av remissinstanserna har inte haft något att erinra mot förslaget. *SIG Security* har efterfrågat en mer flexibel formulering som gör det möjligt att låta ändringarna träda i kraft tidigare än den 1 januari 2007.

Skälen för regeringens förslag: Enligt *artikel 12* i rambeslutet skall medlemsstaterna vidta de åtgärder som är nödvändiga för att uppfylla bestämmelserna i rambeslutet senast den 16 mars 2007.

De föreslagna lagändringarna bör träda i kraft så snart som möjligt. Lagändringarna föreslås därför träda i kraft den 1 juni 2007.

Det krävs inte några särskilda övergångsbestämmelser för de föreslagna lagändringarna. Enligt 5 § brottsbalkens promulgationslag får nya straffrättsliga regler inte ges retroaktiv verkan till den tilltalades nackdel.

9 Kostnader

Förslagen i propositionen innebär att det straffbara området för dataintrång utvidgas. Utvidgningen är av begränsad omfattning.

Antalet ärenden och mål om dataintrång hos polis, åklagare och domstolar är i dag förhållandevis begränsat. 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, om några, för rättsväsendet. Eventuella merkostnader skall finansieras inom myndigheternas befintliga anslag.

10 Författningskommentar

Förslaget till lag om ändring i brottsbalken

4 kap.

9 c §

Paragrafen har genomgått såväl sakliga som redaktionella förändringar. De allmänna övervägandena finns i avsnitt 7.

Paragrafens *första mening* har ändrats i två avseenden. Dels har det s.k. upptagningsbegreppet i sin helhet (delar av nuvarande första meningen och andra meningen) i förtydligande syfte och för en språklig modernisering ersatts med begreppet ”uppgift som är avsedd för automatiserad behandling”, dels har det straffbara området utvidgats till att omfatta även den som olovligen *blockerar* en uppgift som är avsedd för automatiserad behandling.

Avsikten med det nya begreppet ”uppgift som är avsedd för automatiserad behandling” är att förtydliga att alla uppgifter, dvs. fakta, information eller begrepp, som uttrycks i en för en dator anpassad och läsbar form omfattas av bestämmelsen. I detta ligger att även program av olika slag omfattas. Det är för tillämpningen av begreppet utan betydelse var uppgifterna finns eller förvaras i systemet. Det innebär att alla uppgifter oavsett på vilket datamedium de finns omfattas. Därmed innefattas också uppgifter som finns i en dators temporära minne. Det innebär vidare att också uppgifter som är under befordran omfattas. Det senare gäller oavsett på vilket sätt befordran sker. Beträffande uppgifter som befordras via radio gäller dock som regel att avlyssning av sådan radiokommunikation faller utanför det straffbara området. Det följer av principen om att etern är fri och av att olovlighetskravet därmed inte kan anses uppfyllt. Detta har närmare kommenterats i avsnitt 7.2. Om intrånget däremot sker i radiobefordrade uppgifter som t.ex. är krypterade kan dock ansvar för dataintrång komma i fråga. Sådant ansvar kan också komma i fråga för ändring eller utplånande av eller annan påverkan på radiobefordrade uppgifter som anges i paragrafen.

Den brottsliga gärning som lagts till i första meningen beskrivs så att någon olovligen *blockerar* en uppgift som är avsedd för automatiserad behandling. Härmed skall förstås åtgärder som innebär att en sådan uppgift görs oåtkomlig eller att den hindras från att flöda. Det handlar alltså om hindrande eller spärrande åtgärder av olika slag. Som exempel kan nämnas inmatning eller spridning av olika typer av sabotageprogram (t.ex. datavirus, trojaner eller logiska bomber). Det kan t.ex. handla om situationer där en programkod förs in i en dator som fyller minnesutrymmet med ”skräp” så att uppgifterna inte kan nås eller som gör att uppgifterna inte kan lokaliseras. Om uppgifterna förändras eller förstörs, kan ansvar i stället komma i fråga för ändring eller utplånande av dessa.

En förutsättning för straffansvar är att gärningen – i likhet med vad som gäller för övriga i första meningen straffbelagda åtgärder – begås *uppsåtligen* och *olovligen*. Beträffande uppsåtskravet förutsätts inte att gärningsmannen handlar med ett direkt uppsåt att åstadkomma den angivna effekten – blockerar – utan alla uppsåtsformer är tillämpliga. Olovlighetsrekvisitet innebär att i och för sig blockerande åtgärder som sker med samtycke av den som har rätt att förfoga över uppgiften eller som någon vidtar i enlighet med sin behörighet eller befogenhet eller med stöd av gällande rätt faller utanför det straffbara området. Exempelvis är sedvanliga åtgärder som att testa ett systems säkerhet eller skydd eller att installera nya program, som vidtas av behöriga personer i enlighet med behörigheten, alltså inte att anse som olovliga. Olovlighetsrekvisitet har behandlats i avsnitten 6.1.2 och 7.1.

Andra meningen är ny och innebär en utvidgning av straffansvaret för dataintrång. Genom bestämmelsen föreskrivs straffansvar för den som olovligen genom någon annan liknande åtgärd *allvarligt stör eller hindrar användningen av* en uppgift som är avsedd för automatiserad behandling. Det straffbara förfarandet tar alltså sikte på åtgärder som verkar på ett sådant sätt att de stör eller hindrar att sådana uppgifter kan användas på avsett sätt. Som exempel på sådana åtgärder kan nämnas tillgänglighetsattacker eller överbelastningsattacker. Det kan t.ex. handla om program som skapar och sänder så stora mängder e-post att mottagarens system kollapsar eller får kraftigt nedsatt funktion och därmed hindrar eller stör användningen av de uppgifter som finns i systemet. En sådan effekt kan också uppkomma till följd av manuella sändningar av e-post i stor skala. Som ytterligare exempel på åtgärder som kan verka på ett sådant sätt kan nämnas upprepade anrop eller försök till anrop, införing av virusprogram eller annat sabotageprogram.

Med uttrycket ”allvarligt stör” avses att det skall vara frågan om en betydande störning av inte endast tillfällig natur. Bedömningen av om en sådan störning har förelegat skall göras utifrån en helhetsbedömning. Härvid kan bl.a. sådana omständigheter som hur lång tid störningen pågått, störningens art och dess omfattning vara av betydelse. Men också andra omständigheter kan komma i fråga för en sådan bedömning. Med uttrycket ”hindrar” avses sådana fall där användningen av en uppgift som är avsedd för automatiserad behandling helt avbryts eller förhindras. I det senare fallet torde dock som regel ansvar i stället inträda för blockering av en sådan uppgift. Om en allvarlig störning eller ett hindrande orsakas av flera personer, krävs att den enskilde har uppsåt till denna effekt för att ansvar skall komma i fråga.

Gärningsmannen skall ha åstadkommit den angivna effekten – allvarligt störande eller hindrande av användningen av en uppgift avsedd för automatiserad behandling – genom att använda sig av en ”annan liknande åtgärd”. De andra åtgärder som avses skall alltså till sin art vara jämförbara med de i första meningen omnämnda åtgärderna, i första hand ändra, utplåna, blockera eller i register föra in en uppgift som är avsedd för automatiserad behandling. Som exempel kan nämnas att överföra eller mata in en uppgift som är avsedd för automatiserad behandling.

Vidare förutsätts för straffansvar att gärningen sker olovligen. Olovlighetsrekvisitet har närmare kommenterats under första meningen.

Utanför det straffbara området faller rena opinionsyttringar som innebär att meddelanden med visst åsiktsinnehåll sänds, t.ex. med e-post, till en mottagare för att denne skall ta del av innehållet och eventuellt låta sig påverkas av det. Det innebär t.ex. att en situation där flera personer på ett samlat och koncentrerat sätt uttrycker en åsikt i e-post till en myndighet i sådan mängd att myndighetens datorsystem havererar eller annars orsakas en betydande funktionsnedsättning faller utanför kriminaliseringen, om inte den enskilde i själva verket agerat med uppsåt att åstadkomma de angivna effekterna. Kriminaliseringen träffar inte heller fall där någon genom t.ex. e-post gör bruk av sin grundlagsfästa meddelarfrihet. Detsamma gäller reklam i e-post, som regleras i marknadsföringslagen (1995:450).

Paragrafen är fortfarande subsidiär i förhållande till straffbestämmelserna i 4 kap. 8 och 9 §§ brottsbalken om brytande av post- eller telehemlighet och intrång i förvar. Utgångspunkten är i övrigt att sedvanliga konkurrensregler skall tillämpas. Det innebär normalt att när det är fråga om konkurrens mellan dataintrångsbrottet och ett annat brott med samma skyddsintresse skall domstolen döma enbart för det brott med den strängare straffskalan. För övriga konkurrenssituationer som kan förekomma får domstolen göra en prövning i varje enskilt fall enligt gällande konkurrensprinciper.

Försök och förberedelse till dataintrång som om det fullbordats inte skulle ha ansetts som ringa är straffbart enligt 4 kap. 10 § brottsbalken. Som exempel på förberedelse till dataintrång kan nämnas att ta befattning med en programvara som är konstruerad för att användas för att utföra tillgänglighetsattacker. Även att sammanställa uppgifter inför t.ex. en tillgänglighetsattack om aktuell adress, tidpunkt och annat av betydelse för brottets genomförande torde kunna föranleda ansvar för förberedelse till dataintrång förutsatt att informationen är nedtecknad eller på annat sätt lagrad och att faran för brottets fullbordan inte varit ringa. I ett fall som det senare torde försökspunkten i vart fall ha uppnåtts när t.ex. de enskilda e-postsändningarna har påbörjats. För ansvar för försök förutsätts därutöver att det föreligger fara för att handlingen skulle ha lett till brottets fullbordan eller att sådan fara varit utesluten endast på grund av tillfälliga omständigheter.

Medverkan till dataintrång är straffbelagt enligt bestämmelserna i 23 kap. brottsbalken.

RÅDETS RAMBESLUT 2005/222/RIF
av den 24 februari 2005
om angrepp mot informationssystem

EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA RAMBESLUT

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

med beaktande av kommissionens förslag,

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.

(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 eEurope, 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 träng-

[1] EUT C 300 E, 11.12.2003, s. 26.
[2] EGT C 43, 16.2.2002, s. 2.

ande behovet av ytterligare insatser för att tillnärma strafflagstiftningen på detta område.

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

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

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

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

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

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

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

(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.

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

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

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

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

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

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

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

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

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 skall kriminaliseras endast 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 datorbehandlingsba-

ra 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 organisa-

tion 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) frånatagande av rätt till offentliga förmåner eller stöd,

b) tillfälligt eller permanent näringsförbud,

c) rättslig övervakning, eller

d) rättsligt beslut om upplösning av verksamheten.

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

Artikel 10

Behörighet

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

a) helt eller delvis på dess territorium, eller

b) av en av dess medborgare, eller

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

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

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

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

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

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

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

— Medlemsstaten skall vara den i vilken gärningsmannen är medborgare.

— Medlemsstaten skall vara den på vars territorium gärningsmannen påträffats.

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

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

Artikel 11

Utbyte av uppgifter

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

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

Artikel 12

Genomförande

1. Medlemsstaterna skall vidta de åtgärder som är nödvändiga för att följa bestämmelserna i detta rambeslut senast den 16 mars 2007.

2. Senast den 16 mars 2007 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 16 september 2007 skall rådet, på grundval av en rapport som skall utarbetas utifrån information och en skriftlig rapport från kommissionen, bedöma i vilken utsträckning medlemsstaterna har följt bestämmelserna i detta rambeslut.

Artikel 13

Ikraftträdande

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

Utfärdat i Bryssel den 24 februari 2005.

På rådets vägnar
N. SCHMIT
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.

Sammanfattning av departementspromemorian Angrepp mot informationssystem (Ds 2005:5)

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.

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 som är avsedda* för *automatiserad* databehandling.

Denna lag träder i kraft den 1 januari 2007.

[1] Senaste lydelse 1998:206.

Förteckning över remissinstanserna

Efter remiss har yttrande över promemorian avgetts av Riksdagens ombudsmän, Svea hovrätt, Hovrätten för Nedre Norrland, Helsingborgs tingsrätt, Hässleholms tingsrätt, Göteborgs tingsrätt, Justitiekanslern, Domstolsverket, Åklagarmyndigheten, Rikspolisstyrelsen, Säkerhetspolisen, Brottsförebyggande rådet, Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt, Krisberedskapsmyndigheten, Datainspektionen, Statskontoret, Juridiska fakultetsnämnden vid Stockholms universitet, Juridiska fakultetsnämnden vid Uppsala universitet, Radio- och TV-verket, Post- och telestyrelsen, Sveriges advokatsamfund, Svenskt Näringsliv, Sveriges domareförbund, Svenska IT-företagens Organisation AB och SIG Security.

Lagrådets yttrande

Utdrag ur protokoll vid sammanträde 2007-02-23

Närvarande: f.d. regeringsrådet Bengt-Åke Nilsson, regeringsrådet Stefan Ersson och justitierådet Lars Dahllöf.

Angrepp mot informationssystem

Enligt en lagrådsremiss den 15 februari 2007 (Justitiedepartementet) har regeringen beslutat inhämta Lagrådets yttrande över förslag till lag om ändring i brottsbalken.

Förslaget har inför Lagrådet föredragits av hovrättsassessorn Gunilla Berglund.

Lagrådet lämnar förslaget utan erinran.

Justitiedepartementet

Utdrag ur protokoll vid regeringssammanträde den 8 mars 2007

Närvarande: Statsrådet Olofsson, ordförande, statsråden Bildt, Ask, Husmark Pehrsson, Odenberg, Larsson, Erlandsson, Torstensson, Carlgren, Hägglund, Björklund, Carlsson, Littorin, Borg, Malmström, Sabuni, Billström, Adelsohn Liljeroth, Tolgfors

Föredragande: statsrådet Ask

Regeringen beslutar proposition 2006/07:66 Angrepp mot informationssystem