EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV 2013/40/EU

av den 12 augusti 2013

om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 83.1,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ([1]),

i enlighet med det ordinarie lagstiftningsförfarandet ([2]), och

av följande skäl:

(1) Målen för detta direktiv är att tillnärma medlemsstaternas straffrättsliga lagstiftning vad gäller angrepp mot informationssystem, genom att fastställa minimiregler om fastställande av brottsrekvisit och påföljder, och att förbättra samarbetet mellan behöriga myndigheter, inbegripet polismyndigheter och andra specialiserade brottsbekämpande organ i medlemsstaterna samt behöriga specialiserade unionsbyråer och -organ såsom Eurojust, Europol och dess europeiska it-brottscentrum samt Europeiska byrån för nät- och informationssäkerhet (Enisa).

(2) Informationssystem är av central betydelse för det politiska, sociala och ekonomiska samspelet i unionen. Samhället är i högsta grad och i växande utsträckning beroende av sådana system. Att dessa system fungerar smidigt och säkert i unionen är en förutsättning för utvecklingen av den inre marknaden och för en konkurrenskraftig och innovativ ekonomi. Säkerställande av en lämplig skyddsnivå för informationssystem bör ingå i ett effektivt övergripande ramverk med förebyggande åtgärder, tillsammans med straffrättsliga åtgärder mot it-relaterad brottslighet.

(3) Angrepp mot informationssystem, särskilt angrepp som är kopplade till organiserad brottslighet, är ett växande problem både inom unionen och på global nivå, och oron ökar för terroristattacker eller politiskt motiverade angrepp mot de informationssystem som ingår i medlemsstaternas och unionens kritiska infrastruktur. Detta utgör ett hot mot arbetet för att skapa ett säkrare informationssamhälle och ett område med frihet, säkerhet och rättvisa och kräver därför åtgärder på unionsnivå och bättre samarbete och samordning på internationell nivå.

(4) Inom unionen finns det en rad kritiska infrastrukturer för vilka driftstörningar, eller vars förstörelse, skulle kunna få betydande gränsöverskridande konsekvenser. Det har visat sig att behovet av att förbättra förmågan att skydda kritisk infrastruktur i unionen innebär att åtgärderna mot angrepp mot informationssystem bör kompletteras med stränga straffrättsliga påföljder som återspeglar angreppens svårhetsgrad. Med kritisk infrastruktur kan avses anläggningar, system eller delar av dessa belägna i medlemsstaterna som är nödvändiga för att upprätthålla centrala samhällsfunktioner, hälsa, säkerhet, trygghet och människors ekonomiska eller sociala välfärd, såsom kraftverk, transportnät eller myndighetsnätverk, och där störningar i driften eller förstörelse av dessa skulle få betydande konsekvenser i en medlemsstat till följd av att man inte lyckas upprätthålla dessa funktioner.

(5) Det finns tecken på en utveckling mot allt farligare och återkommande storskaliga angrepp mot informationssystem som ofta är av vital betydelse för medlemsstater eller särskilda funktioner i den offentliga eller privata sektorn. Denna tendens är förenad med utvecklingen av alltmer sofistikerade metoder, såsom skapande och användning av s.k. botnät, som omfattar flera skeden i en brottslig gärning, där varje skede i sig kan utgöra ett allvarligt hot mot allmänna intressen. Detta direktiv syftar bland annat till att införa straffrättsliga påföljder för skapandet av botnät, det vill säga övertagande och fjärrstyrning av ett stort antal datorer genom att infektera dem via sabotageprogram genom riktade it-angrepp. När de väl har skapats kan de infekterade datorerna, som utgör botnätet, utan användarnas vetskap aktiveras för storskaliga it-angrepp, som i allmänhet kan orsaka allvarlig skada, på det sätt som avses i detta direktiv. Medlemsstaterna får fastställa vad som utgör allvarlig skada enligt deras nationella rätt och praxis, exempelvis störning av systemtjänster av stort allmänintresse, orsakande av stora ekonomiska kostnader eller förlust av personuppgifter eller känslig information.

(6) Storskaliga it-angrepp kan orsaka betydande ekonomiska skador på grund av avbrott i informationssystemens drift och i kommunikationen och förlust eller förvanskning av hemlig information som är viktig ur kommersiell synpunkt eller andra uppgifter. Särskild uppmärksamhet bör ägnas åt att öka medvetenheten hos innovativa små och medelstora företag om vilka hot sådana angrepp utgör och deras sårbarhet för angrepp av detta slag, med tanke på att de i allt större utsträckning är beroende av att informationssystem fungerar korrekt och är tillgängliga, och de ofta begränsade resurser de har för informationssäkerhet.

([1]) EUT C 218, 23.7.2011, s. 130.

([2]) Europaparlamentets ståndpunkt av den 4 juli 2013 (ännu ej offentliggjord i EUT) och rådets beslut av den 22 juli 2013.

(7) Gemensamma definitioner på detta område är viktiga för att säkerställa att detta direktiv tillämpas enhetligt i medlemsstaterna.

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

(9) Avlyssning omfattar, men är inte nödvändigtvis begränsad till, avlyssning, kontroll eller övervakning av kommunikationsinnehåll och anskaffande av uppgifter, antingen direkt genom åtkomst till och användning av informationssystem eller indirekt med tekniska hjälpmedel, genom användning av olika typer av elektroniska avlyssningsanordningar eller avlyssning med tekniska hjälpmedel.

(10) Medlemsstaterna bör fastställa påföljder för angrepp mot informationssystem. De påföljder som fastställs bör vara effektiva, proportionella och avskräckande och bör inbegripa fängelsestraff och/eller böter.

(11) I detta direktiv föreskrivs straffrättsliga påföljder åtminstone i fall som inte är ringa. Medlemsstaterna får fastställa vad som utgör ett ringa fall enligt deras nationella rätt och praxis. Ett fall kan anses vara ringa till exempel när den skada och/eller risk som gärningen medför för offentliga eller privata intressen, såsom ett datasystems eller datorbehandlingsbara uppgifters integritet eller en persons integritet, rättigheter och andra intressen, är obetydlig eller av sådan art att åläggande av straffrättsliga påföljder inom den lagstadgade gränsen eller åläggande av straffrättsligt ansvar inte är nödvändigt.

(12) Identifiering och rapportering av hot och risker från it-angrepp och svagheter i informationssystem bör ingå i ett effektivt förebyggande av och effektiva åtgärder mot it-angrepp och för att förbättra säkerheten i informationssystem. Effekten kan förstärkas genom incitament att rapportera säkerhetsbrister. Medlemsstaterna bör sträva efter att ge i lag föreskrivna möjligheter att upptäcka och rapportera säkerhetsbrister.

(13) Det är lämpligt att föreskriva strängare påföljder när ett angrepp mot ett informationssystem görs inom ramen för en sådan kriminell organisation som avses i rådets rambeslut 2008/841/RIF av den 24 oktober 2008 om kampen mot organiserad brottslighet ([1]), när it-angreppet är storskaligt och därmed påverkar ett betydande antal informationssystem, inklusive när angreppet syftar till att skapa ett botnät, eller när it-angreppet orsakar allvarlig skada, inklusive när det genomförs via ett botnät. Det är också lämpligt att föreskriva strängare påföljder när ett sådant angrepp riktas mot kritisk infrastruktur i medlemsstaterna eller unionen.

(14) Införandet av effektiva åtgärder mot identitetsstöld och andra identitetsrelaterade brott utgör en annan viktig del i en samlad ansats mot it-relaterad brottslighet. Behovet av unionsåtgärder mot denna typ av brottsligt beteende kan också övervägas vid utvärderingen av behovet av ett övergripande horisontellt unionsinstrument.

(15) Enligt rådets slutsatser av den 27–28 november 2008 bör det utarbetas en ny strategi i samarbete med medlemsstaterna och kommissionen, med hänsyn till Europarådets konvention från 2001 om it-relaterad brottslighet. Konventionen är den viktigaste rättsliga referensramen när det gäller att bekämpa it-relaterad brottslighet, inklusive angrepp mot informationssystem. Detta direktiv bygger på den konventionen. Det bör därför ses som en prioritet att alla medlemsstater slutför ratificeringen av konventionen så snart som möjligt.

(16) Med hänsyn till de olika metoder som kan användas för att angripa informationssystem och till den snabba utvecklingen av hård- och programvara, hänvisar detta direktiv till verktyg som kan användas för att begå brott som anges i detta direktiv. Verktyg i denna mening är exempelvis sabotageprogram, inklusive sådana som kan skapa botnät, som används för it-angrepp. Även om ett verktyg är lämpat eller särskilt lämpat för att utföra ett av de brott som anges i detta direktiv kan verktyget vara tillverkat för lagliga ändamål. Eftersom det finns ett behov av att undvika kriminalisering av fall där sådana verktyg tillverkas och saluförs för lagliga ändamål, t.ex. för test av it-produkters funktionssäkerhet eller informationssystems säkerhet, måste, utöver det allmänna kravet på uppsåt, också ett krav på direkt uppsåt uppfyllas, att dessa verktyg är avsedda att användas för att begå ett eller flera av de brott som anges i detta direktiv.

(17) Detta direktiv ålägger inte straffrättsligt ansvar när de objektiva kriterier för brott som anges i detta direktiv är uppfyllda men då gärningarna begås utan brottsligt uppsåt, till exempel när en person inte visste att det rörde sig om obehörig åtkomst eller vid föreskrivna test eller skydd av informationssystem, till exempel när en person har fått i uppdrag av ett företag eller en leverantör att testa styrkan hos dess säkerhetssystem. Avtalsenliga skyldigheter eller överenskommelser om att begränsa åtkomst till informationssystem genom en användarpolicy eller användarvillkor samt arbetsmarknadstvister om åtkomst till och användning av arbetsgivarens informationssystem för privata ändamål, bör inte föranleda straffrättsligt ansvar enligt detta direktiv, om åtkomsten under dessa omständigheter skulle bedömas vara otillåten och således utgöra den enda grunden för lagföring. Detta direktiv påverkar inte den rätt till åtkomst till information som följer av nationell rätt och unionsrätt, men får samtidigt inte fungera som undantag för att motivera olaglig och godtycklig åtkomst till information.

([1]) EUT L 300, 11.11.2008, s. 42.

(18) It-angrepp kan underlättas av olika omständigheter, till exempel när förövaren har åtkomst till de säkerhetssystem som är inbyggda i de drabbade informationssystemen i tjänsten. Inom ramen för nationell rätt bör sådana omständigheter på lämpligt sätt beaktas vid lagföring.

(19) Medlemsstaternas nationella rätt bör innehålla regler om försvårande omständigheter i enlighet med de tillämpliga regler om försvårande omständigheter som fastställts genom deras rättsystem. De bör se till att rätten vid påföljdsbestämningen har möjlighet ta hänsyn till dessa försvårande omständigheter. Det är upp till rätten att bedöma dessa omständigheter, tillsammans med övriga faktiska sakomständigheter i det enskilda fallet.

(20) Detta direktiv reglerar inte villkoren för utövandet av behörighet när det gäller de brott som avses i direktivet, exempelvis att det ska föreligga en anmälan från offret på den plats där brottet begicks, en formell underrättelse från den stat där brottet begicks, eller att åtal inte väckts mot gärningsmannen på den plats där gärningen har begåtts.

(21) Stater och offentliga organ är, inom ramen för detta direktiv, skyldiga att till fullo garantera respekten för de mänskliga rättigheterna och grundläggande friheterna, i enlighet med gällande internationella förpliktelser.

(22) Genom detta direktiv stärks betydelsen av nätverk, såsom G8 eller Europarådets nätverk av kontaktpunkter, som är tillgängliga dygnet runt alla dagar i veckan. Sådana kontaktpunkter bör kunna ge konkret stöd och till exempel underlätta utbyte av tillgänglig relevant information och tillhandahålla teknisk rådgivning eller rättslig information i utredningar eller rättegångar rörande brott med anknytning till informationssystem och data som rör den begärande medlemsstaten. För att säkerställa att nätverken fungerar smidigt bör varje kontaktpunkt kunna kommunicera med kontaktpunkter i andra medlemsstater omgående, bland annat med hjälp av utbildad och utrustad personal. Med hänsyn till hur snabbt storskaliga it-angrepp kan genomföras, bör medlemsstaterna ha kapacitet att snabbt besvara brådskande förfrågningar från detta nät av kontaktpunkter. I sådana fall kan det vara lämpligt att förfrågan om information åtföljs av en telefonkontakt, för att se till att den anmodade medlemsstaten behandlar förfrågan snabbt och ger återkoppling inom åtta timmar.

(23) Samarbete mellan, å ena sidan, de offentliga myndigheterna och, å andra sidan, den privata sektorn och det civila samhället är mycket viktigt för att förebygga och motverka angrepp mot informationssystem. Det är nödvändigt att främja och förbättra samarbetet mellan tjänsteleverantörer, producenter, brottsbekämpande organ och rättsliga myndigheter samtidigt som rättsstatsprincipen beaktas fullt ut. Samarbetet kan inbegripa t.ex. stöd från tjänsteleverantörernas sida när det gäller att säkra potentiella bevis, bidra till fastställandet av gärningsmännens identitet och, som en sista utväg, i enlighet med nationell rätt och praxis, helt eller delvis stänga ned informationssystem eller funktioner som har angripits eller använts för olagliga ändamål. Medlemsstaterna bör också överväga att inrätta nätverk för samarbete och partnerskap med tjänsteleverantörer och producenter för utbyte av uppgifter om de brott som omfattas av detta direktiv.

(24) Det finns behov av att samla in jämförbara uppgifter om de brott som avses i detta direktiv. Relevanta uppgifter bör göras tillgängliga för behöriga specialiserade unionsbyråer och -organ, t.ex. Europol och Enisa i enlighet med deras uppdrag och informationsbehov, för att få en mer heltäckande bild av problemet med it-relaterad brottslighet och nätverks- och informationssäkerhet på unionsnivå och därigenom medverka till utformningen av mer effektiva åtgärder. Medlemsstaterna bör översända uppgifter om gärningsmännens tillvägagångssätt till Europol och dess europeiska it-brottscentrum för utarbetande av hotbedömningar och strategiska analyser i samband med it-relaterad brottslighet i enlighet med rådets beslut 2009/371/RIF av den 6 april 2009 om inrättande av Europeiska polisbyrån (Europol) ([1]). Tillhandahållandet av information kan bidra till bättre insikt om nuvarande och framtida hot och därmed bidra till att bättre och mer målinriktade beslut fattas om bekämpande och förebyggande av angrepp mot informationssystem.

(25) Kommissionen bör överlämna en rapport om tillämpningen av detta direktiv och lägga fram nödvändiga förslag till lagstiftning som skulle kunna leda till att dess tillämpningsområde utvidgas med hänsyn till utvecklingen på området för it-relaterad brottslighet. Exempel på sådan utveckling är tekniska lösningar som till exempel möjliggör en effektivare bekämpning av angrepp mot informationssystem, eller som gör det lättare att förebygga eller minimera konsekvenserna av sådana angrepp. Kommissionen bör för detta ändamål beakta tillgängliga analyser och rapporter som utarbetats av relevanta aktörer, särskilt Europol och Enisa.

(26) För att man effektivt ska kunna bekämpa it-relaterad brottslighet är det nödvändigt att öka informationssystemens motståndskraft genom lämpliga åtgärder för att bättre skydda dem mot it-angrepp. Medlemsstaterna bör vidta nödvändiga åtgärder för att skydda de informationssystem som utgör del av deras kritiska infrastruktur från it-angrepp, och skyddet av deras informationssystem med tillhörande data bör ingå i det. En viktig del i en heltäckande strategi för att effektivt motverka it-relaterad brottslighet är att se till att juridiska personer har en tillräckligt hög skydds- och säkerhetsnivå på informationssystem, t.ex. i samband med tillhandahållande av offentligt tillgängliga elektroniska kommunikationstjänster i enlighet med gällande unionslagstiftning om integritet och elektronisk kommunikation samt om

([1]) EUT L 121, 15.5.2009, s. 37.

dataskydd. Lämpliga skyddsnivåer bör tillhandahållas mot hot och svagheter som på ett rimligt sätt kan identifieras i enlighet med den senaste utvecklingen inom den specifika sektorn och de konkreta situationerna för databehandlingen. De kostnader och bördor som ett sådant skydd medför bör stå i proportion till den sannolika skadan av ett it-angrepp för de drabbade. Medlemsstaterna uppmanas att fastställa relevanta åtgärder i fråga om ansvar inom ramen för nationell rätt när det är uppenbart att en juridisk person inte har haft en lämplig skyddsnivå mot it-angrepp.

(27) Stora luckor och skillnader i medlemsstaternas lagstiftning och straffrättsliga förfaranden när det gäller angrepp mot informationssystem kan försvåra kampen mot organiserad brottslighet och terrorism, och kan komplicera ett effektivt polisiärt och rättsligt samarbete på detta område. De moderna informationssystemens nationsöverskridande och gränslösa natur innebär att angrepp mot sådana system ofta har en gränsöverskridande dimension, vilket understryker det akuta behovet av ytterligare insatser för att tillnärma den straffrättsliga lagstiftningen på detta område. För övrigt bör adekvata åtgärder för genomförande och tillämpning av rådets rambeslut 2009/948/RIF av den 30 november 2009 om förebyggande och lösning av tvister om utövande av jurisdiktion i straffrättsliga förfaranden [1] göra det lättare att samordna åtal i fall av angrepp mot informationssystem. Medlemsstaterna bör också i samarbete med unionen verka för bättre internationellt samarbete i fråga om säkerheten i informationssystem, datornätverk och datorbehandlingsbara uppgifter. Vederbörlig hänsyn till säkerheten vid dataöverföring och lagring av uppgifter bör tas med i alla internationella avtal som rör uppgiftsutbyte.

(28) Bättre samarbete mellan behöriga brottsbekämpande organ och rättsliga myndigheter i hela unionen är nödvändigt för att man ska kunna bekämpa it-relaterad brottslighet på ett effektivt sätt. I detta sammanhang bör ökade insatser för att ge adekvat utbildning till de berörda myndigheterna för ökad förståelse av it-relaterad brottslighet och dess konsekvenser, och för att främja samarbete och utbyte av bästa metoder, exempelvis genom de behöriga specialiserade unionsbyråerna och -organen, uppmuntras. Sådan utbildning bör bland annat syfta till att öka medvetenheten om de olika nationella rättssystemen, de eventuella rättsliga och tekniska svårigheter som kan uppstå vid brottsutredningar eller fördelningen av befogenheter mellan de relevanta nationella myndigheterna.

(29) Detta direktiv respekterar de mänskliga rättigheterna och de grundläggande friheterna och står i överensstämmelse med de principer som erkänns särskilt i Europeiska unionens stadga om de grundläggande rättigheterna och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, inklusive skyddet av personuppgifter, rätten till privatliv, yttrande- och informationsfrihet, rätten till en rättvis rättegång, oskuldspresumtion och rätten till försvar, samt med legalitetsprincipen och principen om proportionalitet mellan brottet och påföljden. Detta direktiv syftar särskilt till att säkerställa att dessa rättigheter och principer respekteras fullt ut och måste genomföras i enlighet med detta.

(30) Skyddet av personuppgifter är en grundläggande rättighet i enlighet med artikel 16.1 i EUF-fördraget och artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Därför bör all behandling av personuppgifter i samband med genomförandet av detta direktiv vara helt och hållet förenlig med den unionsrätt som gäller beträffande uppgiftsskydd.

(31) I enlighet med artikel 3 i protokollet om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, har dessa medlemsstater meddelat att de önskar delta i antagandet och tillämpningen av detta direktiv.

(32) I enlighet med artiklarna 1 och 2 i protokollet om Danmarks ställning, fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, deltar Danmark inte i antagandet av detta direktiv, som inte är bindande för eller tillämpligt på Danmark.

(33) Eftersom målen för detta direktiv, nämligen att underställa angrepp mot informationssystem i alla medlemsstater effektiva, proportionella och avskräckande straffrättsliga påföljder och att förbättra och uppmuntra samarbete mellan rättsliga och andra behöriga myndigheter, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna, och de därför bättre kan uppnås på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går detta direktiv inte utöver vad som är nödvändigt för att uppnå dessa mål.

(34) Syftet med detta direktiv är att ändra och utöka bestämmelserna i rådets rambeslut 2005/222/RIF av den 24 februari 2005 om angrepp mot informationssystem [2]. Med avseende på de medlemsstater som deltar i antagandet av detta direktiv bör rambeslut 2005/222/RIF för tydlighetens skull ersättas i sin helhet, eftersom de ändringar som görs är många och väsentliga.

[1] EUT L 328, 15.12.2009, s. 42.

[2] EUT L 69, 16.3.2005, s. 67.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Syfte

Detta direktiv fastställer minimiregler om fastställande av brottsrekvisit och påföljder inom området angrepp mot informationssystem. Det syftar också till att främja förebyggande av sådana brott och förbättra samarbetet mellan rättsliga och andra behöriga myndigheter.

Artikel 2

Definitioner

I detta direktiv avses med

a) *informationssystem:* en apparat eller en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program automatiskt behandlar datorbehandlingsbara uppgifter, samt datorbehandlingsbara uppgifter som lagras, behandlas, hämtas eller överförs med hjälp av en apparat eller en grupp av apparater för att de ska 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 status av juridisk person enligt tillämplig rätt, med undantag av stater, eller offentliga organ vid utövandet av de befogenheter som de har i egenskap av statsmakter samt internationella offentliga organisationer,

d) *orättmätigt:* handlande som avses i detta direktiv, inklusive intrång, störning eller avlyssning, utan tillstånd från ägaren eller annan rättighetshavare till systemet eller del av detta, eller som inte är tillåtet enligt nationell rätt.

Artikel 3

Olagligt intrång i informationssystem

Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att orättmätigt intrång som begås uppsåtligen i ett informationssystem som helhet eller en del av ett sådant system straffbeläggs när det begås genom intrång i en säkerhetsåtgärd och åtminstone i fall som inte är ringa.

Artikel 4

Olaglig systemstörning

Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att det är 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.

Artikel 5

Olaglig datastörning

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

Artikel 6

Olaglig avlyssning

Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att avlyssning med tekniska hjälpmedel, som sker uppsåtligen och orättmätigt, av icke-offentliga överföringar av datorbehandlingsbara uppgifter till, från eller inom ett informationssystem, inklusive elektromagnetisk strålning från informationssystem som innehåller sådana uppgifter, straffbeläggs, åtminstone i fall som inte är ringa.

Artikel 7

Verktyg som används för att begå brott

Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att det är straffbart att uppsåtligen tillverka, sälja, anskaffa i syfte att använda, importera, distribuera eller på annat sätt tillgängliggöra ett av följande verktyg, om det sker orättmätigt och med uppsåt att begå något av de brott som avses i artiklarna 3–6, åtminstone i fall som inte är ringa:

a) Ett datorprogram som utformats eller anpassats i första hand för att begå något av de brott som avses i artiklarna 3–6.

b) Ett datorlösenord, en åtkomstkod eller liknande uppgifter som gör det möjligt att få tillgång till ett informationssystem eller delar av ett sådant system.

Artikel 8

Anstiftan, medhjälp och försök

1. Medlemsstaterna ska se till att anstiftan av och medhjälp till de brott som avses i artiklarna 3–7 straffbeläggs.

2. Medlemsstaterna ska se till att försök att begå de brott som avses i artiklarna 4 och 5 straffbeläggs.

Artikel 9

Påföljder

1. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att de brott som avses i artiklarna 3–8 är belagda med effektiva, proportionella och avskräckande straffrättsliga påföljder.

2. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att de brott som avses i artiklarna 3–7 är belagda med ett maximistraff på minst två års fängelse, åtminstone i fall som inte är ringa.

3. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att de brott som avses i artiklarna 4 och 5 är belagda med ett maximistraff på minst tre års fängelse när de

begås uppsåtligen och när ett betydande antal informationssystem har påverkats genom användning av ett verktyg som avses i artikel 7 och som har utformats eller anpassats i första hand för detta syfte.

4. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att de brott som avses i artiklarna 4 och 5 är belagda med ett maximistraff på minst fem års fängelse när de

a) begås inom ramen för en kriminell organisation enligt definitionen i rambeslut 2008/841/RIF, oberoende av den påföljdsnivå som föreskrivs däri, eller

b) förorsakar allvarlig skada, eller

c) begås mot ett informationssystem som utgör kritisk infrastruktur.

5. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att det i enlighet med nationell rätt kan anses som en försvårande omständighet, när de brott som avses i artiklarna 4 och 5 begås genom missbruk av personuppgifter som rör en annan person än gärningsmannen i syfte att vinna tredje mans förtroende och därigenom medför skada för den som identiteten tillhör, om inte dessa omständigheter redan täcks av ett annat brott som är straffbart enligt nationell rätt.

Artikel 10

Juridiska personers ansvar

1. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att juridiska personer kan ställas till ansvar för de brott som avses i artiklarna 3–8 och som begås till deras förmån av en person som agerar antingen enskilt eller som en del av den juridiska personens organisation och har en ledande ställning inom den juridiska personen, grundad på något av följande:

a) Behörighet att företräda den juridiska personen.

b) Befogenhet att fatta beslut på den juridiska personens vägnar.

c) Befogenhet att utöva kontroll inom den juridiska personen.

2. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att juridiska personer kan ställas till ansvar när brister i övervakning eller kontroll som ska 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 något av de brott som avses i artiklarna 3–8.

3. Juridiska personers ansvar enligt punkterna 1 och 2 ska inte utesluta lagföring av fysiska personer som begår, anstiftar eller medverkar till något av de brott som avses i artiklarna 3–8.

Artikel 11

Påföljder för juridiska personer

1. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att en juridisk person som har fällts till ansvar enligt artikel 10.1 kan bli föremål för effektiva, proportionella och avskräckande påföljder, som ska innefatta bötesstraff eller administrativa avgifter och som får inbegripa andra påföljder, som

a) fråntagande av rätt till offentliga förmåner eller stöd,

b) tillfälligt eller permanent näringsförbud,

c) rättslig övervakning,

d) rättsligt beslut om upplösning av verksamheten,

e) tillfällig eller permanent stängning av inrättningar som har använts för att begå brottet.

2. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att en juridisk person som har fällts till ansvar enligt artikel 10.2 kan bli föremål för effektiva, proportionella och avskräckande påföljder eller andra åtgärder.

Artikel 12

Behörighet

1. Medlemsstaterna ska fastställa sin behörighet beträffande de brott som avses i artiklarna 3–8, när brottet har begåtts

a) helt eller delvis på deras territorium, eller

b) av en medborgare i medlemsstaten, åtminstone i sådana fall där gärningen utgör ett brott på den plats där den begicks.

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

a) gärningsmannen är fysiskt närvarande på dess 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 dess territorium, oavsett om gärningsmannen är fysiskt närvarande på territoriet när brottet begås eller inte.

3. En medlemsstat ska underrätta kommissionen om den beslutar att fastställa sin behörighet över ett brott som avses i artiklarna 3–8 vilket har begåtts utanför dess territorium, inbegripet när

a) gärningsmannen har sin hemvist på denna medlemsstats territorium, eller

b) gärningen har begåtts till förmån för en juridisk person som är etablerad inom denna medlemsstats territorium.

Artikel 13

Informationsutbyte

1. För utbyte av uppgifter om de brott som avses i artiklarna 3–8 ska medlemsstaterna se till att ha en operativ nationell kontaktpunkt och att använda det befintliga nät med operativa kontaktpunkter som kan nås dygnet runt alla dagar i veckan. Medlemsstaterna ska också se till att ha förfaranden som gör att de vid brådskande begäran om bistånd inom högst åtta timmar efter mottagandet kan ange åtminstone huruvida begäran kommer att besvaras samt formen och den beräknade tidpunkten för svaret.

2. Medlemsstaterna ska underrätta kommissionen om sin utsedda kontaktpunkt som avses i punkt 1. Kommissionen ska vidarebefordra denna information till de andra medlemsstaterna och behöriga specialiserade unionsbyråer och -organ.

3. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att lämpliga rapporteringskanaler är tillgängliga för att underlätta att de brott som avses i artiklarna 3–6 rapporteras till behöriga nationella myndigheter utan onödigt dröjsmål.

Artikel 14

Övervakning och statistik

1. Medlemsstaterna ska se till att det finns ett system för registrering, insamling och tillhandahållande av statistiska uppgifter om de brott som avses i artiklarna 3–7.

2. De statistiska uppgifter som avses i punkt 1 ska åtminstone omfatta befintliga uppgifter om antalet sådana brott som avses i artiklarna 3–7 som registrerats av medlemsstaterna och antalet personer som åtalats och dömts för sådana brott som avses i artiklarna 3–7.

3. Medlemsstaterna ska översända de uppgifter som samlas in enligt denna artikel till kommissionen. Kommissionen ska se till att en samlad översikt över dessa statistiska rapporter offentliggörs och översänds till behöriga specialiserade unionsbyråer och -organ

Artikel 15

Ersättande av rambeslut 2005/222/RIF

Rambeslut 2005/222/RIF ersätts härmed med avseende på medlemsstater som deltar i antagandet av detta direktiv, utan att detta påverkar medlemsstaternas skyldigheter vad gäller tidsfristen för införlivande av rambeslutet med nationell rätt.

Med avseende på de medlemsstater som deltar i antagandet av detta direktiv ska hänvisningar till rambeslut 2005/222/RIF anses som hänvisningar till detta direktiv.

Artikel 16

Införlivande

1. Medlemsstaterna ska senast den 4 september 2015 sätta i kraft de lagar och andra författningar som är nödvändiga för att följa detta direktiv.

2. Medlemsstaterna ska till kommissionen överlämna texten till de bestämmelser genom vilka skyldigheterna enligt detta direktiv införlivas med deras nationella lagstiftning.

3. När en medlemsstat antar dessa bestämmelser ska de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen ska göras ska varje medlemsstat själv utfärda.

Artikel 17

Rapportering

Kommissionen ska senast den 4 september 2017 överlämna en rapport till Europaparlamentet och rådet med en utvärdering av i vilken utsträckning medlemsstaterna har vidtagit de åtgärder som är nödvändiga för att följa detta direktiv, vid behov åtföljd av lagstiftningsförslag. Kommissionen ska även beakta den tekniska och rättsliga utvecklingen på området för it-relaterad brottslighet, särskilt vad gäller tillämpningsområdet för detta direktiv.

Artikel 18

Ikraftträdande

Detta direktiv träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Artikel 19

Adressater

Detta direktiv riktar sig till medlemsstaterna i enlighet med fördragen.

Utfärdat i Bryssel den 12 augusti 2013.

På Europaparlamentets vägnar	*På rådets vägnar*
M. SCHULZ	L. LINKEVIČIUS
Ordförande	*Ordförande*