# Regeringskansliet
# Faktapromemoria 2010/11:FPM15

# Direktiv om angrepp mot informationssystem

Justitiedepartementet

2010-11-04

## Dokumentbeteckning

KOM (2010) 517
Förslag till Europaparlamentets och rådets direktiv om angrepp mot informationssystem och om upphävande av rambeslut 2005/222/RIF

## Sammanfattning

Direktivförslaget, som avser att ersätta rambeslutet om angrepp mot informationssystem (2005/222/RIF), syftar till att ytterligare tillnärma medlemsstaternas strafflagstiftning på området för angrepp mot informationssystem. Vidare är avsikten att förbättra samarbetet mellan rättsliga och andra behöriga myndigheter, inbegripet polismyndigheter och andra specialiserade brotts-bekämpande organ i medlemsstaterna.

Förslaget bygger i stora delar på rambeslutet från 2005 men innehåller också bestämmelser om utvidgad kriminalisering av angrepp mot informationssystem, liksom av anstiftan av och medhjälp och försök till sådana brott. Vidare föreslås skärpta lägsta maximistraff och utvidgade regler om försvårande omständigheter. I övrigt innehåller initiativet regler om ansvar och sanktioner för juridiska personer, utvidgad jurisdiktion, utbyte av uppgifter samt statistik.

Regeringen välkomnar initiativet till fortsatt arbete inom EU i syfte att ytterligare förstärka arbetet med att motverka och bekämpa angrepp mot informationssystem. Det finns dock skäl att i vissa delar noggrant analysera förslagets bestämmelser, bl.a. i fråga om de nya handlingar som ska utgöra brott, straffnivåer och försvårande omständigheter.

# 1 Förslaget

## 1.1 Ärendets bakgrund

Inom EU antogs i februari 2005 ett rambeslut om angrepp mot informationssystem (2005/222/RIF). Syftet med rambeslutet var att närma medlemsstaternas straffrättsliga lagstiftning till varandra när det gäller angrepp mot informationssystem och därigenom förbättra samarbetet mellan rättsliga och andra myndigheter. Rambeslutet omfattar åtaganden att kriminalisera olagligt intrång i informationssystem, olaglig systemstörning och olaglig datastörning, liksom anstiftan, medhjälp och försök. Det reglerar även vilka straffrättsliga påföljder som gärningarna ska kunna leda till. Vidare finns bestämmelser om försvårande omständigheter, ansvar och sanktioner för juridiska personer, behörighet samt utbyte av uppgifter. Svenska lagändringar med anledning av rambeslutet trädde i kraft den 1 juni 2007 (prop. 2006/07:66, bet. 2006/07:JuU13, rskr. 2006/07:147, SFS 2007:213).

Den 30 september 2010 presenterade kommissionen ett förslag till direktiv om angrepp mot informationssystem, vilket föreslås ersätta det befintliga rambeslutet.

## 1.2 Förslagets innehåll

I *artikel 1* beskrivs det övergripande syftet med direktivet, nämligen att fastställa vilka gärningar som ska definieras som brott när det gäller angrepp mot informationssystem och att införa miniminormer med avseende på påföljder för sådana brott. Direktivet syftar också till att införa gemensamma bestämmelser för att förebygga sådana angrepp och förbättra det straffrättsliga samarbetet i EU inom detta område.

I *artikel 2* anges vad som i direktivet avses med begreppen informationssystem, datorbehandlingsbara uppgifter, juridisk person och orättmätigt.

Enligt *artiklarna 3−7* ska följande handlingar utgöra brott, om de utförs uppsåtligt och orättmätigt:

Artikel 3: intrång i ett informationssystem som helhet eller en del av ett sådant system, åtminstone i fall som inte är ringa (olagligt intrång i informationssystem).

Artikel 4: att 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 (olaglig systemstörning).

Artikel 5: att 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 (olaglig datastörning).

Artikel 6: avlyssning med tekniska hjälpmedel av icke-offentliga överföringar av datorbehandlingsbara uppgifter till, från eller inom ett informationssystem, inklusive elektromagnetisk strålning från informationssystem som innehåller sådana uppgifter (olaglig avlyssning).

Artikel 7: att tillverka, sälja, anskaffa i syfte att använda, importera, inneha, distribuera eller på annat sätt tillgängliggöra vissa verktyg, om gärningen utförs i syfte att begå något av de brott som anges i artiklarna 3–6. Verktygen som avses är dels anordning, inklusive datorprogram, som utformats eller anpassats i första hand för att begå brotten i fråga, dels lösenord, åtkomstkod eller liknande uppgifter som gör det möjligt att få tillgång till ett informationssystem eller delar av ett sådant system.

Enligt *artikel 8* ska anstiftan av och medhjälp till brott som avses i artiklarna 3–7 vara straffbelagda. Detsamma gäller försök till brott som avses i artiklarna 3–6.

*Artikel 9* anger att 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. För brott som avses i artiklarna 3–7 (i den svenska översättningen anges felaktigt artiklarna 3–6) ska maximistraffet vara minst två års fängelse.

*Artikel 10* innehåller bestämmelser om försvårande omständigheter och innebär att brott enligt direktivet ska vara belagda med ett maximistraff på minst fem års fängelse när de begås

1. inom ramen för en sådan kriminell organisation som avses i rambeslut 2008/841/RIF om kampen mot organiserad brottslighet (gäller brott enligt artiklarna 3–7),

2. med hjälp av ett verktyg som är avsett antingen att iscensätta angrepp som skadar ett betydande antal informationssystem eller orsakar avsevärd skada, till exempel i form av störda systemtjänster, ekonomiska kostnader eller förlust av personuppgifter (gäller brott enligt artiklarna 3–6), eller

3. genom att gärningsmannens verkliga identitet döljs, och detta är till skada för den som den använda identiteten faktiskt tillhör (gäller brott enligt artiklarna 3–6).

I *artiklarna 11* och *12* finns bestämmelser om ansvar och sanktioner för juridiska personer. Medlemsstaterna ska se till att juridiska personer kan hållas ansvariga för brott enligt direktivet och att sanktionerna ska vara effektiva, proportionella och avskräckande.

Enligt *artikel 13* ska medlemsstaterna se till att de har domsrätt när brott enligt direktivet har begåtts

a) helt eller delvis på medlemsstatens territorium, eller

b) av en medborgare i medlemsstaten eller av en person som har hemvist på dess territorium, eller

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

*Artikel 14* reglerar att medlemsstaterna för utbyte av uppgifter om brott enligt direktivet, med iakttagande av bestämmelser om dataskydd, ska 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 kan svara på brådskande framställningar inom högst åtta timmar. Av dessa svar ska det åtminstone framgå huruvida framställan om bistånd kommer att besvaras (i den svenska översättningen används dock uttrycket beviljas) och, om så är fallet, hur och när detta kommer att ske.

Enligt *artikel 15* ska medlemsstaterna se till att det finns ett system för registrering, insamling och tillhandahållande av statistiska uppgifter om brott enligt direktivet. Statistiken ska åtminstone omfatta antalet sådana brott som avses i direktivet som rapporterats till medlemsstaterna och uppföljningen av dessa rapporter samt på årsbasis ange antalet fall som undersökts, antalet personer som åtalats och antalet personer som dömts. Medlemsstaterna ska översända de uppgifter som samlas in enligt denna artikel till kommissionen. De ska också se till att en samlad översikt över dessa statistiska rapporter offentliggörs.

I *artiklarna 16–20* finns slutbestämmelser.

## 1.3 Gällande svenska regler och förslagets effekt på dessa

Bestämmelserna om olagligt intrång i informationssystem, olaglig systemstörning och olaglig datastörning (artiklarna 3–5) överensstämmer med artiklarna 2–4 i rambeslutet. Handlingarna är i svensk rätt straffbelagda genom främst bestämmelsen om dataintrång i 4 kap. 9 c § brottsbalken och kriminaliseringen av skadegörelse och sabotage i 12 och 13 kap. samma balk. Till skillnad från rambeslutet finns enligt förslaget ingen möjlighet att begränsa kriminaliseringen av olagligt intrång i informationssystem endast till när brottet begås genom intrång i en säkerhetsåtgärd (artikel 2.2. i rambeslutet). Eftersom något sådant intrång inte krävs för straffansvar enligt svensk rätt saknar denna förändring dock betydelse.

Bestämmelsen om olaglig avlyssning i artikel 6 är ny. Det finns i svensk rätt inte någon straffbestämmelse som direkt tar sikte på sådan avlyssning som avses. Brottsbalkens reglering av främst brytande av telehemlighet (4 kap. 8 § brottsbalken) och dataintrång torde delvis täcka denna handling, men det är tveksamt om dessa eller andra straffbud fullt ut täcker förslagets krav. Ytterligare analys av bestämmelsens överensstämmelse med svensk rätt krävs och det kan inte uteslutas att förslaget kan komma att kräva lagändringar.

Även artikel 7 är ny. Enligt denna bestämmelse ska befattning med vissa angivna verktyg i syfte att begå brott vara straffbart. Den svenska bestämmelsen om förberedelse och medverkan till brott i 23 kap. 2 och 4 §§ brotts-

balken skulle i vart fall delvis kunna motsvara förslagets krav. Bestämmelsen väcker dock flera frågor, inte minst om den praktiska tillämpningen och avgränsningen av det straffbara området. Förslagets innebörd behöver klargöras under de kommande förhandlingarna och analyseras vidare. Lagändringar till följd av förslaget i denna del kan inte uteslutas.

Bestämmelsen om anstiftan, medhjälp och försök i artikel 8 motsvarar regleringen i rambeslutet, med den skillnaden att möjligheten att inte kriminalisera försök till olagligt intrång i informationssystem har tagits bort. Denna möjlighet saknar dock betydelse för svenskt vidkommande. I konsekvens med vad som anges ovan om de nya artiklarna 6 och 7 behöver artikel 8 analyseras ytterligare.

De föreslagna straffnivåerna i artikel 9 är högre än i rambeslutet, men ligger inom straffskalan för t.ex. dataintrång, grov skadegörelse och sabotage. Vad gäller straffen för brott enligt artiklarna 6 och 7 får förhållandet till svensk rätt analyseras vidare. Detsamma gäller regleringen om försvårande omständigheter i artikel 10, som torde innebära att relevanta straffbestämmelser i vissa fall inte är tillräckliga. Den senare artikeln väcker för övrigt ytterligare frågor som behöver klargöras och analyseras vidare, inte minst när det gäller bestämmelsen i artikel 10.3.

Ansvar och sanktioner för juridiska personer (artiklarna 11 och 12) regleras på motsvarande sätt i flera redan antagna instrument inom ramen för EU-samarbetet. Bestämmelserna om företagsbot i 36 kap. 7–10 a §§ brottsbalken bedöms motsvara de krav som ställs i direktivet.

Bestämmelser om tillämpligheten av svensk lag finns huvudsakligen i 2 kap. brottsbalken. Vid genomförandet av rambeslutet gjordes bedömningen att svensk domsrätt förelåg i de fall då sådan ovillkorligen skulle kunna utövas. En skillnad i förhållande till rambeslutet är emellertid att det inte längre finns någon möjlighet att inte tillämpa bestämmelsen om behörighet för brott som begåtts till förmån för en juridisk person som har sitt huvudkontor på medlemsstatens territorium (artikel 13.1 c). Bestämmelsen i denna punkt motsvaras inte av en likalydande behörighetsregel i svensk rätt.

Bestämmelsen om utbyte av information i artikel 14 motsvarar artikel 11 i rambeslutet, men har kompletterats med en skyldighet att hörsamma en begäran om bistånd inom en viss tidsfrist. Rikskriminalpolisens IT-brottsrotel har en beredskap dygnet runt som innebär att en IT-specialist alltid kan nås. Förslaget får analyseras ytterligare, men torde inte innebära något problem för svensk del.

Artikel 15 om övervakning och statistik är ny. I Sveriges officiella kriminalstatistik finns uppgift om bl.a. antalet brott, uppklarade brott, misstänkta personer och lagförda personer. Förslaget kräver en fördjupad analys liksom klargöranden bl.a. i fråga om vilka uppgifter som ska samlas in och hur rutinerna för detta ska se ut samt inte minst hur denna bestämmelse förhåller sig till det övergripande statistikarbete som bedrivs inom EU på det straffrättsliga området.

Övriga artiklar i direktivet innehåller inte några bestämmelser som föranleder någon närmare redogörelse för innehållet i svensk rätt.

### 1.4 Budgetära konsekvenser / Konsekvensanalys

Kommissionen har angett att förslaget har liten inverkan på unionens budget. Mer än 90 procent av den beräknade kostnaden på 5 913 000 Euro skulle bäras av medlemsstaterna och det finns möjlighet att ansöka om EU-finansiering för att minska bördan.

Det är inte möjligt att i nuläget närmare bedöma eventuella budgetära konsekvenser. Utgångspunkten är dock att eventuella sådana konsekvenser, såväl nationella som inom EU, ska finansieras inom befintlig budgetram.

## 2 Ståndpunkter

### 2.1 Preliminär svensk ståndpunkt

Regeringen välkomnar att kommissionen presenterat ett förslag till direktiv om angrepp mot informationssystem. Förslaget överensstämmer i stora delar med det tidigare rambeslutet, men innehåller därtill bestämmelser som ytterligare förstärker arbetet inom EU med att motverka och bekämpa dessa företeelser. Internationell samverkan är en förutsättning för framgång och det europeiska samarbetet av central betydelse. Det finns dock skäl att noggrant analysera förslagets olika bestämmelser, bl.a. i fråga om de nya handlingar som ska utgöra brott, straffnivåer och försvårande omständigheter.

### 2.2 Medlemsstaternas ståndpunkter

Medlemsstaternas ståndpunkter är ännu inte kända.

### 2.3 Institutionernas ståndpunkter

Europaparlamentets ståndpunkt är ännu inte känd.

### 2.4 Remissinstansernas ståndpunkter

Förslaget har inte remitterats.

# 3 Förslagets förutsättningar

## 3.1 Rättslig grund och beslutsförfarande

Artikel 83(1) i fördraget om Europeiska unionens funktionssätt (EUF-fördraget). Direktivet antas i enlighet med det ordinarie lagstiftningsförfarandet (artikel 294 EUF-fördraget). Rådet beslutar med kvalificerad majoritet och Europaparlamentet är medbeslutande.

## 3.2 Subsidiaritets- och proportionalitetsprincipen

I motiveringen till förslaget till direktiv gör kommissionen bedömningen att förslaget är förenligt med subsidiaritets- respektive proportionalitetsprincipen.

Som skäl för att medlemsstaterna inte i tillräcklig utsträckning själva kan uppnå målen med förslaget anges följande. IT-brottslighet och, mer specifikt, angrepp mot informationssystem har en betydande gränsöverskridande dimension, som framgår tydligast när det gäller storskaliga angrepp, eftersom de olika element som tillsammans bildar ett angrepp ofta finns på olika platser och i olika länder. Detta kräver åtgärder på EU-nivå, särskilt för att hålla jämna steg med utvecklingen mot allt mer storskaliga angrepp i Europa och i världen som helhet. Insatser på EU-nivå och en uppdatering av rambeslut 2005/222/RIF efterlystes också i rådets slutsatser från november 2008 (En samordnad arbetsstrategi och konkreta åtgärder mot IT-brottslighet), eftersom målet att på ett effektivt sätt skydda människor från IT-brott inte i tillräcklig utsträckning kan uppnås av medlemsstaterna på egen hand.

Genom att EU vidtar åtgärder kommer det enligt kommissionen att bli lättare att uppnå målen, och detta av följande skäl. Förslaget innebär att medlemsstaternas materiella straffrätt och regler om straffrättsliga förfaranden tillnärmas ytterligare, vilket får positiva verkningar för kampen mot denna typ av brottslighet. För det första är det ett sätt att förhindra att gärningsmän flyttar till medlemsstater där lagstiftningen mot IT-angrepp är mindre sträng. För det andra innebär gemensamma definitioner att det blir möjligt att utbyta information samt samla in och jämföra relevanta data. För det tredje kan de förebyggande åtgärderna i EU göras mer effektiva och det internationella samarbetet förbättras.

Direktivet begränsas enligt kommissionen till det minimum som krävs för att uppnå målen på europeisk nivå och går inte utöver vad som är nödvändigt för att uppnå detta syfte med beaktande av den straffrättsliga lagstiftningens krav på exakthet.

Regeringen delar kommissionens bedömning.

# 4 Övrigt

## 4.1 Fortsatt behandling av ärendet

Förslaget till direktiv kommer enligt uppgift att behandlas i rådsarbetsgruppen materiell straffrätt. Förhandlingarna kommer att inledas tidigast i december 2010.

## 4.2 Fackuttryck/termer

-