U 50/2010 rd

Statsrådets skrivelse till Riksdagen om ett förslag till Europaparlamentets och rådets direktiv om angrepp mot informationssystem och om upphävande av rådets rambeslut 2005/222/RIF

I enlighet med 96 § 2 mom. i grundlagen översänds till riksdagen förslaget till Europaparlamentets och rådets direktiv om angrepp mot informationssystem och om upphävande av rådets rambeslut 2005/222/RIF samt en promemoria om förslaget

Helsingfors den 2 december 2010

Justitieminister *Tuija Brax*

Lagstiftningsdirektör Asko Välimaa

295391

JUSTITIEMINISTERIET PROMEMORIA EU/2010/1522

FÖRSLAG TILL EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV OM ANGREPP MOT INFORMATIONSSYSTEM OCH OM UPPHÄVANDE AV RÅDETS RAMBESLUT 2005/222/RIF

1 Allmänt

Europeiska kommissionen har den 30 september 2010 lagt fram ett förslag till Europaparlamentets och rådets direktiv om angrepp mot informationssystem och om upphävande av rådets rambeslut 2005/222/RIF (KOM(2010) 517 slutlig). Syftet med direktivförslaget är att tillnärma medlemsstaternas strafflagstiftning på området för angrepp mot informationssystem och att förbättra samarbetet mellan rättsliga och andra behöriga myndigheter, inbegripet polismyndigheter och andra brottsbekämpande organ i medlemsstaterna.

I förslaget är det fråga om att upphäva rådets rambeslut 2005/222/RIF om angrepp mot informationssystem, nedan rambeslutet, och ersätta det med ett nytt direktiv. Det föreslagna direktivet innehåller de motsvarande bestämmelserna i det nuvarande direktivet i huvudsak som sådana. I direktivet ska även intas vissa kriminaliseringsskyldigheter som motsvarar kriminaliseringsskyldigheterna i Europarådets straffrättsliga konvention om IT-relaterad brottslighet (FördrS 60/2007), nedan konventionen. I förslaget ingår också nya bestämmelser som syftar bland annat till att ingripa i nya hot, såsom massiva angrepp mot informationssystem genom användning av så kallade botnät och missbruk av någon annans identitet vid it-relaterade brott.

Vikten av att vidta ytterligare åtgärder för att intensifiera kampen mot it-brottslighet betonades i 2004 års Haagprogram för ett stärkt område med frihet, säkerhet och rättvisa och i 2009 års Stockholmsprogram med tillhörande handlingsplan (KOM(2010) 171 slutlig). Behovet av att möta it-brott på EU-nivå konstateras också i den digitala agendan för Europa som är ett led i Europa 2020-strategin.

Lagändringarna som genomförandet av rambeslutet och ikraftsättandet av konventionen förutsätter i Finland har trätt i kraft den 11 maj 2007 (RP 153/2006 rd). Konventionen trädde i kraft internationellt den 1 juli 2004 och den har satts i kraft nationellt av 30 stater, varav 17 är EU-medlemsstater.

2 Det huvudsakliga innehållet

Bestämmelserna i det föreslagna direktivet som motsvarar bestämmelserna i rambeslutet som avses att upphävas gäller definitionerna av informationssystem, datorbehandlingsbara uppgifter, juridisk person och begreppet orättmätigt (artikel 2 i direktivförslaget), olagligt intrång i informationssystem (artikel 3), olaglig systemstörning (artikel 4), olaglig datastörning (artikel 5), anstiftan, medhjälp och försök till brott (artikel 8), juridiska personers ansvar (artiklarna 11 och 12) och straffrättslig behörighet (artikel 13). Föreslagna bestämmelser som ingår i konventionen, men inte i rambeslutet, gäller olaglig avlyssning (artikel 6 i direktivförslaget) och verktyg som används för att begå brott (artikel 7). I direktivförslaget har dock inte intagits alla de möjligheter som ingår i rambeslutet och konventionen att nationellt begränsa tillämpningsområdet av vissa av de ovan nämnda bestämmelserna eller göra reservationer i fråga om bestämmelserna.

I förslaget ingår också bestämmelser om utbyte av information mellan myndigheterna i medlemsstaterna (artikel 14) som är mer tvingande än motsvarande bestämmelser i rambeslutet och konventionen.

I förslaget finns också bestämmelser som inte ingår i rambeslutet eller konventionen. I bestämmelserna om försvårande omständigheter har fogats massiva angrepp genom användning av så kallade botnät (artikel 10.2) och döljande av gärningsmannens identitet så

att detta är till skada för den som identiteten faktiskt tillhör (artikel 10.3). Med termen botnät avses ett nätverk av datorer som har infekterats av sabotageprogram (datorvirus) och som styrs via en värddator, ofta utan att de som använder de infekterade datorerna är medvetna om det. Ett botnät kan aktiveras för att utföra särskilda uppgifter, till exempel angripa informationssystem (it-angrepp).

I direktivförslaget finns också en ny bestämmelse om insamling av statistiska uppgifter (artikel 15).

Bestämmelserna om påföljderna för fysiska personer är strängare än i rambeslutet och konventionen.

3 Konsekvenser för lagstiftningen i Finland

I 38 kap. i strafflagen (39/1889) finns bestämmelser om informations- och kommunikationsbrott. I kapitlet ingår bestämmelser om kränkning av kommunikationshemlighet (3 §), grov kränkning av kommunikationshemlighet (4 §), systemstörning (7 a §), grov systemstörning (7 b §), dataintrång (8 §) och grovt dataintrång (8 a §). I 34 kap. i strafflagen finns bestämmelser om orsakande av fara för informationsbehandling (9 a §) och innehav av hjälpmedel vid nätbrott (9 b §). I kap. 35 1 § 2 mom. i strafflagen föreskrivs om skadegörelse i sådant fall att någon förstör information som har upptagits på ett datamedium. I strafflagen finns också andra straffbestämmelser som gäller gärningar som riktar sig mot informationssystem eller som utförs med hjälp av en dator. Till exempel bestämmelserna i 28 kap 7—9 § om olovligt brukande gäller även användning av datasystem och i 36 kap. 1 § 2 mom. om bedrägeri föreskrivs om orsakande av ekonomisk skada för någon annan genom att ingripa i ett informationssystems funktion.

De ovan nämnda bestämmelserna uppfyller de kriminaliseringsskyldigheter som ingår i det föreslagna direktivet och om vilka det finns motsvarande bestämmelser i rambeslutet och konventionen till den delen verkställigheten av skyldigheterna inte har begränsats på det sätt som rambeslutet eller konventionen tillåter. Också de förutsättningar enligt förslaget som gäller straffbeläggande av anstiftan, medhjälp och försök till brott samt juridiska personer straffansvar uppfylls med stöd av den gällande lagstiftningen (RP 153/2006).

I direktivförslagets artikel 3 om olagligt intrång i informationssystem ska inte på samma sätt som i motsvarande bestämmelse i rambeslutet och konventionen ingå möjlighet att nationellt besluta att handlandet kriminaliseras endast när brottet begås genom intrång i en säkerhetsåtgärd. Tillämpning av bestämmelsen om dataintrång i 38 kap. 8 § i strafflagen förutsätter någon tränger in i ett datasystem genom att göra bruk av en användaridentifikation som han inte har rätt till eller genom att annars bryta säkerhetsarrangemang. Om någon tränger in i ett datasystem och olovligt använder informationen i det utan att bryta säkerhetsarrangemang, uppfyller gärningen oftast rekvisitet för olovligt brukande enligt 28 kap. 7 § i strafflagen. Lagstiftningen överensstämmer dock inte fullt ut med direktivförslagets artikel 3.

Bestämmelsen i direktiveförslagets artikel 8.2 om skyldigheten att straffbelägga försök motsvarar till andra delar rambeslutets bestämmelser, men gäller även olagligt intrång i informationssystem enligt artikel 3 och olaglig avlyssning enligt artikel 6. Eftersom försök till motsvarande brott redan nu är straffbart enligt strafflagen förutsätter denna bestämmelse inte att lagstiftningen ändras.

Enligt artikel 9 i direktivförslaget ska medlemsstaterna vidta de åtgärder som är nödvändiga för att se till att de brott som avses i artiklarna 3—7 är belagda med straffrättsliga påföljder som innebär ett maximistraff på minst två års fängelse. Det föreslagna maximistraffet är strängare än i rambeslutet enligt vilket fängelse i ett år kan vara ett tillräckligt maximistraff för motsvarande gärningar som omfattas av rambeslutet (artikel 6.2 i rambeslutet). I konventionen förutsätts enbart att påföljderna som fastställs för brotten ska vara effektiva, proportionella och tillräckliga frihetsstraff (artikel 13.1 i konventionen). Det krav på maximistraff som förutsätts i direktivförslaget uppfylls inte i fråga om kränkning av kommunikationshemlighet, dataintrång och skadegörelse, för vilka maximistraffet är fängelse i högst ett år och inte heller i fråga om innehav av hjälpmedel vid

nätbrott, för vilket maximistraffet är fängelse i högst sex månader.

I artikel 10 i direktivförslaget föreskrivs om sådana försvårande omständigheter som innebär att maximistraffet för ett brott som omfattas av direktivets tillämpningsområde ska vara fängelse i minst fem år. Enligt artikel 10.1 skulle en sådan försvårande omständighet vara att ett brott som avses i artiklarna 3-7 i direktivförslaget begås inom ramen för en kriminell organisation enligt definitionen i rambeslut 2008/841/RIF om kampen mot organiserad brottslighet. Definitionen av en organiserad kriminell sammanslutning i 17 kap. 1 a § 4 mom. i strafflagen motsvarar nämnda definition av kriminell organisation.

Enligt artikel 10.2 i direktivet skulle en försvårande omständighet vara att ett brott som avses i artiklarna 3—6 begås med hjälp av ett verktyg som är avsett antingen att skada ett betydande antal informationssystem eller att orsaka avsevärd skada, till exempel i form av störda systemtjänster, ekonomiska kostnader eller förlust av personuppgifter. Denna brottsbeskrivning avser enligt förslaget särskilt användningen av botnät.

Bestämmelser som närmast motsvarar skyldigheterna enligt 10.1 och 10.2 är grov kränkning av kommunikationshemlighet, grov systemstörning, grovt dataintrång och grov skadegörelse. Att gärningen begås som ett led i en organiserad kriminell sammanslutnings verksamhet nämns i ovan nämnda bestämmelser enbart i brottsbeskrivningen för grovt dataintrång och grov skadegörelse.

Dessutom finns det enbart i en del av bestämmelserna sådana tillämpningsgrunder att dessa eventuellt kunde tillämpas på en sådan massiv gärning som avses i artikel 10.2.

De ovan nämnda bestämmelserna omfattar inte heller alla sådana brott som avses i artiklarna 3—7, för vilka de försvårande omständigheterna enligt 10.1 och 10.2 gäller. Det finns till exempel inte bestämmelser en grov form av orsakande av fara för informationsbehandling eller innehav av hjälpmedel vid nätbrott. Dessutom är maximistraffet för dessa gärningar fängelse i tre eller fyra år, vilket inte motsvarar det föreslagna maximistraffet på minst fem års fängelse.

Enligt artikel 10.3 skulle en försvårande omständighet vara att ett brott som avses i artiklarna 3—6 begås genom att gärningsmannens verkliga identitet döljs så att detta är till skada för den som den använda identiteten faktiskt tillhör. Innehållet av förslaget är inte riktigt tydligt. I förslaget definieras bl.a. inte vad som avses med identitet eller med att dölja det. Inte heller skadans art definieras. Trots att bestämmelsen är otydlig konstateras det i motiveringen att dessa bestämmelser ska överensstämma med legalitetsprincipen och befintlig lagstiftning om skydd av personuppgifter (s. 7).

I den finska lagstiftning ingår inga bestämmelser som skulle motsvara en sådan försvårande omständighet som avses i artikel 10.3.

Bestämmelsen om behörighet i artikel 13 i direktivförslaget överensstämmer med motsvarande bestämmelser i rambeslutet. Enligt rambeslutet får medlemsstaterna dock besluta att inte tillämpa bestämmelsen om behörighet bl.a. i sådant fall att brottet har begåtts till förmån för en juridisk person som har sitt huvudkontor på medlemsstatens territorium. I direktivförslaget ingår ingen motsvarande möjlighet att avvika från bestämmelsen. Artikel 13 i direktivet förutsätter således att lagstiftningen ändras.

I direktivförslagets artikel 14 om utbyte av information har jämfört med motsvarande bestämmelser i rambeslutet och konventionen fogats en skyldighet för medlemsstaterna att se till att de har förfaranden som gör att deras kontaktpunkter som kan nås dygnet runt alla dagar i veckan kan svara på brådskande framställningar inom högst åtta timmar. Av dessa svar ska det åtminstone framgå huruvida framställan om bistånd kommer att beviljas, hur detta görs och när detta kommer att ske. I Finland fungerar centralkriminalpolisen som en sådan kontaktpunkt som avses i direktivet. Artikeln förutsätter inga ändringar i lagstiftningen.

Artikel 15 i direktivförslaget gäller övervakning och statistik. I rambeslutet eller konventionen ingår ingen motsvarande bestämmelse. Enligt bestämmelsen ska medlemsstaterna ha ett system för registrering, insamling och tillhandahållande av statistiska uppgifter om de brott som anges i artiklarna

3—8 i direktivet. De statistiska uppgifterna ska offentliggöras och översändas till kommissionen. I Finland svarar statistikcentralen för de statistiska uppgifter som avses i artikeln. Bestämmelsen förutsätter inga ändringar i lagstiftningen.

4 Ålands behörighet

Enligt 27 § 22 punkten i självstyrelselagen för Åland (1144/1991) har riket lagstiftningsbehörighet i fråga om straffrätt med undantag av vad som stadgas i 18 § 25 punkten. Enligt den sistnämnda punkten har landskapet lagstiftningsbehörighet i fråga om beläggande med straff och storleken av straff inom rättsområden som hör till landskapets lagstiftningsbehörighet. Utifrån de andra punkterna i 18 § har landskapet inte lagstiftningsbehörighet i fråga om lagstiftningen som gäller datorbrott.

5 Förslagets konsekvenser

Genom direktivet ska medlemsstaternas lagstiftning tillnärmas genom att förutsätta att skadliga gärningar mot informationssystem kriminaliseras och genom att fastställa minimistraffen för dessa gärningar. Denna harmonisering kan bidra till att främja medlemsstaternas samarbete i kampen mot sådan brottslighet som omfattas av direktivets tillämpningsområde.

Genom direktivet intensifieras också utredningen av brott genom att stärka och försnabba verksamheten av de kontaktpunkter som kan nås dygnet runt alla dagar i veckan. De nya skyldigheterna som gäller statistiska uppgifter underlättar uppföljningen av it-brottsligheten inom EU-området.

I sin konsekvensbedömning gällande direktivförslaget antar kommissionen att stärkandet av verksamheten av de kontaktpunkter som kan nås dygnet runt kan medföra tilläggskostnader för medlemsstaterna. Eftersom verksamheten av centralkriminalpolisens kontaktpunkt redan nu uppfyller de föreslagna skyldigheterna, medför direktivet till denna del inga tilläggskostnader för Finland.

6 Rättslig grund

Artikel 83.1 i fördraget om Europeiska unionens funktionssätt.

7 Subsidiaritetsprincipen

It-brottslighet har en gränsöverskridande dimension. Förslaget innebär att medlemsstaternas förfaranden i fråga om internationellt samarbete tillnärmas ytterligare, vilket får positiva verkningar för kampen mot denna typ av brottslighet. Statsrådet anser att förslaget är förenligt med subsidiaritetsprincipen.

8 De övriga medlemsstaternas ståndpunkter

Behandlingen av förslaget har inte ännu inletts i arbetsgruppen.

9 Institutionernas och andra ståndpunkter

Europaparlamentet har inte ännu behandlat förslaget.

10 Den nationella behandlingen av förslaget och behandlingen i Europeiska unionen

Direktivförslaget har behandlats skriftligt vid avdelningen för polissamarbete och straffrättsligt samarbete i sektionen för rättsliga och inrikes frågor (sektion 7).

Kommissionen har lagt fram förslaget för rådet för rättsliga och inrikes frågor den 8/9 november 2010 samt för rådets arbetsgrupp den 13 oktober 2010. Behandlingen i arbetsgruppen inleds enligt uppskattningar under Ungerns ordförandeskap.

Det ansvariga utskottet inom Europaparlamentet är utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor (LIBE). Rapportören har inte ännu utnämnts.

11 Statsrådets ståndpunkt

Statsrådet förhåller sig positivt till Europeiska unionens gemensamma verksamhet i kampen mot allvarliga brott som riktar sig

mot datasystem. Brotten begås i en snabbt föränderlig omvärld och är mycket ofta gränsöverskridande. Därför är det viktigt att strafflagstiftningen i alla EU-medlemsstater är tidsenlig och omfattande. Området för de föreslagna kriminaliseringsskyldigheterna motsvarar i huvudsak bestämmelserna i det gällande rambeslutet, Europarådets konvention och Finlands gällande lagstiftning. Förslaget kan enligt statsrådets åsikt generellt sett anses vara nödvändigt och bör understödas trots Europarådets motsvarande konvention, eftersom 10 medlemsstater hittills inte har nationellt satt i kraft konventionen.

De föreslagna nya bestämmelserna om användning av botnät och missbruk av någon annans identitet återspeglar utvecklingen under den senaste tiden. Dessa bestämmelser utvidgar dock inte området för straffbarhet utan de gäller maximistraffen för dessa gärningar. Det mest konsekventa sättet att sätta i kraft dessa bestämmelser i Finland är att de skulle utgöra tillämpningsgrunder för de grova formerna av dessa brott. Därför bör bestämmelserna i den fortsatta beredningen av förslaget formuleras så att de kan sättas i kraft nationellt på det sätt som förutsätts av den straffrättsliga legalitetsprincipen.

De föreslagna maximistraffen är strängare än de nuvarande straffen och jämfört med allmänna straffnivån i strafflagen synnerligen stränga. Skyldigheterna i anslutning till maximistraffen har inte heller specificerats på ett sätt som beaktar de olika graderna av allvarlighet i fråga om brotten som avses i direktivet. Problematiskt är bland annat att ett maximistraff på minst två års fängelse ska fastställas både för orättmätigt intrång i ett datasystem och för innehav av verktyg som används för att begå en sådan gärning när avsikten med innehavet är att använda dessa verktyg för att begå ett brott som avses i direktivet.

Straffvärdet och straffskalorna för en gärning ska i enlighet med proportionalitetsprincipen stå i rätt proportion till syftet och brottets allvarlighet. När det gäller att förebygga brott fungerar en förhöjd risk för att åka fast, t.ex. genom att effektivisera det internationella samarbetet mellan myndigheterna, bättre än skärpta straffskalor. Det är viktigt att man inom EU-straffrätten i tillräcklig grad beaktar en enskild medlemsstats praxis för straffskalor och inte äventyrar konsekvensen i medlemsstatens straffrätt.