Kommittédirektiv

Tilläggsdirektiv till Utredningen om tillträde till Europarådets konvention om it-relaterad brottslighet med tilläggsprotokoll
(Ju 2011:12)

Dir. 2012:102

Beslut vid regeringssammanträde den 11 oktober 2012

Sammanfattning av tilläggsuppdraget

Utredningen om it-brottskonventionen (Ju 2011:12) ska utöver vad som framgår av redan beslutade kommittédirektiv

- analysera behovet av och lämna förslag till de författningsändringar som behövs för att genomföra Europaparlamentets och rådets kommande men ännu inte formellt antagna direktiv om angrepp mot informationssystem och upphävande av rambeslut 2005/222/RIF, och
- överväga behovet av skärpta straff för brytande av post- eller telehemlighet och dataintrång för att ge ett ökat utrymme att på ett nyanserat sätt beakta allvaret i storskaliga angrepp mot informationssystem.

Utredningstiden förlängs. Uppdraget ska i stället slutredovisas senast den 3 juni 2013.

Utredningens nuvarande uppdrag

Regeringen beslutade den 27 oktober 2011 kommittédirektiv om tillträde till Europarådets konvention om it-relaterad brottslighet med tilläggsprotokoll (dir. 2011:98). Utredningen har tagit namnet Utredningen om it-brottskonventionen (Ju

2011:12). I utredningens uppdrag ingår att analysera behovet av författningsändringar för att Sverige ska kunna tillträda konventionen och dess tilläggsprotokoll och lämna förslag till de författningsändringar som behövs för att möjliggöra ett svenskt tillträde till instrumenten.

Tilläggsuppdraget

EU-direktivet om angrepp mot informationssystem

Inom EU pågår förhandlingar om ett direktiv om angrepp mot informationssystem (Europaparlamentets och rådets direktiv om angrepp mot informationssystem och upphävande av rambeslut 2005/222/RIF). Direktivet syftar till att ytterligare närma medlemsstaternas strafflagstiftning till varandra på området för angrepp mot informationssystem. Vidare är avsikten att förbättra samarbetet mellan myndigheter och brottsbekämpande organ i medlemsstaterna. Tyngdpunkten i direktivet utgörs av materiella straffrättsliga bestämmelser. Efter artikel 1 och 2 som innehåller en beskrivning av syftet med direktivet och definitioner av vissa begrepp, behandlas i artiklarna 3–7 vilka gärningar som ska utgöra brott, om de utförs uppsåtligen och orättmätigt. Dessa gärningar är olagligt intrång i informationssystem (artikel 3), olaglig systemstörning (artikel 4), olaglig datastörning (artikel 5), olaglig avlyssning (artikel 6) och vissa åtgärder med verktyg som används för att begå brott (artikel 7). I artikel 8 anges att anstiftan av och medhjälp till sådana gärningar som utgör brott enligt direktivet ska straffbeläggas. Det anges även vilka gärningar som ska straffbeläggas på försöksnivå. Artikel 9 innehåller både generella och artikelspecifika bestämmelser om vilka påföljder som ska kunna dömas ut för brotten i direktivet. Artikel 10 har under förhandlingarna utgått ur utkastet till direktiv. I artiklarna 11 och 12 regleras juridiska personers ansvar samt påföljder för juridiska personer. Jurisdiktionsfrågor regleras i artikel 13. Därefter följer i artikel 14 bestämmelser om informationsutbyte och i artikel 15 bestämmelser om övervakning och statistik. Direktivet avslutas med bestämmelser om ersättande av 2005

års rambeslut, införlivande och om rapporteringsskyldighet m.m. (artiklarna 16–20).

Förhandlingarna om direktivet är i allt väsentligt slutförda. Det återstår för EU:s institutioner att formellt anta den text som har godkänts av företrädare för rådet och Europaparlamentet (dok. 11399/12). Efter att direktivet antas har medlemsstaterna två år på sig att genomföra det.

Direktivets bestämmelser, i synnerhet på straffrättens område, överensstämmer till stor del med dem som finns i Europarådets konvention om it-relaterad brottslighet. De lagändringar som kan föranledas av direktivet är därför sådana att de sannolikt behövs även för att tillträda konventionen. Mot denna bakgrund och med beaktande av den tid som Sverige har på sig att genomföra direktivet efter att det antas, finns det skäl att ge Utredningen om it-brottskonventionen i uppdrag att även

- analysera behovet av och lämna förslag till de författningsändringar som behövs för att genomföra det kommande men ännu inte formellt antagna direktivet om angrepp mot informationssystem.

Straffskalorna för angrepp mot informationssystem

Artikel 9 i direktivet innehåller, till skillnad från konventionen, specifika bestämmelser om straffskalornas utformning när det gäller olika former av angrepp mot informationssystem. Förutom att brotten i direktivet generellt ska ha påföljder som är effektiva, proportionerliga och avskräckande fordras att samtliga brott, undantaget osjälvständiga brottsformer, ska ha en straffskala med ett lägsta maximistraff på två år.

För brotten olaglig systemstörning (artikel 4) och olaglig datastörning (artikel 5) krävs dessutom ett lägsta maximistraff på tre år när ett stort antal informationssystem har påverkats genom användning av ett verktyg som har utformats primärt för detta syfte. För dessa brott ställs slutligen ett krav på ett lägsta maximistraff på fängelse i fem år under tre förutsättningar:

- (a) att brottet har begåtts inom ramen för en kriminell organisation,
- (b) att brottet har orsakat allvarlig skada, eller

- (c) att brottet har begåtts mot ett kritiskt informationsinfrastruktursystem.

I brottsbalken finns primärt två brott som bedöms som centrala när det gäller att uppfylla flera av de olika former av angrepp mot informationssystem som beskrivs i direktivet: brytande av post- eller telehemlighet (4 kap. 8 § brottsbalken) och dataintrång (4 kap. 9 c § brottsbalken). Dessa brott har straffskalor som sträcker sig från böter till fängelse i högst två år. Det finns redan mot den bakgrunden ett behov av att göra överväganden om straffskalornas utformning för dessa brott.

Straffskalan för brytande av post- eller telehemlighet har varit oförändrad sedan brottsbalkens tillkomst. Även dataintrångsbestämmelsen har samma straffskala som när bestämmelsen först infördes i datalagen (1973:289), även om den ändrats i sak vid ett flertal tillfällen.

Sedan brottsbalkens och datalagens tillkomst har det skett en betydande samhällsutveckling och informationssystem har i dag en ojämförligt större betydelse i samhället än när bestämmelserna infördes. Det finns tecken på att utvecklingen går mot allt farligare och mer storskaliga angrepp mot informationssystem, till exempel intrång i eller överbelastningsattacker mot bankers och myndigheters informationssystem. Angreppen begås med sofistikerade metoder och kan orsaka betydande ekonomiska skador på grund av avbrott i informationssystemens drift och kommunikation. De kan också leda till förlust eller förvanskning av hemlig eller i övrigt integritetskänslig information. Många gånger kan ett sådant beteende träffas av straffansvaret för sabotage i 13 kap. 4 § brottsbalken. Beroende på omständigheterna, t.ex. att skadan i och för sig är omfattande men av tillfällig karaktär eller att den infrastruktur som skadas inte utgör för samhället viktig egendom, kan emellertid vissa mycket straffvärda beteenden falla utanför sabotagebestämmelsens tillämpningsområde. Regeringen anser därför att det finns anledning att – även vid sidan av vad som bedöms nödvändigt för att genomföra direktivet – överväga att skärpa straffskalorna för brytande av post- eller telehemlighet och dataintrång.

Utredaren ska mot den bakgrunden

- överväga behovet av och – om det finns anledning till det – lämna förslag till skärpta straff för brytande av post- eller telehemlighet och dataintrång för att ge ett ökat utrymme att på ett nyanserat sätt beakta allvaret i storskaliga angrepp mot informationssystem, och
- redovisa sin bedömning av om en sådan straffskärpning bör ske enbart genom förändringar av straffskalorna eller om särskilda straffskalor för grova brott bör införas samt beskriva de straffrättsliga och systematiska konsekvenserna av dessa alternativ.

Arbetets bedrivande och redovisning av uppdraget

Förslagens konsekvenser ska redovisas enligt 14–15 a §§ kommittéförordningen.

Utredningstiden förlängs. Uppdraget ska i stället slutredovisas senast den 3 juni 2013.

(Justitiedepartementet)