Regeringens proposition 2013/14:92

Skärpt straff för dataintrång

Prop. 2013/14:92

Regeringen överlämnar denna proposition till riksdagen.

Stockholm den 13 mars 2014

Fredrik Reinfeldt

Beatrice Ask
(Justitiedepartementet)

Propositionens huvudsakliga innehåll

Dagens samhälle präglas av att användningen av informationsteknik genomsyrar i stort sett alla sektorer. Myndigheter, företag och organisationer är i hög grad beroende av fungerande informationssystem. Den tekniska utvecklingen innebär samtidigt att samhället blir mer sårbart för brottsliga angrepp. Det finns tecken på att utvecklingen går mot allt farligare och mer storskaliga angrepp mot informationssystem. Det är angeläget att strafflagstiftningen är utformad så att denna typ av brottslighet kan mötas med påföljder som står i proportion till brottens allvar.

I propositionen föreslås därför att det införs en bestämmelse om *grovt dataintrång* i brottsbalken. Straffet föreslås vara fängelse i lägst sex månader och högst sex år. Vid bedömningen av om brottet är grovt ska det särskilt beaktas om gärningen har orsakat allvarlig skada eller avsett ett stort antal uppgifter eller annars varit av särskilt farlig art. Även försök och förberedelse till grovt dataintrång ska vara straffbart.

Vidare föreslås att bestämmelsen om dataintrång inte längre ska vara subsidiär i förhållande till straffbestämmelserna om brytande av post- eller telehemlighet och intrång i förvar.

I propositionen behandlas även genomförandet av EU:s direktiv om angrepp mot informationssystem. Genom den straffskärpning som föreslås uppfyller Sverige kraven i direktivet.

Lagändringarna föreslås träda i kraft den 1 juli 2014.

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[1] att 4 kap. 9 c och 10 §§ brottsbalken ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	4 kap.
	9 c §[2]
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.	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 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.
	Är brottet grovt, döms för grovt dataintrång till fängelse i lägst sex månader och högst sex år. Vid bedömande av om brottet är grovt ska det särskilt beaktas om gärningen har orsakat allvarlig skada eller avsett ett stort antal uppgifter eller annars varit av särskilt farlig art.
	10 §[3]
För försök, förberedelse eller stämpling till människorov, människohandel eller olaga frihetsberövande och för underlåtenhet att avslöja sådant brott döms till ansvar enligt *vad som sägs i* 23 kap. Detsamma gäller för försök eller förberedelse till olaga tvång som är grovt *eller till* dataintrång som om det fullbordats inte skulle ha varit att	För försök, förberedelse eller stämpling till människorov, människohandel eller olaga frihetsberövande och för underlåtenhet att avslöja *ett* sådant brott döms *det* till ansvar enligt 23 kap. Detsamma gäller för försök eller förberedelse till olaga tvång som är grovt, dataintrång som om det fullbordats inte skulle ha varit att anse som ringa, *eller grovt*

[1] Jfr 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 (EUT L 218, 14.8.2013, s. 8–14, Celex 32013L0040).
[2] Senaste lydelse 2007:213.
[3] Senaste lydelse 2004:406.

Denna lag träder i kraft den 1 juli 2014.

3 Ärendet och dess beredning

Den 30 september 2010 lade Europeiska kommissionen fram ett förslag till direktiv om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF. Förslaget byggde i stora delar dels på det tidigare rambeslutet, dels på Europarådets konvention om it-relaterad brottslighet. En faktapromemoria om direktivförslagets innehåll har överlämnats till riksdagen (2010/11:FPM15).

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 (fortsättningsvis direktivet) trädde i kraft den 3 september 2013. Direktivet ska vara genomfört senast den 4 september 2015. Direktivet finns i *bilaga 1*.

Regeringen gav den 27 oktober 2011 en särskild utredare i uppdrag att efter en behovsanalys lämna förslag på de författningsändringar som krävs för att Sverige ska kunna tillträda Europarådets konvention om it-relaterad brottslighet och dess tilläggsprotokoll (dir. 2011:98). Utredningen, som tog namnet Utredningen om it-brottskonventionen, fick genom tilläggsdirektiv den 11 oktober 2012 i uppdrag att även analysera behovet av och lämna förslag till de författningsändringar som behövs för att genomföra direktivet. Utredningen fick dessutom i uppgift att överväga behovet av skärpta straff för brytande av post- eller telehemlighet och dataintrång (dir. 2012:102).

Utredningen lämnade i juni 2013 betänkandet Europarådets konvention om it-relaterad brottslighet (SOU 2013:39). I betänkandet lämnas bl.a. förslag till de lagändringar som bedöms nödvändiga för att tillträda konventionen och dess tilläggsprotokoll samt för att genomföra direktivet.

Denna proposition behandlar de frågor som omfattades av utredningens tilläggsuppdrag, dvs. genomförandet av direktivet och frågan om skärpta straff för dataintrång och brytande av post- eller telehemlighet. Utredningens övriga förslag bereds vidare inom Regeringskansliet.

En sammanfattning av betänkandet och dess lagförslag i relevanta delar finns i *bilaga 2* respektive *bilaga 3*.

Betänkandet har remissbehandlats och en förteckning över remissinstanserna finns i *bilaga 4*. En sammanställning av remissyttrandena i nu aktuella delar finns tillgänglig i Justitiedepartementet (Ju2013/4173/Å).

Lagrådet

Regeringen beslutade den 16 januari 2014 att inhämta Lagrådets yttrande över det lagförslag som finns i *bilaga 5*. Lagrådets yttrande finns i *bilaga 6*. Lagrådet har lämnat förslaget utan erinran.

I förhållande till lagrådsremissens lagförslag har en mindre språklig ändring gjorts.

4 Bakgrund och allmänna utgångspunkter

4.1 Angrepp mot informationssystem

Dagens samhälle präglas av att användningen av informationsteknik genomsyrar i stort sett alla sektorer. Myndigheter, företag och organisationer är i hög grad beroende av fungerande informationssystem. Många företag baserar sin verksamhet på internet. Även inom den offentliga sektorn har beroendet av internet ökat bl.a. med satsningar på självbetjäningstjänster och 24-timmarsmyndigheter. Internet är också av avgörande betydelse för människors vardag, t.ex. för att söka information, kommunicera med andra eller sköta bankärenden. Denna tekniska utveckling är i allt väsentligt eftersträvansvärd och positiv.

Samtidigt har utvecklingen medfört att samhället är mer sårbart för olika former av brottsliga angrepp som riktar sig mot informationssystem. Det finns tecken på att utvecklingen går mot farligare och mer storskaliga angrepp, till exempel intrång i eller överbelastningsattacker mot bankers och myndigheters informationssystem. Angreppen begås med allt mer sofistikerade metoder och kan orsaka betydande ekonomiska skador på grund av avbrott i informationssystemens drift och i kommunikationen. Angreppen kan även orsaka förlust eller förvanskning av hemlig eller i övrigt integritetskänslig information som är av stor betydelse för enskilda.

Informationssystemens ökade betydelse visar att det är en angelägen uppgift för samhället att motverka och bekämpa angrepp mot sådana system. I det ligger att säkerställa att brottsligheten kan mötas med straffrättsliga påföljder som motsvarar brottens svårhetsgrad.

4.2 Tidigare åtgärder inom EU och Europarådet

EU:s rambeslut om angrepp mot informationssystem (2005/222/RIF)

Inom EU antogs i februari 2005 ett rambeslut om angrepp mot informationssystem (2005/222/RIF). Rambeslutet omfattade åtaganden att kriminalisera olagligt intrång i informationssystem, olaglig systemstörning och olaglig datastörning samt förstadier till dessa gärningar. Det reglerade även vilka påföljder som gärningarna ska kunna leda till. Vidare fanns bestämmelser om försvårande omständigheter, ansvar och sanktioner för juridiska personer, domsrätt samt utbyte av uppgifter. Rambeslutet föranledde ändringar i brottsbalkens bestämmelse om dataintrång. Bestämmelsen utvidgades 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. Lagändringarna trädde i kraft den 1 juni 2007 (prop. 2006/07:66, bet. 2006/07:JuU13, rskr. 2006/07:147). I och med antagandet av direktivet ersattes rambeslutet.

Europarådets konvention om it-relaterad brottslighet (Convention on Cybercrime, ETS No.185) har till stor del utgjort en förebild för såväl EU:s rambeslut om angrepp mot informationssystem som direktivet.

Konventionen innehåller bl.a. bestämmelser om vilka handlingar som ska vara straffbelagda som olagligt intrång i datorsystem, olaglig avlyssning, datastörning, systemstörning och missbruk av apparatur. Därutöver innehåller konventionen ytterligare straffbestämmelser om it-relaterade brott. Konventionen innehåller också processuella bestämmelser och bestämmelser om internationellt samarbete.

Frågor om kriminalisering av gärningar av rasistisk och främlingsfientlig natur som har begåtts med hjälp av datorsystem behandlas i ett tilläggsprotokoll till konventionen. Sverige har undertecknat, men inte tillträtt, konventionen och tilläggsprotokollet.

4.3 Gällande rätt

Den centrala straffbestämmelsen när det gäller olika former av angrepp mot informationssystem är bestämmelsen om dataintrång i 4 kap. 9 c § brottsbalken. Bestämmelsen fick sitt nuvarande innehåll genom en lagändring 2007, som i huvudsak syftade till att genomföra EU:s rambeslut om angrepp mot informationssystem. Samtidigt förtydligades bestämmelsen och moderniserades språkligt.

För *dataintrång* döms 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. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift.

Avsikten med begreppet ”uppgift som är avsedd för automatiserad behandling” är att alla uppgifter, dvs. fakta, information eller begrepp, som uttrycks i en för en dator anpassad och läsbar form ska omfattas av bestämmelsen. 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. Även uppgifter som är under befordran omfattas, oavsett på vilket sätt befordran sker (prop. 2006/07:66 s. 38 f.).

När det gäller 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 att olovlighetskravet därmed inte kan anses vara uppfyllt. Om intrånget däremot sker i radiobefordrade uppgifter som t.ex. är krypterade kan dock ansvar för dataintrång komma i fråga (s. 49).

Det handlande som straffbeläggs i bestämmelsen är för det första att någon bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling. Det krävs inte att det sker i ett visst syfte eller att det medför någon särskild effekt, t.ex. skada. Inte heller behöver någon säkerhetsåtgärd kringgås.

Vidare straffbeläggs att ändra, utplåna eller blockera en uppgift som är avsedd för automatiserad behandling. En ändring kan direkt gälla den

uppgift som ska databehandlas eller göras i det datorprogram som styr den aktuella databehandlingen. Att en uppgift utplånas innebär att den helt eller delvis förstörs genom t.ex. radering. Med begreppet blockera ska förstås åtgärder som innebär att en sådan uppgift görs oåtkomlig eller att den hindras från att flöda.

Det kan även vara straffbart att föra in en uppgift som är avsedd för automatiserad behandling i ett register. Registerbegreppet medför en begränsning av det straffbara området så till vida att endast sådana införingar som sker i uppgifter som är strukturerade på visst sätt omfattas.

Slutligen omfattar dataintrångsbestämmelsen även den som genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en uppgift som är avsedd för automatiserad behandling. Exempel på sådana åtgärder är tillgänglighets- eller överbelastningsattacker.

Bestämmelsen om dataintrång är subsidiär i förhållande till straffbestämmelserna i 4 kap. 8 och 9 §§ brottsbalken om brytande av post- eller telehemlighet respektive intrång i förvar.

Straffskalan för dataintrång sträcker sig från böter till fängelse i högst två år. Försök och förberedelse till dataintrång som om det fullbordats inte skulle ha ansetts som ringa är straffbart enligt 4 kap. 10 § brottsbalken. Av 23 kap. 2 § tredje stycket brottsbalken framgår att straffet för förberedelse ska bestämmas under den högsta och får sättas under den lägsta gräns som gäller för fullbordat brott. Högre straff än fängelse i två år får bestämmas endast om fängelse i åtta år eller däröver kan följa på det fullbordade brottet. Medverkan till dataintrång är straffbelagd enligt 23 kap. 4 § brottsbalken.

Förfaranden som innebär angrepp mot informationssystem kan även vara straffbara som t.ex. brytande av post- eller telehemlighet (4 kap. 8 § brottsbalken), skadegörelse (12 kap. 1 § brottsbalken), grov skadegörelse (12 kap. 3 § brottsbalken), sabotage (13 kap. 4 § brottsbalken), grovt sabotage (13 kap. 5 § brottsbalken) eller under vissa förutsättningar som terroristbrott enligt lagen (2003:148) om straff för terroristbrott.

5 EU:s direktiv om angrepp mot informationssystem

Europaparlamentets och rådets direktiv om angrepp mot informationssystem har ersatt det tidigare rambeslutet. Direktivets mål är att närma medlemsstaternas strafflagstiftning till varandra när det gäller angrepp mot informationssystem genom att fastställa minimiregler för brottsrekvisit och påföljder. Syftet är också att främja förebyggandet av sådana brott och förbättra samarbetet mellan rättsliga och andra behöriga myndigheter. Tyngdpunkten i direktivet utgörs av materiella straffrättsliga bestämmelser som till stor del överensstämmer med dem som finns i rambeslutet och konventionen.

Efter artikel 1 som innehåller en beskrivning av syftet med direktivet följer i artikel 2 definitioner av vissa begrepp som används i direktivet.

I artiklarna 3–7 anges de gärningar som ska vara straffbelagda när de begås uppsåtligen och orättmätigt. Ringa fall behöver dock inte straffbeläggas. Artikel 3, *Olagligt intrång i informationssystem*, reglerar intrång i informationssystem när det begås genom intrång i en säkerhetsåtgärd. Enligt artikel 4, *Olaglig systemstörning*, ska det vara straffbart 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. Av artikel 5, *Olaglig datastörning*, följer att det ska vara straffbart att radera, skada, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter i ett informationssystem. Enligt artikel 6, *Olaglig avlyssning*, ska 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 vara straffbelagda. Enligt artikel 7, *Verktyg som används för att begå brott*, ska det vara straffbart att tillverka, sälja, anskaffa i syfte att använda, importera, distribuera eller på annat sätt tillgängliggöra vissa uppräknade verktyg, om det sker orättmätigt och med uppsåt att begå något av de brott som avses i artiklarna 3–6. De verktyg som avses är datorprogram som utformats eller anpassats i första hand för att begå något av de brott som avses i artiklarna 3–6. Vidare avses ett lösenord, en åtkomstkod eller liknande uppgifter som gör det möjligt att få tillgång till ett informationssystem eller delar av ett sådant system.

I artikel 8 anges att anstiftan av och medhjälp till sådana gärningar som ska utgöra brott enligt direktivet ska straffbeläggas. Där anges även de gärningar för vilka försök ska vara straffbart, nämligen de i artiklarna 4 och 5.

Artikel 9 reglerar vilka påföljder som ska kunna dömas ut. Enligt punkt 1 ska påföljderna vara effektiva, proportionella och avskräckande. Enligt punkt 2 ska brott som avses i artiklarna 3–7 ha ett maximistraff på minst två års fängelse, åtminstone i fall som inte är ringa. Av punkt 3 följer att *olaga systemstörning* och *olaglig datastörning* ska ha ett maximistraff på minst tre års fängelse när ett betydande antal informationssystem har påverkats genom användningen av ett verktyg som avses i artikel 7 och som har utformats eller anpassats i första hand för detta syfte. För dessa brott ställs vidare i punkt 4 ett krav på lägsta maximistraff på fängelse i minst fem år om brottet:

a) begåtts inom ramen för en kriminell organisation,
b) förorsakat allvarlig skada, eller
c) begåtts mot ett informationssystem som utgör kritisk infrastruktur.

Av punkt 5 följer att det ska ses som en försvårande omständighet när *olaglig systemstörning* och *olaglig datastörning* begåtts genom missbruk av personuppgifter.

I artiklarna 10 och 11 regleras juridiska personers ansvar samt påföljder för dessa. Frågor om domsrätt regleras i artikel 12. Därefter följer i artikel 13 bestämmelser om informationsutbyte och i artikel 14 bestämmelser om övervakning och statistik. Avslutningsvis ges i artiklarna 15–19 bestämmelser om bl.a. införlivande, rapportering och

ikraftträdande. Direktivet ska vara genomfört senast den 4 september 2015.

6 Genomförandet av direktivet

Regeringens bedömning: Svensk rätt uppfyller genom befintlig lagstiftning kraven enligt direktivet med undantag för att det krävs straffskärpning för brottet dataintrång.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Flertalet remissinstanser har på ett övergripande plan förklarat sig dela bedömningarna som utredningen har gjort i betänkandet. Enligt *Stockholms universitet* är dock hållbarheten av bedömningen beträffande olovlig avlyssning i artikel 6 beroende både av hur direktivbestämmelsen tolkas och av hur principen om eterns frihet förstås. Frågan bör därför övervägas ytterligare under den fortsatta beredningsprocessen. *Hovrätten över Skåne och Blekinge* har ansett att eftersom bestämmelsen i 4 kap. 9 b § brottsbalken endast omfattar en mycket specifik befattning med det tekniska hjälpmedlet kan det finnas anledning att överväga om kraven i artikel 7 är uppfyllda i svensk rätt.

Skälen för regeringens bedömning

Genomförandet av direktivet i svensk rätt

Ett EU-direktiv är bindande med avseende på det resultat som ska uppnås men överlåter åt de nationella myndigheterna att bestämma form och tillvägagångsätt för genomförandet. I den utsträckning som det som föreskrivs i direktivet redan är uppfyllt är det tillräckligt att hänvisa till befintlig lagstiftning och andra åtgärder. Det är regeringen som ansvarar för att EU-rättsliga direktiv genomförs korrekt och i rätt tid. I den utsträckning det krävs lagändringar för att genomföra hela eller delar av ett direktiv sker det i enlighet med den ordinarie lagstiftningsprocessen, vilket innefattar sedvanlig remiss- och riksdagsbehandling.

I samband med att det nu aktuella förslaget till direktiv presenterades gjordes inom Regeringskansliet en analys av förslaget liksom av dess konsekvenser för svensk lagstiftning vid ett kommande genomförande. En faktapromemoria som beskrev innehållet i förslaget samt gällande svenska regler och förslagets effekt på dessa överlämnades till riksdagen. I faktapromemorian redogjordes bl.a. för att artiklarna 6 och 7 om olovlig avlyssning respektive befattning med vissa angivna verktyg var nya i förhållande till rambeslutet och att det krävdes ytterligare analys av bestämmelsernas överenstämmelse med svensk rätt. Vidare klargjordes att även direktivets bestämmelser om påföljder och försvårande omständigheter behövde analyseras vidare.

Därefter har en särskild utredare haft i uppdrag att bl.a. analysera behovet av och lämna förslag till de författningsändringar som krävs för att genomföra direktivet i svensk rätt.

Enligt utredningen krävs lagstiftningsåtgärder för att uppfylla direktivets bestämmelse i artikel 9 om påföljder. Utredningen har konstaterat att punkten 2 ställer krav på att vissa straffbara befattningar med verktyg som avses i artikel 7 ska vara belagda med ett maximistraff på minst två års fängelse. Enligt utredningen uppfyller svensk rätt kriminaliseringsåtagandet genom främst bestämmelserna om förberedelse till brott, bl.a. förberedelse till dataintrång. Eftersom straffskalan för dataintrång inte medger att ett fängelsestraff som uppgår till två år döms ut för förberedelse till brottet, har utredningen ansett att det krävs en skärpning av straffskalan.

Vidare har utredningen konstaterat att punkterna 3 och 4 kräver att sådana gärningar som beskrivs i artiklarna om *olaglig systemstörning* och *olaglig datastörning* i vissa fall ska vara belagda med ett maximistraff på minst tre respektive fem års fängelse. Utredningen har gjort bedömningen att svensk rätt uppfyller direktivets kriminaliseringskrav främst genom dataintrångsbestämmelsen. Eftersom det högsta straffet för dataintrång är fängelse i högst två år, har utredningen gjort bedömningen att direktivet även i denna del kräver en skärpning av straffskalan. När det gäller övriga artiklar i direktivet har utredningen gjort bedömningen att svensk rätt uppfyller de krav som ställs.

Sverige uppfyller genom befintlig lagstiftning i huvudsak kraven enligt direktivet

Regeringen delar utredningens bedömning av vilka lagstiftningsåtgärder som krävs för att Sverige ska uppfylla direktivets förpliktelser. I likhet med utredningen anser alltså regeringen att direktivet kräver en skärpning av straffet för dataintrång.

När det gäller de synpunkter som remissinstanserna har framfört gör regeringen följande överväganden.

Regeringen instämmer inledningsvis i utredningens bedömning att det som direktivet betecknar som *olovlig avlyssning* kan utgöra brytande av telehemlighet, om det är fråga om överföring av meddelanden via ett allmänt kommunikationsnät. Likaså ansluter sig regeringen till utredningens bedömning att förfarandet annars kan utgöra dataintrång bestående i att någon bereder sig tillgång till uppgifter avsedda för automatiserad behandling.

För straffansvar för brytande av telehemlighet och dataintrång krävs dock också att intrånget varit olovligt. Som regel faller då avlyssning av uppgifter som befordras via radio utanför det straffbara området. Det följer av principen om att etern är fri och att olovlighetskravet därmed inte är uppfyllt. Om intrånget däremot sker i radiobefordrade uppgifter som är t.ex. krypterade kan dock ansvar för dataintrång komma ifråga (prop. 2006/07:66 s. 49).

Utredningen har uttalat att det är osäkert hur långt principen om eterns frihet sträcker sig när det gäller information som inte kan avlyssnas med t.ex. en vanlig radiomottagare, utan vars avlyssning kräver användning av speciella tekniska hjälpmedel. Enligt regeringens mening saknas det bärande skäl för att inom ramen för detta lagstiftningsärende göra uttalanden om eller närmare beröra hur principen om eterns frihet ska avgränsas med beaktande av t.ex. den tekniska utvecklingen. En

avgörande utgångspunkt för denna bedömning är att direktivet endast ställer krav på straffbeläggande av sådan avlyssning som sker orättmätigt. I begreppet orättmätigt ligger bl.a. enligt definitionen i direktivets artikel 2 d) att handlandet inte är tillåtet enligt nationell rätt. Direktivet måste därför förstås så att ett handlande som är tillåtet i enlighet med etablerade principer i ett land, t.ex. principen om eterns frihet, inte kan anses begås orättmätigt och därmed inte omfattas av kriminaliseringsåtagandet.

Regeringen anser därför sammantaget att svensk rätt uppfyller kraven på vad som ska vara straffbelagt som olovlig avlyssning enligt artikel 6.

Beträffande sådan befattning med verktyg som ska vara straffbar enligt artikel 7 instämmer regeringen i utredningens bedömning att direktivets krav uppfylls genom främst bestämmelserna om förberedelse till de brott som motsvarar kriminaliseringsåtagandena i artiklarna 3–6, dvs. i första hand dataintrång, men även brytande av telehemlighet, skadegörelse och sabotage. Ett handlande som faller utanför tillämpningsområdet för den särskilda bestämmelsen om förberedelse till brytande av telehemlighet i 4 kap. 9 b § brottsbalken kan alltså beroende på omständigheterna vara straffbart som förberedelse till något av de andra brott som nämnts. Dessutom kan vissa av de förfaranden som beskrivs i artikeln även utgöra medverkan till brott. Regeringen bedömer därför att direktivets åtaganden i artikel 7 är uppfyllda.

Sammanfattningsvis kan således konstateras att det som framkommit vid remissbehandlingen inte föranleder regeringen att göra någon annan bedömning av behovet av lagstiftning än den som utredningen har gjort. Regeringen anser följaktligen att det krävs en lagändring i form av skärpt straff för dataintrång för att Sverige ska kunna genomföra direktivet. Regeringen gör vidare bedömningen att svensk rätt i övrigt uppfyller direktivets krav.

7 Skärpt straff för dataintrång

Regeringens förslag: Straffbestämmelsen om dataintrång ska kompletteras med en särskild straffskala och egen rubricering för grovt brott, *grovt dataintrång*. Straffet ska vara fängelse i lägst sex månader och högst sex år. Vid bedömande av om brottet är grovt ska det särskilt beaktas om gärningen har orsakat allvarlig skada eller avsett ett stort antal uppgifter eller annars varit av särskilt farlig art. Det ska vidare särskilt anges att försök och förberedelse till grovt dataintrång är straffbart. Bestämmelsen om dataintrång ska inte längre vara subsidiär i förhållande till brytande av post- eller telehemlighet och intrång i förvar.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen har som en särskild omständighet även föreslagit att gärningen *kunnat* orsaka allvarlig skada.

Remissinstanserna: Majoriteten av de remissinstanser som yttrat sig är positiva till en särskild straffskala för grovt dataintrång. Ingen

remissinstans har yttrat sig över förslaget att särskilt reglera försöks- och förberedelseansvaret för grovt dataintrång eller dataintrångs-bestämmelsens subsidiaritet. *Åklagarmyndigheten, Rikspolisstyrelsen* och *Säkerhetspolisen* har särskilt framhållit behovet av en särskild straffskala för grova dataintrång, eftersom utvecklingen synes gå mot allt farligare och mer storskaliga angrepp. *Stockholms universitet*, som i och för sig har godtagit förslaget, har dock ansett att det bör övervägas ytterligare i vilken utsträckning de gärningar som bestämmelsen tar sikte på redan utgör brott enligt andra kvalificerade bestämmelser och hur stort behovet är av den förhöjda straffskalan. *Uppsala universitet* har påpekat att införandet av det nya särskilda brottet skapar konkurrensproblem i förhållande till brotten grov skadegörelse, sabotage och i speciella fall även terroristbrott och att lagstiftaren därför bör ange en prioritetsordning mellan brotten. *Lunds universitets internetinstitut* har ansett att det tydligt bör framgå att omständigheten ”allvarlig skada” ska täckas av gärningsmannens avsikt och uppsåt. Dessutom har internetinstitutet framhållit att antalet uppgifter inte bör vara vägledande för om ett brott är grovt eftersom det av den omständigheten inte går att dra någon slutsats om skadeverkningarna. *Juliagruppen* har framfört att det grova brottet bör formuleras så att det mer betonar fall där någon försöker få fram synnerligen känsliga uppgifter eller använder sig av raffinerade och avancerade metoder. Juliagruppen har vidare framfört att lagen måste formuleras tydligare när det gäller bruk och innehav av olika verktyg för datorintrång samt att lagstiftningen bör göra skillnad på intrång och systemstörning. *Sveriges Advokatsamfund* har ansett att brottet dataintrång bör kompletteras med en bestämmelse om datastörning. Dessutom har samfundet pekat på behovet av ökade kunskaper inom it-området bland rättsväsendets företrädare och angett att möjligheterna för offentliga förvarare att få ersättning för allmänna medel för anlitandet av tekniskt sakkunnig måste ses över. Enligt *Försvarsmakten* finns det mot bakgrund av vad som avses med begreppet orättmätigt i Europarådets konvention om it-relaterad brottslighet anledning att i svensk rätt förtydliga vad som faller utanför det straffbara området när det gäller dataintrång.

Skälen för regeringens förslag

Behovet av skärpt straff

Straffskalan för dataintrång, som sträcker sig från böter till fängelse i högst två år, har inte ändrats sedan bestämmelsen först infördes i datalagen (1973:289).

Samhällsutvecklingen har inneburit att informationssystem har en ojämförligt större betydelse i samhället idag än de hade när bestämmelsen infördes. Samtidigt innebär en ökad användning av informationsteknik en förhöjd risk för att datorer och deras nätverk används som verktyg eller mål för att begå brott. Utvecklingen innebär således att samhället har blivit allt mer sårbart för it-angrepp. Under de senaste åren har också flera allvarliga och omfattande angrepp mot informationssystem mot myndigheter och organisationer uppmärksammats i såväl Sverige som utomlands. Det finns alltså tecken på att utvecklingen går mot allt farligare och återkommande storskaliga

angrepp mot viktiga informationssystem. Tendensen är förenad med utvecklingen av allt mer sofistikerade metoder, såsom skapande och användning av s.k. botnät, som innebär övertagande och fjärrstyrning av ett stort antal datorer genom att vid riktade it-angrepp infektera dem via sabotageprogram.

Storskaliga angrepp 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 dessa typer av angrepp träffas av straffansvaret för sabotage i 13 kap. 4 § brottsbalken. Även bestämmelserna om grov skadegörelse i 12 kap. 3 § brottsbalken och terroristbrott i lagen (2003:148) om straff för terroristbrott kan i vissa fall vara tillämpliga. Beroende på omständigheterna, t.ex. att skadan i och för sig är omfattande men av tillfällig karaktär eller att den infrastruktur som skadas inte har avsevärd betydelse för samhället, kan emellertid mycket straffvärda beteenden falla utanför de nämnda bestämmelsernas tillämpningsområden. Ett sådant exempel kan vara olika typer av tillgänglighetsattacker riktade mot företag och organisationer. Det kan således bli aktuellt att tillämpa dataintrångsbestämmelsen på gärningar som fått allvarliga konsekvenser för informationssystem som kan ha stor betydelse för såväl företag som enskilda.

Straffskalan för ett brott ska spegla dess allvar. Det är en grundläggande princip att allvarligare brott ska bedömas strängare än mindre allvarliga brott och att lika allvarliga brott ska bedömas lika strängt. Straffskalan måste vara utformad så att ett straff som motsvarar brottets svårhet kan dömas ut.

Mot bakgrund av vad som anförts om konsekvenserna av allvarliga och storskaliga angrepp mot informationssystem, kan det enligt regeringens mening finnas fall som har ett betydligt högre straffvärde än vad som ryms inom dagens straffskala. Härtill kommer, såsom konstaterats i avsnitt 6, att direktivet kräver skärpta lägsta maximistraff i vissa avseenden. Regeringen delar därför utredningens och flertalet remissinstansers bedömning att det finns ett behov av att vid straffvärdebedömningen kunna beakta allvaret i storskaliga och andra betydande angrepp mot informationssystem och att straffskalan för dataintrång därför bör skärpas.

En särskild straffskala och rubricering för grovt dataintrång

Regeringen anser, i likhet med utredningen, att straffskärpningen bör ske genom att bestämmelsen om dataintrång kompletteras med en särskild straffskala för grovt brott. Det grova brottet bör föras in i ett nytt andra stycke i bestämmelsen och ges en egen brottsrubricering, *grovt dataintrång*.

När det gäller straffskalans utformning har utredningen föreslagit fängelse i lägst sex månader och högst sex år. Som skäl för sin bedömning har utredningen inledningsvis lyft fram att direktivet kräver ett minsta maximistraff om fem år men ansett att ett sådant maximistraff skulle passa mindre väl in i den svenska systematiken när det gäller utformning av straffskalor. Utredningen har också bedömt att den föreslagna straffskalan är tillräckligt vid för att medge en nyanserad

bedömning av olika former av dataintrång. Slutligen har lyfts fram att utformningen av straffskalan passar väl in i brottsbalkens systematik när det gäller gradindelade brott.

Regeringen ansluter sig till utredningens bedömning och anser att den föreslagna straffskalan framstår som väl avvägd. Regeringen kan också konstatera att den föreslagna straffskalan medför att det blir möjligt att döma till fängelse i två år för förberedelse till dataintrång, vilket är nödvändigt för att uppfylla förpliktelserna i direktivet.

I likhet med vad utredningen har föreslagit bör de omständigheter som särskilt ska beaktas vid bedömningen av om brottet är grovt anges i lagtexten. En sådan utformning främjar förutsebarheten och ger en bättre ledning och en större enhetlighet i rättstillämpningen. Samtidigt bör framhållas att domstolen alltid måste göra en helhetsbedömning av samtliga omständigheter i det enskilda fallet.

När det gäller vilka omständigheter som särskilt bör nämnas delar regeringen i allt väsentligt utredningens bedömning. Som en första särskild omständighet bör således anges att gärningen har orsakat allvarlig skada. De skador som uppkommer till följd av ett dataintrång är som regel av ekonomisk karaktär men även andra typer av skador kan förekomma och bör kunna beaktas. Som utredningen har pekat på finns ett starkt intresse av att skydda säkerheten i systemen och allmänhetens tillit till dem. Därför bör till exempel allvarliga skadeverkningar som ett rubbat förtroende har fört med sig kunna beaktas. Även annan allvarlig skada än ekonomisk som drabbar enskilda till följd av dataintrånget bör kunna beaktas. Det kan handla om skada till följd av ett intrång som innebär åtkomst till synnerligen känsliga personuppgifter som kan komma att missbrukas med allvarliga konsekvenser för den enskilde. Som exempel kan nämnas uppgifter som kan röja identiteten avseende en person som har fingerade personuppgifter eller adressuppgifter för personer som medgetts kvarskrivning.

En annan omständighet som särskilt bör beaktas är gärningens omfattning. Typiskt sett är det försvårande att ett dataintrång avsett ett stort antal uppgifter. Detta bör därför utgöra en särskild omständighet som ska beaktas vid bedömande av om brottet är grovt. Under denna omständighet hör att en betydande mängd uppgifter har manipulerats på något av de sätt som nämns i bestämmelsens första stycke eller att någon har berett sig tillgång till en stor mängd uppgifter. Ett annat exempel är omfattande tillgänglighetsattacker eller andra storskaliga attacker som inneburit betydande ingrepp i viktiga kommunikationer genom att gärningsmannen har allvarligt stört eller hindrat att ett stort antal uppgifter kan användas på avsett sätt. Som *Lunds universitets internetinstitut* har framhållit bör enbart det förhållandet att gärningen avsett ett stort antal uppgifter dock inte alltid medföra att gärningen bedöms som grovt dataintrång. Omständigheterna vid t.ex. en tillgänglighetsattack kan vara sådana att den endast fått begränsade konsekvenser.

Slutligen bör även den omständigheten att en gärning varit av särskilt farlig art särskilt anges i lagtexten. Den sista omständigheten är avsedd att träffa bl.a. sådana fall där själva förfarandet i sig eller det mål som gärningen riktat sig mot är att se som en försvårande omständighet. Så kan vara fallet om tillvägagångsättet varit förslaget och gjort

brottsligheten svårupptäckt. Den omständighet som *Juliagruppen* har pekat på, dvs. att en gärning begås med raffinerade och särskilt avancerade metoder, kan alltså falla in under särskilt farlig art. Det bör även beaktas om brottet begåtts mot ett kritiskt infrastruktursystem som upprätthåller viktiga samhällsfunktioner, t.ex. inom hälso- och sjukvård eller allmänna kommunikationsmedel. Även bankers informations- och betalningssystem tillhör särskilt skyddsvärda mål.

Utredningen har som ytterligare en särskild omständighet föreslagit att gärningen *kunnat* orsaka allvarlig skada. Enligt regeringens mening kan ett handlande som kunnat orsaka allvarlig skada i vissa fall vara att anse som av särskilt farlig art, t.ex. på grund av det tillvägagångssätt som gärningsmannen använt sig av eller det mål som gärningen riktat sig mot. Att gärningsmannens syfte sträckt sig längre än till den effekt som gärningen fått är dessutom en omständighet som ska beaktas i skärpande riktning vid straffvärdesbedömningen enligt 29 kap. 2 § 1 brottsbalken.

Under vissa omständigheter kan gärningar som träffas av dataintrångsbrottet även omfattas av straffansvaret i bestämmelserna om t.ex. sabotage eller skadegörelse. Regeringen anser dock inte att det finns tillräckliga skäl för att, såsom *Uppsala universitet* efterfrågat, ange en prioritetsordning mellan brotten. Utgångspunkten är att sedvanliga konkurrensregler ska tillämpas. Det innebär normalt att när det är fråga om konkurrens mellan dataintrångsbrottet och ett annat brott med samma skyddsintresse ska 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.

Eftersom de objektiva rekvisiten för dataintrång i bestämmelsens första stycke inte är föremål för överväganden i detta lagstiftningsarbete finns inte anledning att här göra några uttalanden om hur t.ex. rekvisitet ”olovligen” ska förstås såsom *Försvarsmakten* har förespråkat.

När det gäller *Sveriges Advokatsamfunds* och *Juliagruppens* förslag att komplettera dataintrångsbestämmelsen med en bestämmelse om datastörning konstaterar regeringen att en sådan ändring kräver överväganden och en omarbetning av dataintrångsbestämmelsen som inte låter sig göras inom ramen för detta lagstiftningsarbete. Inte heller frågorna om bruk av verktyg för datorintrång och möjligheterna till ersättning av allmänna medel för anlitandet av tekniskt sakkunnig kan behandlas i detta sammanhang.

Konsekvenser av förslaget

Den föreslagna straffskalan för grovt dataintrång får vissa konsekvenser bl.a. för möjligheten att använda straffprocessuella tvångsmedel. Bland annat medför den möjlighet att besluta om hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning under förutsättning att domstolen gör bedömningen att brottets straffvärde är högre än två år.

Förslaget påverkar också preskriptionstidens längd. För grovt dataintrång kommer preskriptionstiden att bli tio år.

Regeringen bedömer liksom utredningen att dessa konsekvenser är rimliga.

Försök och förberedelse till grovt dataintrång

Försök och förberedelse till dataintrång som om det fullbordats inte skulle ha ansetts som ringa är straffbart enligt 4 kap. 10 § brottsbalken. Eftersom en särskild straffskala med en egen brottsrubricering införs för grovt brott bör 10 § kompletteras så att det uttryckligen framgår att straffansvaret för försök och förberedelse gäller även grovt dataintrång.

Dataintrångsbestämmelsens förhållande till brytande av post- eller telehemlighet och intrång i förvar

Bestämmelsen om dataintrång är uttryckligen subsidiär i förhållande till brytande av post- eller telehemlighet och intrång i förvar.

När bestämmelsen om dataintrång fanns i datalagen var den subsidiär i förhållande till brottsbalken och straffbestämmelserna i lagen (1990:409) om skydd för företagshemligheter. När dataintrångsbestämmelsen överfördes till brottsbalken slopades subsidiaritetsklausulen i förhållande till lagen om skydd mot företagshemligheter. Samtidigt klargjordes förhållandet till bestämmelserna om straff för brytande av post- eller telehemlighet och intrång i förvar uttryckligen i bestämmelsen.

Den ändring som regeringen nu föreslår innebär att dataintrångsbestämmelsen kompletteras med en särskild straffskala och brottsrubricering för grovt brott. Motsvarande straffskala och gradindelning finns inte för brytande av post- eller telehemlighet eller intrång i förvar. Mot den bakgrunden är det inte lämpligt att behålla subsidiariteten i förhållande till de straffbestämmelserna. Inte heller i övrigt finns det skäl för att behålla den nuvarande ordningen.

Regeringen delar därför utredningens bedömning att dataintrångsbestämmelsen inte längre bör vara subsidiär i förhållande till brytande av post- eller telehemlighet och intrång i förvar. Förhållandet mellan bestämmelsen om dataintrång och bestämmelserna om brytande av post- eller telehemlighet och om intrång i förvar får i fortsättningen i stället avgöras enligt sedvanliga principer för bedömningen av konkurrens mellan överlappande straffstadganden i brottsbalken.

Slutsatser

Sammanfattningsvis föreslår regeringen följande. Straffbestämmelsen om dataintrång kompletteras med en särskild straffskala och egen rubricering för grovt brott, *grovt dataintrång*. Straffet ska vara fängelse i lägst sex månader och högst sex år. Vid bedömande av om brottet är grovt ska det särskilt beaktas om gärningen har orsakat allvarlig skada eller avsett ett stort antal uppgifter eller annars varit av särskilt farlig art. Det ska vidare särskilt anges att försök och förberedelse till grovt dataintrång är straffbart. Bestämmelsen om dataintrång ska inte längre vara subsidiär i förhållande till brytande av post- eller telehemlighet och intrång i förvar.

8 Straffskalan för brytande av post- eller telehemlighet

Regeringens bedömning: Det finns inget behov av att ändra straffskalan för brytande av post- eller telehemlighet.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Det stora flertalet av remissinstanserna har inte yttrat sig särskilt i frågan. *Myndigheten för samhällsskydd och beredskap* har delat utredningens bedömning. *Sveriges Advokatsamfund* och *IT & Telekomföretagen* har emellertid uppfattningen att straffskalan för brytande av post- eller telehemlighet bör ändras på samma sätt som föreslås beträffande dataintrång. Samfundet har dessutom framfört att även straffbestämmelserna om intrång i förvar och olovlig avlyssning bör kompletteras med ett grovt brott.

Skälen för regeringens bedömning: Enligt 4 kap. 8 § brottsbalken döms den som olovligen bereder sig tillgång till ett meddelande, som ett post- eller telebefordringsföretag förmedlar som postförsändelse eller i telemeddelande för brytande av post- eller telehemlighet till böter eller fängelse i högst två år. Bestämmelsen skyddar såväl meddelanden i traditionell form som elektroniska meddelanden. Den brottsliga gärningen består i att bereda sig tillgång till meddelandet. För ansvar förutsätts uppsåt och att handlingen vidtas olovligen. Straffskalan har varit oförändrad sedan brottsbalkens tillkomst.

Av den officiella kriminalstatistiken framgår att antalet lagföringar för brottet har varit ytterst få. Totalt har det rört sig om ett 20-tal lagföringar under den senaste tioårsperioden. Som utredningen har konstaterat går det inte av statistiken att utläsa hur många – om ens någon – av lagföringarna som har avsett intrång i elektroniska meddelanden.

Regeringen delar utredningens bedömning att det är svårt att se att det förfarande som bestämmelsen straffbelägger skulle kunna orsaka motsvarande skada och få så vittgående konsekvenser som vissa av de förfaranden som dataintrångsbestämmelsen straffbelägger. I de fall ett intrång i ett elektroniskt meddelande under befordran utgör ett led i ett storskaligt angrepp torde angreppet regelmässigt också träffas av straffansvaret i bestämmelserna om dataintrång, sabotage, skadegörelse eller terroristbrott. Det finns heller inget krav i direktivet som innebär att straffskalan för brytande av post- eller telehemlighet måste ändras.

I likhet med utredningen gör regeringen därför bedömningen att den nuvarande straffskalan är väl avvägd. En oförändrad straffskala för brytande av post- eller telehemlighet innebär vidare att straffskalan även fortsättningsvis kommer att vara densamma som för straffbestämmelserna om intrång i förvar och olovlig avlyssning. Det finns inom ramen för detta lagstiftningsarbete inte förutsättningar att göra en sådan översyn av straffskalorna för intrång i förvar och olovlig avlyssning som *Sveriges Advokatsamfund* efterfrågar.

Sammanfattningsvis anser regeringen att det för närvarande inte finns något behov av att ändra straffskalan för brytande av post- eller telehemlighet.

9 Ikraftträdande- och övergångsbestämmelser

Regeringens förslag: Lagändringarna ska träda i kraft den 1 juli 2014.

Regeringens bedömning: Några särskilda övergångsbestämmelser behövs inte.

Utredningens förslag och bedömning: Utredningen har föreslagit att lagändringarna ska träda i kraft den 1 januari 2015. Utredningen har bedömt att lagändringarna inte kräver några särskilda övergångsbestämmelser.

Remissinstanserna: Ingen av remissinstanserna har yttrat sig särskilt i frågan.

Skälen för regeringens förslag och bedömning: Lagändringarna bör träda i kraft så snart som möjligt. Regeringen föreslår att detta sker den 1 juli 2014. Det krävs inga särskilda övergångsbestämmelser.

10 Ekonomiska konsekvenser

Regeringens bedömning: De föreslagna ändringarna leder inte till annat än begränsade kostnadsökningar. Dessa kan finansieras inom ramen för befintliga anslag.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Ingen av remissinstanserna har särskilt yttrat sig i frågan.

Skälen för regeringens bedömning: De föreslagna lagändringarna innebär bl.a. att dataintrångsbrottet kompletteras med en särskild straffskala och egen rubricering för grovt brott, grovt dataintrång. Straffet ska vara fängelse i lägst sex månader och högst sex år. Ändringen kan antas resultera i att påföljden för allvarliga dataintrång i fler fall än i dag kommer att bestämmas till fängelse, vilket kan medföra en viss ökning av Kriminalvårdens kostnader. Det kan heller inte uteslutas att begränsade merkostnader kan uppkomma för Polisen, åklagare och domstolarna till följd av att möjligheten att använda vissa tvångsmedel ökar genom förslaget och att en längre preskriptionstid kommer att gälla för grovt dataintrång i förhållande till dataintrång. Regeringen gör bedömningen att eventuella merkostnader kan finansieras inom myndigheternas befintliga anslag.

11 Författningskommentar

Förslaget till lag om ändring i brottsbalken

4 kap.

9 c § 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 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.

Är brottet grovt, döms för grovt dataintrång till fängelse i lägst sex månader och högst sex år. Vid bedömande av om brottet är grovt ska det särskilt beaktas om gärningen har orsakat allvarlig skada eller avsett ett stort antal uppgifter eller annars varit av särskilt farlig art.

Ändringen av paragrafen, som föreskriver straffansvar för dataintrång, har behandlats i avsnitt 7.

Ändringen i *första stycket* innebär att bestämmelsen inte längre är subsidiär i förhållande till straffbestämmelserna i 4 kap. 8 och 9 §§ brottsbalken om brytande av post- eller telehemlighet och intrång i förvar.

I *andra stycket*, som är nytt, införs en särskild straffskala och rubricering för grovt dataintrång. Straffskalan är fängelse i lägst sex månader och högst sex år. Ändringen syftar till att det vid allvarliga fall av dataintrång ska vara möjligt att döma ut ett straff som står i proportion till brottets allvar.

Vid bedömande av om brottet är grovt ska det särskilt beaktas om gärningen har orsakat allvarlig skada eller avsett ett stort antal uppgifter eller annars varit av särskilt farlig art. Omständigheten ska vara täckt av den tilltalades uppsåt.

Med allvarlig skada avses främst betydande ekonomiska skador. Vid sidan av de rent ekonomiska effekterna kan det emellertid även finnas andra skador som särskilt bör beaktas. Allvarliga skadeverkningar som ett rubbat förtroende har fört med sig för en verksamhet kan beaktas som en allvarlig skada i bestämmelsens mening. Även annan allvarlig skada än ekonomisk som drabbar enskilda till följd av dataintrånget bör kunna beaktas. Det kan handla om skada till följd av ett intrång som innebär åtkomst till synnerligen känsliga personuppgifter som kan komma att missbrukas med allvarliga konsekvenser för den enskilde. Som exempel kan nämnas uppgifter som kan röja identiteten avseende en person som har fingerade personuppgifter eller adressuppgifter för personer som medgetts kvarskrivning.

Med att gärningen avsett ett stort antal uppgifter avses bl.a. omfattande spridning av datavirus eller andra sabotageprogram. Även fall där ett stort antal uppgifter har raderats eller ändrats eller om någon har berett sig tillgång till en stor mängd uppgifter kan medföra att brottet bedöms som grovt. Ett annat exempel är omfattande tillgänglighetsattacker eller andra storskaliga attacker som inneburit betydande ingrepp i viktiga kommunikationer genom att gärningsmannen allvarligt har stört eller hindrat att ett stort antal uppgifter kan användas på avsett sätt. Enbart det

förhållande att gärningen avsett ett stort antal uppgifter bör dock inte alltid medföra att gärningen bedöms som grovt dataintrång. Omständigheterna vid t.ex. en tillgänglighetsattack kan vara sådana att den endast fått begränsade konsekvenser.

Med att gärningen annars varit av särskilt farlig art avses bl.a. fall där själva förfarandet i sig eller det mål som gärningen riktat sig mot är att se som en försvårande omständighet. Så kan vara fallet om tillvägagångsättet varit förslaget och gjort brottsligheten svårupptäckt. Också när gärningar begås med raffinerade metoder såsom t.ex. användningen av botnät, det vill säga övertagande och fjärrstyrning av ett stort antal datorer genom att infektera dem via sabotageprogram genom riktade angrepp, kan det vara fråga om särskilt farlig art. Det bör även beaktas om brottet begåtts mot ett kritiskt infrastruktursystem som upprätthåller viktiga samhällsfunktioner, t.ex. inom hälso- och sjukvård eller allmänna kommunikationsmedel. Även bankers informations- och betalningssystem tillhör särskilt skyddsvärda mål.

Uppräkningen är inte uttömmande utan även andra försvårande omständigheter ska beaktas. Domstolen ska göra en helhetsbedömning av samtliga omständigheter i det enskilda fallet.

Förhållandet mellan dataintrång och övriga brott får avgöras enligt sedvanliga konkurrensregler. Det innebär normalt att när det är fråga om konkurrens mellan dataintrångsbrottet och ett annat brott med samma skyddsintresse, så ska domstolen enbart döma för det brott som har den strängare straffskalan. För övriga konkurrenssituationer som kan förekomma får domstolen göra en prövning i varje enskilt fall enligt gällande konkurrensprinciper.

10 § För försök, förberedelse eller stämpling till människorov, människohandel eller olaga frihetsberövande och för underlåtenhet att avslöja *ett* sådant brott döms *det* till ansvar enligt 23 kap. Detsamma gäller för försök eller förberedelse till olaga tvång som är grovt, dataintrång som om det fullbordats inte skulle ha varit att anse som ringa, *eller grovt dataintrång*.

Paragrafen har ändrats på så sätt att grovt dataintrång har lagts till i sista meningen. Ändringen innebär att det uttryckligen framgår att försök och förberedelse till grovt dataintrång är straffbart. Ändringen har behandlats i avsnitt 7. Paragrafen har också ändrats språkligt.

L 218/8 SV Europeiska unionens officiella tidning 14.8.2013

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 rättssystem. 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*

Sammanfattning av betänkandet Europarådets konvention om it-relaterad brottslighet (SOU 2013:39)

Behovet av lagändringar mot bakgrund av direktivet

Inom EU antogs 2005 ett rambeslut om angrepp mot informationssystem. Europaparlamentets och rådets direktiv om angrepp mot informationssystem och om ersättande av rambeslut 2005/222/RIF syftar till att ytterligare närma medlemsstaternas strafflagstiftning till varandra på området för angrepp mot informationssystem och att ändra och utöka bestämmelserna i rambeslutet. Vidare är avsikten att förbättra samarbetet mellan myndigheter och brottsbekämpande organ i medlemsstaterna.

Tyngdpunkten i direktivet utgörs av materiellt straffrättsliga bestämmelser. Bestämmelserna överensstämmer till stor del med de som finns i Europarådets konvention om it-relaterad brottslighet. Till skillnad från konventionen ställer direktivet emellertid precisa krav på vilka påföljder som ska kunna dömas ut för vissa av brotten i direktivet.

Enligt artikel 9.3 och 9.4 ska brotten olaglig systemstörning och olaglig datastörning i vissa fall vara belagda med ett maximistraff på minst tre respektive fem års fängelse. Svensk rätt uppfyller genom främst dataintrångsbestämmelsen direktivets krav på vilka handlingar som ska vara straffbelagda som olaglig systemstörning och olaglig datastörning. Straffskalan för dataintrång är böter eller fängelse i högst två år. Utredningen bedömer därför att straffskalan för dataintrång måste skärpas för att Sverige ska kunna genomföra direktivet. Av artikel 9.2 följer vidare att vissa straffbara befattningar med verktyg ska vara belagda med ett maximistraff på minst två års fängelse. Svensk rätt uppfyller i denna del kravet på straffbarhet genom främst bestämmelserna om förberedelse till brott, bl.a. förberedelse till dataintrång. För förberedelse till dataintrång är det inte möjligt att döma till två års fängelse. Det krävs alltså även av detta skäl en skärpning av straffskalan för dataintrång.

I övrigt anser utredningen att svensk rätt redan uppfyller de krav som ställs i direktivet.

En särskild straffskala för grovt dataintrång

Straffskalan för brytande av post- eller telehemlighet sträcker sig från böter till fängelse två år. Enligt utredningens mening är den nuvarande straffskalan alltjämt väl avvägd. Något skäl att skärpa straffet för brytande av post- eller telehemlighet anser utredningen alltså inte finnas.

Även straffskalan för dataintrång sträcker sig från böter till fängelse två år. Den nuvarande straffskalan för dataintrång ger emellertid enligt utredningens uppfattning inte tillräckligt utrymme för att kunna beakta allvaret i storskaliga angrepp mot informationssystem. Av olika skäl är det inte alltid möjligt att vid sådana angrepp mot informationssystem tillämpa andra straffbestämmelser med högre straffskalor, såsom bestämmelserna om sabotage, grov skadegörelse och terroristbrott. Enligt

utredningens mening finns kriminalpolitiska skäl för att skärpa straffskalan för dataintrång.

Utredningen föreslår därför att det införs en särskild straffskala för grovt dataintrång. Straffskalan ska sträcka sig från fängelse sex månader till fängelse sex år. Vid bedömande av om ett dataintrång är grovt ska särskilt beaktas om gärningen har orsakat eller kunnat orsaka allvarlig skada eller har avsett ett stort antal uppgifter eller om gärningen annars varit av särskilt farlig art.

Bestämmelsen om dataintrång ska inte längre vara subsidiär i förhållande till straffbestämmelserna om brytande av post- eller telehemlighet och om intrång i förvar. Försök och förberedelse till grovt dataintrång ska vara straffbart.

Betänkandets lagförslag

Förslag till lag om ändring i brottsbalken

Härigenom föreskrivs att 4 kap. 9 c och 10 §§ brottsbalken ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
4 kap.	
9 c §[4]	
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.	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 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. *Om brottet är grovt, döms för grovt dataintrång till fängelse i lägst sex månader och högst sex år. Vid bedömande av om brottet är grovt ska särskilt beaktas om gärningen har orsakat eller kunnat orsaka allvarlig skada eller har avsett ett stort antal uppgifter eller om gärningen annars varit av särskilt farlig art.*
10 §[5]	
För försök, förberedelse eller stämpling till människorov, människohandel eller olaga frihetsberövande och för underlåtenhet att avslöja sådant brott döms till ansvar enligt vad som sägs i 23 kap. Detsamma gäller för försök eller förberedelse till olaga tvång som är grovt eller till dataintrång som om det fullbordats inte skulle ha varit att anse som ringa.	För försök, förberedelse eller stämpling till människorov, människohandel eller olaga frihetsberövande och för underlåtenhet att avslöja sådant brott döms till ansvar enligt vad som sägs i 23 kap. Detsamma gäller för försök eller förberedelse till olaga tvång som är grovt, till dataintrång som om det fullbordats inte skulle ha varit att anse som ringa, *eller till grovt dataintrång*.

[4] Senaste lydelse 2007:213.
[5] Senaste lydelse 2004:406.

Denna lag träder i kraft den 1 januari 2015.

Förteckning över remissinstanserna

Efter remiss har yttrande över betänkandet avgetts av Riksdagens ombudsmän, Hovrätten för Västra Sverige, Hovrätten över Skåne och Blekinge, Helsingborgs tingsrätt, Hässleholms tingsrätt, Göteborgs tingsrätt, Gävle tingsrätt, Luleå tingsrätt, Justitiekanslern, Domstolsverket, Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen, Säkerhetspolisen, Statens kriminaltekniska laboratorium, Säkerhets- och integritetsskyddsnämnden, Brottsförebyggande rådet, Migrationsverket, Datainspektionen, Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt, Myndigheten för samhällsskydd och beredskap, Kustbevakningen, Totalförsvarets forskningsinstitut, Barnombudsmannen, Länsstyrelsen i Stockholms län, Statskontoret, Tullverket, Skatteverket, Uppsala universitet (Juridiska fakultetsnämnden), Stockholms universitet (Juridiska fakultetsnämnden), Post- och telestyrelsen, Diskrimineringsombudsmannen, Bahnhof AB, ECPAT Sverige, Rättighetsalliansen, IT&Telekomföretagen, Svenska Journalistförbundet, Sveriges advokatsamfund och Juliagruppen.

Yttrande har också inkommit från Lunds universitets internetinstitut och .SE (Stiftelsen för Internetinfrastruktur).

Svenskt Näringsliv har avstått från att yttra sig.

Centrum mot rasism, Stiftelsen Expo, SIG Security, Svenska avdelningen av Internationella juristkommissionen, Civil Rights Defenders, Svenska Tidningsutgivareföreningen, Föreningen Utgivarna, Sveriges Domareförbund, Netnod Internet Exchange i Sverige AB, Tele2 AB och TeliaSonera AB har beretts tillfälle att avge yttrande men har avstått.

Lagrådsremissens lagförslag

Förslag till lag om ändring i brottsbalken

Härigenom föreskrivs[6] att 4 kap. 9 c och 10 §§ brottsbalken ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
4 kap.	
9 c §[7]	
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.	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 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.
	Är brottet grovt, döms för grovt dataintrång till fängelse i lägst sex månader och högst sex år. Vid bedömande av om brottet är grovt ska det särskilt beaktas om gärningen har orsakat allvarlig skada eller avsett ett stort antal uppgifter eller annars varit av särskilt farlig art.
10 §[8]	
För försök, förberedelse eller stämpling till människorov, människohandel eller olaga frihetsberövande och för underlåtenhet att avslöja sådant brott döms till ansvar enligt *vad som sägs i* 23 kap. Detsamma gäller för försök eller förberedelse till olaga tvång som är grovt *eller*	För försök, förberedelse eller stämpling till människorov, människohandel eller olaga frihetsberövande och för underlåtenhet att avslöja sådant brott döms *det* till ansvar enligt 23 kap. Detsamma gäller för försök eller förberedelse till olaga tvång som är grovt*,* dataintrång som om det

[6] Jfr 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 (EUT L 218, 14.8.2013, s. 8–14, Celex 32013L0040).
[7] Senaste lydelse 2007:213.
[8] Senaste lydelse 2004:406.

till dataintrång som om det fullbordats inte skulle ha varit att anse som ringa.	fullbordats inte skulle ha varit att anse som ringa*, eller grovt dataintrång*.

Denna lag träder i kraft den 1 juli 2014.

Lagrådets yttrande

Utdrag ur protokoll vid sammanträde 2014-01-21

Närvarande: F.d. justitierådet Leif Thorsson samt justitieråden Gudmund Toijer och Olle Stenman.

Skärpt straff för dataintrång

Enligt en lagrådsremiss den 16 januari 2014 (Justitiedepartementet) har regeringen beslutat inhämta Lagrådets yttrande över förslag till lag om ändring i brottsbalken.

Förslaget har inför Lagrådet föredragits av rättssakkunniga Jenny Engvall.

Lagrådet lämnar förslaget utan erinran.

Justitiedepartementet

Utdrag ur protokoll vid regeringssammanträde den 13 februari 2014

Närvarande: Statsministern Reinfeldt, ordförande, och statsråden Björklund, Bildt, Ask, Larsson, Erlandsson, Borg, Ohlsson, Norman, Attefall, Engström, Kristersson, Elmsäter-Svärd, Ullenhag, Hatt, Ek, Lööf, Enström, Arnholm, Svantesson

Föredragande: statsrådet Ask

Regeringen beslutar proposition 2013/14:92 Skärpt straff för dataintrång

Författningsrubrik	Bestämmelser som inför, ändrar, upphäver eller upprepar ett normgivningsbemyndigande	Celexnummer för bakomliggande EU-regler
Lag om ändring i brottsbalken		32013L0040