RP 232/2014 rd

Regeringens proposition till riksdagen med förslag till lagar om ändring av vissa bestämmelser om nätbrott i strafflagen och av vissa lagar som har samband med den

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det ändringar i strafflagen, tvångsmedelslagen, polislagen och militära rättegångslagen. Genom de föreslagna lagarna genomförs Europaparlamentets och rådets direktiv om angrepp mot informationssystem.

Enligt propositionen ska anskaffning av ett hjälpmedel vid nätbrott i syfte att använda det kriminaliseras som orsakande av fara för informationsbehandling. I lagen föreslås det en ny kriminalisering som gäller dataskadegörelse samt en grov och lindrig gärningsform av dataskadegörelse. Det föreslås att maximistraffet för dataskadegörelse ska vara fängelse i två år. Maximistraffet för grov dataskadegörelse ska vara fem års fängelse. Kvalifikationsgrunderna hänför sig till användningen av s.k. botnät, kriminella sammanslutningar, betydande skada och kritisk infrastruktur. Bestämmelserna om åtalsrätt, åtgärdseftergift och juridiska personers straffansvar ändras för att motsvara den ändring som nämns ovan.

Enligt propositionen ska kränkning av kommunikationshemlighet även täcka överföring av konfidentiella data inom ett informationssystem. Maximistraffet för kränkning av kommunikationshemlighet höjs till två års fängelse. Subsidiaritetsklausulen i fråga om systemstörning slopas. Det föreslås också att i bestämmelserna om grovt störande av post- och teletrafik och grov systemstörning ska tas in motsvarande kvalifikationsgrunder som för grov dataskadegörelse. Maximistraffet för de nämnda grova gärningsformerna ska vara fem års fängelse. Enligt propositionen ska dataintrång även täcka att skaffa sig tillgång till eller ta reda på data i ett informationssystem. Maximistraffet för dataintrång höjs till två års fängelse. Med anledning av detta föreslås det att också maximistraffet för grovt dataintrång ska höjas från två till tre års fängelse. I lagen föreslås det även en ny bestämmelse med definitioner av informationssystem och data, i enlighet med förpliktelserna i direktivet.

Tvångsmedelslagen och polislagen ändras så att de motsvarar de ändringar i strafflagen som anges ovan.

I strafflagen föreslås dessutom en ny bestämmelse som gäller identitetsstöld. Identitetsstöld ska vara ett målsägandebrott. Identitetsstöld fogas även till förteckningen i militära rättegångslagen över de brott som ska handläggas som militära rättegångsärenden.

Lagarna avses träda i kraft den 4 september 2015, då direktivet ska genomföras i medlemsstaterna.

297394

INNEHÅLL

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL 1
INNEHÅLL 2
ALLMÄN MOTIVERING 3
1 INLEDNING 3
2 NULÄGE 3
2.1 Lagstiftning 3
2.2 Den internationella utvecklingen och lagstiftningen i EU 3
2.3 Bedömning av nuläget 4
3 MÅLSÄTTNING OCH DE VIKTIGASTE FÖRSLAGEN 4
4 PROPOSITIONENS KONSEKVENSER 5
5 BEREDNINGEN AV PROPOSITIONEN 6
6 ANDRA OMSTÄNDIGHETER SOM INVERKAT PÅ PROPOSITIONENS INNEHÅLL 8
DETALJMOTIVERING 9
1 DIREKTIVETS INNEHÅLL OCH FÖRHÅLLANDE TILL LAGSTIFTNINGEN I FINLAND 9
2 LAGFÖRSLAG 31
2.1 Strafflagen 31
34 kap. Om allmänfarliga brott 31
35 kap. Om skadegörelse 31
38 kap. Om informations- och kommunikationsbrott 34
2.2 Tvångsmedelslagen 39
2.3 Polislagen 39
2.4 Militära rättegångslagen 40
3 IKRAFTTRÄDANDE 40
4 FÖRHÅLLANDE TILL GRUNDLAGEN SAMT LAGSTIFTNINGSORDNING 40
LAGFÖRSLAG 42
1. Lag om ändring av strafflagen 42
2. Lag om ändring av 10 kap. 3 och 6 § i tvångsmedelslagen 46
3. Lag om ändring av 5 kap. 8 § i polislagen 47
4. Lag om ändring av 2 § i militära rättegångslagen 48
BILAGA 49
PARALLELLTEXTER 49
1. Lag om ändring av strafflagen 49
2. Lag om ändring av 10 kap. 3 och 6 § i tvångsmedelslagen 58
3. Lag om ändring av 5 kap. 8 § i polislagen 60
4. Lag om ändring av 2 § i militära rättegångslagen 62

ALLMÄN MOTIVERING

1 Inledning

Syftet med propositionen är att få den finska lagstiftningen att motsvara de krav som följer av Europaparlamentets och rådets direktiv 2013/40/EU om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF, nedan direktivet eller nätbrottsdirektivet. Den finska lagstiftningen om nätbrott reviderades senast i omfattande utsträckning vid det nationella ikraftsättandet av den i Budapest den 23 november 2001 ingångna Europarådskonventionen om it-relaterad brottslighet (CETS 185), nedan konventionen eller nätbrottskonventionen (FördrS 60/2007, RP 153/2006 rd). I det sammanhanget ändrades lagstiftningen så att den uppfyllde kraven i Europeiska unionens råds rambeslut av den 24 februari 2005 om angrepp mot informationssystem (2005/222/RIF, EUT L 69/67, 16.3.2005), nedan rambeslutet, som ersätts med det nu aktuella direktivet. I rambeslutet finns det bestämmelser om samma saker som i konventionen.

Direktivet innehåller i stor utsträckning samma bestämmelser som konventionen och rambeslutet. I konventionen finns det dock ännu mer heltäckande och omfattande bestämmelser om nätbrott än i rambeslutet och direktivet. Den innehåller bl.a. bestämmelser om internationellt samarbete i straffrättsliga frågor. Ett av syftena med direktivet är också att få lagstiftningen i alla medlemsstaterna att uppfylla vissa krav i konventionen. Direktivet innehåller emellertid en del kompletteringar jämfört med de tidigare instrumenten, bl.a. bestämmelser om s.k. botnät och missbruk av identitetsuppgifter. Dessutom harmoniseras genom direktivet de lägsta nivåerna på maximistraffen för de brott som avses där i större utsträckning än i rambeslutet. Nätbrotten och många frågor som i sak motsvarar direktivet behandlas utförligt i den regeringsproposition, 153/2006 rd, som gäller konventionen och rambeslutet. Man kan således hänvisa till den regeringspropositionen när det gäller den allmänna presentationen av ämnesområdet och många av bestämmelserna, och det är inte ändamålsenligt med en upprepning i denna proposition.

Denna proposition täcker endast de kompletteringar av den gällande lagstiftningen som direktivet förutsätter.

De författningar som krävs för att följa direktivet ska sättas i kraft senast den 4 september 2015.

2 Nuläge

2.1 Lagstiftning

Den nationella lagstiftningen i Finland har ändrats i samband med ikraftsättandet av konventionen och åtgärderna för att genomföra rambeslutet så att den till många delar uppfyller kraven i direktivet. Av betydelse med tanke på direktivet är strafflagens (39/1889) 38 kap. om informations- och kommunikationsbrott. I det kapitlet finns bl.a. med tanke på direktivet väsentliga bestämmelser om kränkning av kommunikationshemlighet (3 §), grov kränkning av kommunikationshemlighet (4 §), störande av post- och teletrafik (5 §), grovt störande av post- och teletrafik (6 §), lindrigt störande av post- och teletrafik (7 §), systemstörning (7 a §), grov systemstörning (7 b §), dataintrång (8 §) och grovt dataintrång (8 a §). Också strafflagens 34 kap. om allmänfarliga brott, där det bl.a. föreskrivs om orsakande av fara för informationsbehandling (9 a §) och innehav av hjälpmedel vid nätbrott (9 b §) är av betydelse med tanke på direktivet. Även bestämmelserna om skadegörelse i 35 kap. är relevanta.

2.2 Den internationella utvecklingen och lagstiftningen i EU

Den internationella lagstiftning som hänför sig till nätbrott har varit föremål för en förhållandevis intensiv utveckling. Den ovan nämnda nätbrottskonventionen, som utarbetats inom Europarådet och som varit förebild

också för det direktiv som behandlas i denna proposition, kan fortfarande anses som det viktigaste internationella instrumentet. På grund av nätbrottslighetens globala och i högsta grad gränsöverskridande karaktär är målet att så många stater som möjligt också utanför Europarådet ska tillträda konventionen. Eftersom inte ens alla EU-medlemsstaterna i dag har tillträtt konventionen, kan detta direktiv antas bidra till att även de stater som ännu inte har gjort det tillträder konventionen.

Ett annat viktigt instrument är det tidigare nämnda EU-rambeslutet, som har ersatts med det direktiv som avses i denna proposition. Rambeslutet innehöll bestämmelser om samma frågor som konventionen.

2.3 Bedömning av nuläget

Den finska strafflagstiftningen uppfyller redan nu i hög grad kraven i direktivet, på grund av de åtgärder som vidtogs för att sätta i kraft konventionen och genomföra rambeslutet. De viktigaste ändringarna som direktivet förutsätter hänför sig till att höja maximistraffnivåerna och ta in en del straffskärpningsgrunder i den nationella lagstiftningen.

3 Målsättning och de viktigaste förslagen

Syftet med propositionen är att få den finska lagstiftningen att uppfylla kraven i direktivet. I propositionen föreslås det att man gör de ändringar i strafflagen som direktivet förutsätter.

Det föreslås att till orsakande av fara för informationsbehandling i strafflagens 34 kap. 9 a § fogas gärningssättet anskaffar i syfte att använda ett hjälpmedel vid nätbrott. Innehav är straffbart redan i dag enligt 9 b §. Ändringen är delvis teknisk, eftersom det inte på grund av direktivet finns någon orsak att höja maximistraffet för innehav från ett fängelsestraff på sex månader till två års fängelse. I kapitlet föreslås också en ny 14 §, där det i fråga om orsakande av fara för informationsbehandling som avses i 9 a § och innehav av hjälpmedel vid nätbrott som avses i 9 b § hänvisas till den föreslagna nya 38 kap. 13 §, som innehåller definitioner av informationssystem och data.

I strafflagens 35 kap. föreslås en ny kriminalisering som gäller dataskadegörelse (3 a §) och en grov (3 b §) och lindrig (3 c §) gärningsform av dataskadegörelse. De ändringarna görs främst av tekniska skäl och för att det inte finns anledning att utsträcka bl.a. den höjning av maximistraffet som direktivet förutsätter till att omfatta vanlig skadegörelse. Det föreslås därför att 2 och 3 mom. i kapitlets 1 §, som gäller skadegörelse, och 1 mom. 2 punkten i 2 §, som gäller grov skadegörelse, upphävs. Även gärningssätten för dataskadegörelse preciseras. Grov dataskadegörelse innehåller de kvalifikationsgrunder för vars del direktivet förutsätter ett lägsta maximistraff på tre och fem års fängelse när det gäller dataskadegörelse. De kvalifikationsgrunderna hänför sig till användningen av s.k. botnät, kriminella sammanslutningar, betydande skada och kritisk infrastruktur. När de gärningar som utgör dataskadegörelse avskiljs till självständiga kriminaliseringar krävs det också en teknisk ändring av 6 § om åtalsrätt, 7 § om åtgärdseftergift och 8 § om straffansvar för juridiska personer, så att de bestämmelserna motsvarar den ändring som nämns ovan. I kapitlet föreslås också en ny 9 §, där det i fråga om dataskadegörelse som avses i 3 a § och grov dataskadegörelse som avses i 3 b § hänvisas till den föreslagna nya 38 kap.13 §, som innehåller definitioner av informationssystem och data.

Det föreslås att kränkning av kommunikationshemlighet i 38 kap. 3 § i strafflagen ändras så att den även täcker överföring av konfidentiella data inom ett informationssystem, i enlighet med kraven i direktivet. Dessutom föreslås det att maximistraffet för kränkning av kommunikationshemlighet höjs till två års fängelse. För att undvika att det uppstår oändamålsenliga situationer vid tillämpningen av bestämmelsen på grund av de ändringar i straffnivåerna för andra brott som direktiver förutsätter, föreslås det att subsidiaritetsklausulen i 7 a § om systemstörning ska slopas. Tillämpningssituationerna ska lösas enligt de allmänna principerna om lagkonkurrens. Det

föreslås också att bestämmelserna om grovt störande av post- och teletrafik (SL 38 kap. 6 §) och grov systemstörning (7 b §) ändras så att de innehåller motsvarande kvalifikationsgrunder som grov dataskadegörelse, i enlighet med kraven i direktivet. Maximistraffet för de nämnda grova gärningsformerna föreslås bli höjt till fem års fängelse, enligt vad som förutsätts i direktivet. Det föreslås också att dataintrång som avses i 38 kap. 8 § i strafflagen ändras så att det även täcker fall där någon skaffar sig tillgång till eller tar reda på data i ett informationssystem, i enlighet med kraven i direktivet. Maximistraffet för dataintrång föreslås bli höjt till två års fängelse. Av den anledningen föreslås det att även maximistraffet för grovt dataintrång (8 a §) höjs från två till tre års fängelse. I strafflagens 38 kap. föreslås det även öppna definitioner av informationssystem och data, som grundar sig på förpliktelserna i direktivet (den nya 13 §).

För att uppfylla förpliktelserna i direktivet föreslås i strafflagens 38 kap. en ny 9 b § om identitetsstöld. Enligt 10 §, som gäller åtalsrätten, ska identitetsstöld vara ett målsägandebrott. Identitetsstöld fogas även till förteckningen i 2 § i militära rättegångslagen över de brott som ska handläggas som militära rättegångsärenden.

Det föreslås att den felaktiga paragrafhänvisningen i 38 kap. 11 § i strafflagen korrigeras.

I tvångsmedelslagen ändras 10 kap. 3 § så att ett omnämnande av den föreslagna bestämmelsen om grov dataskadegörelse tas in i lagen. I kapitlets 6 §, som gäller teleövervakning, görs en teknisk ändring som beror på att det inte längre är behövligt att uttryckligen förteckna vissa av de brott som nämns där, på grund av den föreslagna höjningen av maximistraffnivåerna för dem. En motsvarande ändring görs också i bestämmelserna om teleövervakning i 5 kap. 8 § i polislagen.

4 Propositionens konsekvenser

De nya bestämmelserna som tas in i strafflagen utvidgar det straffrättsliga skyddet för information och informationsförmedling i elektronisk form. Tillnärmningen av den lagstiftning som hänför sig till nätbrottslighet mellan Europeiska unionens medlemsstater kan i viss mån främja de finska myndigheternas möjligheter att utreda gränsöverskridande brott som har skadliga följder i Finland. När verksamheten hos den jourpunkt som kan nås dygnet runt effektiviseras på det sätt som avses i propositionen förbättras förutsättningarna för samarbetet vid utredningen av gränsöverskridande brott. Meningen är att jourpunkten fortsättningsvis ska finnas vid centralkriminalpolisen. Till dessa delar är propositionens konsekvenser för polisens organisation och personal endast obetydliga och kräver inte ökade resurser.

Höjningen av maximinivån på de eventuella fängelsestraff som döms ut för brotten kan medföra en ökning av verkställighetskostnaderna. Eftersom maximistraffen dock är teoretiska, kan kostnadsökningen inte antas vara betydande. Identitetsstöld som föreslås i propositionen är emellertid en helt ny kriminalisering. Inte heller när det gäller identitetsstöld kan verkställighetskostnaderna antas öka i någon större utsträckning. Identitetsstöld kommer sannolikt ofta att utgöra en del av ett annat straffbart handlande, så att den påföljd som döms ut är en del av ett gemensamt straff. Påföljden för det självständiga brottet föreslås vara böter. Det är troligt att fallen av identitetsstöld inte kommer att vara särskilt sällsynta. Det kommer således sannolikt att krävas att myndigheterna riktar resurser även till utredningen av dessa fall. Det att identitetsstöld enligt förslaget ska vara ett målsägandebrott kommer att påverka antalet fall som ska utredas.

Generellt sett kan nätbrottsligheten antas ha betydande konsekvenser för hela samhället, även ekonomin. Ett effektivt ingripande i denna brottslighet med hjälp av heltäckande och fungerande kriminaliseringar kan således antas ha positiva samhälleliga och ekonomiska konsekvenser.

De ändringar av strafflagen som föreslås i propositionen har även konsekvenser för vissa av befogenheterna i tvångsmedelslagen (806/2011). Detta beror på att en del tvångsmedel blir tillämpliga när maximistraffen höjs, utan att tvångsmedelslagen ändras.

I propositionen föreslås det att maximistraffet för dataintrång och kränkning av

kommunikationshemlighet höjs till fängelse i två år. Även maximistraffet för dataskadegörelse föreslås vara fängelse i två år. Detta betyder att man för dessa gärningars del även får tillämpa systematisk observation enligt 12 §, datanätsbaserad täckoperation enligt 27 § 3 mom. och bevisprovokation genom köp enligt 34 § i tvångsmedelslagens 10 kap., eftersom dessa tvångsmedel får användas, om en person är skäligen misstänkt för ett brott för vilket det strängaste föreskrivna straffet är fängelse i minst två år. Enligt kapitlets 6 § 2 mom. 3 punkt är teleövervakning redan nu möjlig i fråga om skadegörelse, kränkning av kommunikationshemlighet och dataintrång som begåtts med användning av en teleadress eller teleterminalutrustning, trots att de i dag inte innehåller något maximistraff på fängelse i två år. De maximistraff som föreslås i propositionen, dvs. två års fängelse, utvidgar således inte i sak möjligheten att använda teleövervakning som avses i 6 §. Däremot utvidgas, i och med att maximistraffet höjs, den rätt att utföra teleövervakning med samtycke av den som innehar en teleadress eller teleterminalutrustning som det bestäms om i kapitlets 7 § till att även täcka situationer där dataskadegörelse, kränkning av kommunikationshemlighet eller dataintrång inte har begåtts med användning av en teleadress eller teleterminalutrustning.

När det gäller användning av överskottsinformation som avses i 10 kap. 56 § i tvångsmedelslagen kommer det i fortsättningen att vara möjligt att, under de förutsättningar som anges i tvångsmedelslagen, använda överskottsinformation även för utredning av grovt dataintrång, eftersom maximistraffet för det brottet enligt propositionen ska vara tre års fängelse.

De föreslagna ändringarna i strafflagen har motsvarande konsekvenser som för tvångsmedelslagens del också för befogenheterna enligt polislagen (872/2011) när det gäller systematisk observation i 13 §, datanätsbaserad täckoperation i 28 § 3 mom., bevisprovokation genom köp i 35 § och användning av överskottsinformation i 54 § i lagens 5 kap. Konsekvenserna för teleövervakning enligt 8 § och teleövervakning med samtycke av den som innehar en teleadress eller teleterminalutrustning enligt 9 § motsvarar dem som gäller tvångsmedelslagen ovan.

Genom propositionen genomförs åtgärd 62 i verkställighetsprogrammet för den nationella cybersäkerhetsstrategin. Säkerhetskommittén godkände verkställighetsprogrammet den 11 mars 2014.

5 Beredningen av propositionen

Den 27 september 2013 tillsatte justitieministeriet en arbetsgrupp som fick i uppdrag att bereda ett förslag till nationell lagstiftning om genomförande av direktivet 2013/40/EU om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF. Förslaget skulle ha formen av en regeringsproposition. Arbetsgruppen skulle i sitt arbete även beakta bedömningspromemorian om identitetsstöld (OM 4/41/2013) och remissyttrandena om den, till den del den gäller strafflagstiftningen i fråga som hör till justitieministeriets verksamhetsområde.

I arbetsgruppen fanns företrädare förutom för justitieministeriet även för inrikesministeriet, kommunikationsministeriet, riksåklagarämbetet, dataombudsmannens byrå och Finlands Advokatförbund.

Arbetsgruppen hörde under sitt arbete Tietoturva ry, FISC ry (Finnish Information Security Cluster), Kommunikationsverket och centralkriminalpolisen.

Propositionen grundar sig på arbetsgruppens betänkande (Genomförande av direktivet om it-relaterad brottslighet, Betänkanden och utlåtanden 27/2014) och de utlåtanden som fåtts om betänkandet. Betänkandet sändes på remiss till 39 myndigheter, organisationer och sakkunniga. Ett sammandrag har utarbetats över utlåtandena (Justitieministeriet, betänkanden och utlåtanden, 35/2014). Allmänt taget förhöll sig remissinstanserna positivt till arbetsgruppens förslag. I remissvaren uppmärksammades den föreslagna särskilda kriminaliseringen av identitetsstöld, som fick brett understöd. Vissa av remissinstanserna önskade dock i enlighet med inrikesministeriets företrädare i arbetsgruppen, som lät anteckna avvikande mening, att teleövervakning enligt 10 kap. 6 § i tvångsmedelslagen också skulle vara möjlig i de fall

när identitetsstölden förekommer som ett självständigt brott och inte i samband med t.ex. bedrägeri som begåtts med användning av en teleadress eller teleterminalutrustning, varvid teleövervakning får användas vid utredningen av bedrägeriet.

I propositionen har man till de delar som nämns ovan hållit sig till förslagen i arbetsgruppens betänkande. För det första finns det olika undersökningsmetoder och -befogenheter som kan användas i samband med identitetsstöld, beroende på det aktuella fallet. De undersökningsmetoder som står till buds vid utredning av identitetsstöld behandlas i detaljmotiveringen till propositionen. I motiveringen nämns möjligheterna att utreda ett nätmeddelandes identifieringsuppgifter enligt 17 § i lagen om yttrandefrihet i masskommunikation (460/2003). Vidare nämns i motiveringen möjligheterna att använda teleövervakning med samtycke av den som innehar en teleadress eller teleterminalutrustning enligt 10 kap. 7 § i tvångsmedelslagen i de fall när gärningen har begåtts genom användning av en teleadress eller teleterminalutrustning. Även de metoder att få information som avses i 4 kap. 3 § i polislagen får användas vid utredning av identitetsstöld.

I vissa fall kan de situationer där ett brott har begåtts genom användning av flera teleterminalutrustningar innebära en utmaning vid utredningen (RP 14/2013 rd, s. 19—20). Vid samtyckesbaserad teleövervakning krävs det samtycke till teleövervakningen av flera parter i en informationskedja. I framtiden kan också förändringar i verksamhetsmiljön medföra nya oförutsedda utmaningar, om traditionella brottstyper flyttar över till datanätet. Vid sidan av den straffbestämmelse om identitetsstöld som nu föreslås finns det emellertid i strafflagen redan i dag, och kommer även i framtiden att finnas, också andra förhållandevis ringa brott för vars del polisen inte har tillgång till alla hemliga tvångsmedel, bl.a. på grund av skyddet för de grundläggande rättigheterna, som behandlas nedan.

De tvångsmedel som används ska vara proportionella. Hemliga tvångsmedel ska som utgångspunkt endast användas vid utredning av allvarliga brott. Enligt 10 kap. 6 § i tvångsmedelslagen är det en allmän förutsättning för att använda teleövervakning att det strängaste föreskrivna straffet för brottet är fängelse i minst fyra år. När det gäller brott som har begåtts genom användning av en teleadress eller teleterminalutrustning är den allmänna förutsättningen för teleövervakning ett maximistraff på minst två års fängelse. Identitetsstöld som ett självständigt brott är dock en lindrig gärning, som också lätt uppfyller rekvisitet för något annat grövre brott.

Även bestämmelserna om skydd för privatlivet och förtroliga meddelanden i grundlagens 10 § begränsar användningen av hemliga teletvångsmedel i fråga om bötesbrott och förhållandevis lindriga brott i högre grad än vad som anges i propositionen. Grundlagsutskottet har i sin tidigare praxis ansett att ett meddelandes identifieringsuppgifter inte hör till kärnan för den grundläggande rättigheten i grundlagens 10 §, skyddet för förtroliga meddelanden. Grundlagsutskottet har dock kommit med ett färskt utlåtande (GrUU 18/2014 rd) i anslutning till den föreslagna informationssamhällesbalken och Europeiska unionens domstols dom av den 8 april 2014. Genom den domen konstaterade domstolen att Europaparlamentets och rådets direktiv 2006/24/EG om lagring av identifieringsuppgifter i sin helhet var ogiltigt. Grundlagsutskottet konstaterar i sitt utlåtande (s. 6) att i praktiken kan dock identifieringsuppgifter som ansluter till elektronisk kommunikation samt möjligheten att sammanställa och kombinera dem vara problematiska med hänsyn till skyddet för privatlivet på så sätt att en kategorisk uppdelning av skyddet i ett kärnområde och ett randområde inte alltid är motiverad, utan man måste på ett allmännare plan fästa vikt också vid hur betydelsefulla begränsningarna är.

Vidare analyserar grundlagsutskottet i sitt utlåtande användningen av lagrade uppgifter och konstaterar att de endast får användas för att kunna undersöka brott som avses i 10 kap. 6 § i tvångsmedelslagen. Enligt utskottet uppfyller bestämmelserna domens krav på kriteriet att de lagrade uppgifterna endast används i samband med *allvarliga* brott.

6 Andra omständigheter som inverkat på propositionens innehåll

Riksdagen behandlar just nu regeringens proposition (RP 18/2014 rd) med förslag till lagstiftning om terroristbrott. I propositionen föreslås det ändringar i bl.a. 10 kap. 3 och 6 § i tvångsmedelslagen och 5 kap. 8 § i polislagen. I det förslag som behandlas nu föreslås det också ändringar i de paragraferna i tvångsmedelslagen och polislagen. På grund av det som sägs ovan bör de förslagen samordnas vid behandlingen i riksdagen.

DETALJMOTIVERING

1 Direktivets innehåll och förhållande till lagstiftningen i Finland

Artikel 1. *Syfte.* Enligt artikeln fastställer direktivet 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. Artikeln förutsätter inte ändringar i lagstiftningen.

Artikel 2. *Definitioner.* Artikeln innehåller definitioner. Definitionerna i direktivet motsvarar som utgångspunkt till sitt sakinnehåll de motsvarande definitioner som finns i konventionen och rambeslutet och som behandlas mer ingående i regeringens proposition 153/2006 rd. Enligt led a i artikeln avses med 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. Datorbehandlingsbara uppgifter definieras i led b nedan. Definitionen motsvarar för informationssystemens del till sitt innehåll definitionen av datorsystem i artikel 1 a i konventionen och definitionen av informationssystem i artikel 1 a i rambeslutet. Skrivningen i direktivet och rambeslutet avviker dock från motsvarande definition i konventionen på så sätt att datorbehandlingsbara uppgifter i ett datorsystem inte i konventionen nämns särskilt som en del av begreppet datorsystem. Den preciseringen är av betydelse bl.a. när det gäller artikel 3 i direktivet, som i och med definitionen innehåller en kriminaliseringsförpliktelse som gäller inte bara intrång i informationssystem utan också att skaffa sig tillgång till data i ett informationssystem. Definitionen används också i artiklarna 3–7 för att begränsa området för de brott som straffbeläggs. Definitionen av datorsystem i konventionen har införlivats med den nationella lagstiftningen i Finland genom lagen om sättande i kraft av konventionen. Definitionerna i rambeslutet har inte uttryckligen införlivats med den finska lagstiftningen. För tydlighetens skull föreslås det i propositionen att man i strafflagens 38 kap. tar in den definition av informationssystem som finns i artikel 2 a i direktivet för de brotts del som motsvarar kriminaliseringsförpliktelserna i detta direktiv. Definitionen är öppen och teknikneutral, så att begreppet informationssystem inte heller i fråga om de bestämmelser i strafflagen som det hänvisas till ska begränsas till den definition som finns i direktivet, utan med informationssystem ska även avses det som i direktivet avses med informationssystem och data (datorbehandlingsbara uppgifter) i ett informationssystem. Genom detta uppfylls kraven i direktivet. Eftersom det handlar om en öppen definition som tas in för att säkerställa att förpliktelserna i direktivet kan genomföras, föreslås det i propositionen att den endast ska täcka de kriminaliseringar som är avsedda att täcka förpliktelserna i direktivet.

Enligt artikel 2 b avses med datorbehandlingsbara uppgifter en 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. Definitionen motsvarar ordagrant de motsvarande definitionerna i konventionen och rambeslutet. Begreppet datorbehandlingsbara uppgifter används ovan i definitionen av informationssystem i artikel 2 a och i artiklarna 4, 5 och 6 för att begränsa området av de brott som straffbeläggs. Definitionen av datorbehandlingsbara uppgifter i konventionen har införlivats med den nationella lagstiftningen i Finland genom lagen om sättande i kraft av konventionen. För tydlighetens skull och eftersom definitionen av datorbehandlingsbara uppgifter i enlighet med vad som sägs ovan vid punkt a hör nära samman med definitionen av informationssystem, föreslås det i propositionen att i strafflagens 38 kap. på samma sätt som när det gäller begreppet informationssystem ska tas

in en öppen definition, som motsvarar definitionen i artikel 2 b i direktivet och enligt vilken med data också avses sådana datorbehandlingsbara uppgifter som avses i direktivet i fråga om de brott som motsvarar kriminaliseringsförpliktelserna i direktivet. Genom detta uppfylls kraven i direktivet. Eftersom det handlar om en öppen definition som tas in för att säkerställa att förpliktelserna i direktivet kan genomföras, föreslås det i propositionen att den endast ska täcka de kriminaliseringar som är avsedda att täcka förpliktelserna i direktivet.

Enligt artikel 2 c avses med juridisk person en 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. Punkten motsvarar ordagrant definitionen i rambeslutet. Definitionen är en standardformulering, som allmänt används i de straffrättsliga författningarna inom Europeiska unionen. Av definitionen följer att begreppet juridisk person bestäms enligt nationell lagstiftning. Definitionens enda innehåll är den avgränsning enligt vilken stater och andra motsvarande offentliga organ inte omfattas av definitionen. Definitionen används i artiklarna 10 och 11 för att begränsa tillämpningsområdet för bestämmelserna om juridiska personers straffansvar och i artikel 12.3 b, som är en specialbestämmelse om behörighet. Det finns inte någon motsvarande definition i konventionen. Enligt 9 kap. 1 § 2 mom. i strafflagen tillämpas bestämmelserna i kapitlet om straffansvar för juridiska personer inte på brott som begåtts vid utövande av offentlig makt. Punkten förutsätter inte ändringar i lagstiftningen.

Enligt artikel 2 d avses med orättmätigt ett handlande som avses i direktivet, 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. Definitionen används i artiklarna 3–7 för att från tillämpningsområdet för artiklarna utesluta handlingar som utförs med tillstånd av ägaren eller som en person annars har rätt att utföra. I rambeslutet finns en i sak liknande definition. I den nämns dock inte olaglig avlyssning, eftersom rambeslutet inte innehåller någon artikel om saken. I definitionen i direktivet hänvisas det dessutom till allt handlande som avses i direktivet och som sker utan tillstånd eller inte är tillåtet enligt nationell rätt. Det finns inte någon motsvarande definition i konventionen. Enligt de grundläggande allmänna principerna för straffrätten är ett handlande som sker med tillstånd inte obehörigt. Ett handlande som är tillåtet enligt nationell rätt är givetvis inte heller obehörigt. Led d förutsätter inte ändringar i lagstiftningen.

Artikel 3. *Olagligt intrång i informationssystem.* Enligt artikeln ska medlemsstaterna 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. Artikeln motsvarar till sitt sakinnehåll motsvarande artikel i rambeslutet. I rambeslutet har den förutsättning som gäller intrång i en säkerhetsåtgärd visserligen varit en frivillig möjlighet, medan den i direktivet har tagits in i beskrivningen av själva grundformen av gärningen. I sak har denna skillnad inte någon betydelse från Finlands synpunkt. Även konventionen innehåller en motsvarande artikel, även om det i den inte finns någon uttrycklig undantagsbestämmelse om ringa fall. Dessutom tillåter konventionen en begränsning enligt vilken brottet ska hänföra sig till ett datorsystem som är kopplat till ett annat datorsystem. Dessa skillnader har inte någon praktisk betydelse från Finland synpunkt.

Den motsvarande bestämmelsen i konventionen och rambeslutet behandlades utförligt i den regeringsproposition som gäller genomförandet av rambeslutet och ikraftsättandet av konventionen (RP 153/2006 rd), och en upprepning i samma omfattning är därför inte ändamålsenlig i detta sammanhang. I Finland finns de gällande bestämmelserna om olagligt intrång i informationssystem enligt artikeln i strafflagens 38 kap. 8 §, som gäller dataintrång. Enligt den paragrafen ska den dömas för dataintrång som genom att göra bruk av en användaridentifikation som han eller hon inte har rätt till eller genom att annars bryta säkerhetsarrangemang obehörigen

tränger in i ett datasystem där data behandlas, lagras eller överförs elektroniskt eller med någon annan sådan teknisk metod eller i en särskilt skyddad del av ett sådant system. Enligt samma paragrafs 2 mom. döms för dataintrång också den som utan att tränga in i datasystemet eller en del av detta med tekniska specialanordningar obehörigen tar reda på information som finns i ett sådant datasystem som avses i 1 mom. Bestämmelsen täcker således också intrång i ”data”, vilket är väsentligt med anledning av definitionen av begreppet informationssystem. Enligt paragrafens 3 mom. är försök till dataintrång straffbart. I 4 mom. föreskrivs det att bestämmelsen är subsidiär.

Enligt regeringens proposition 153/2006 rd uppfyllde de då gällande bestämmelserna förpliktelserna i artikeln. I samband med konventionen gav Finland en förklaring som konventionen tillåter och enligt vilken Finland använder sig av rätten att som ett villkor för straffbarheten kräva att brottet har begåtts genom att bryta säkerhetsarrangemang.

På det sätt som konstateras ovan i samband med definitionen av informationssystem i artikel 2 a täcker begreppet informationssystem även datorbehandlingsbara uppgifter (data) i ett informationssystem. Kriminaliseringsförpliktelsen i artikeln gäller således även i intrång i data i ett informationssystem, när gärningen har begåtts orättmätigt och genom intrång i en säkerhetsåtgärd. I den svenska versionen av direktivet är begreppet ”intrång” delvis oklart och vilseledande, eftersom det till dessa delar i sak är fråga om att ta reda på information som finns i ett datasystem på det sätt som avses i strafflagens 38 kap. 8 § 2 mom. (I den engelska versionen av direktivet används formuleringen ”access to”). Enligt det nämnda 2 mom. döms för dataintrång också den som utan att tränga in i datasystemet eller en del av detta med tekniska specialanordningar obehörigen tar reda på information som finns i ett sådant datasystem som avses i 1 mom. I den bestämmelsen finns det inte utöver det kriterium som gäller handlingens obehörighet någon annan begränsning av straffbarheten för denna än att tekniska specialanordningar används. Detta är väsentligt, eftersom 2 mom. uppfyller de skyldigheter i konventionen och artikel 6 i direktivet som gäller olaglig avlyssning i fråga om elektromagnetisk strålning från informationssystem som innehåller data. På grund av det som sägs ovan föreslås det i propositionen att bestämmelsen om dataintrång 38 kap. 8 § 2 mom. i strafflagen kompletteras så att momentet utöver användning av tekniska specialanordningar även täcker att annars med tekniska metoder ta sig förbi säkerhetsarrangemang, utnyttja ett informationssystems sårbarhet eller annars med uppenbart svikliga medel ta reda på information eller data som finns i ett informationssystem. Ett uppenbart svikligt medel kan t.ex. vara att utnyttja ett dataprogram.

Genom den föreslagna ändringen täcker 2 mom. på ett teknikneutralt sätt alla de situationer där någon obehörigen och med uppenbart svikliga medel tar reda på information eller data som finns i ett informationssystem utan att göra intrång i systemet. Det är således meningen att det föreslagna 2 mom. ska täcka bl.a. situationer där någon genom att mata in data får ett informationssystem att fungera felaktigt och lämna ut information (t.ex. så kallade SQL-injektioner) och situationer där någon tar reda på information eller data i systemet med hjälp av ett sabotageprogram.

Det föreslås att man i 1 mom. i paragrafen om dataintrång vid sidan av ordet ”data” tar in ordet ”information”, för att på ett mer heltäckande sätt ange det som man avser att reglera i paragrafen. Det föreslås att begreppet data ska definieras på det sätt som direktivet förutsätter.

Det är skäl att notera att frågan om vilken brottsrubricering som blir tillämplig i respektive fall i allmänhet, beroende på det konkreta fallet, avgörs utifrån om kriminaliseringen har karaktären av specialbestämmelse, om ett särskilt gärningssätt har använts och om den gärning som avses i kriminaliseringen har karaktären av förberedelse i förhållande till en eventuell annan kriminalisering som blir tillämplig samt det intresse som kriminaliseringen avser att skydda. Tillämpningssituationerna bör avgöras från fall till fall enligt de allmänna principerna om lagkonkurrens, och det går inte att ge några absoluta tolkningsanvisningar på grund av att fallen är så olika.

Om t.ex. någon genom att göra intrång i ett informationssystem avlyssnar en upptagning som innehåller ett meddelande som är skyddat mot utomstående, blir i allmänhet endast kränkning av kommunikationshemlighet enligt 38 kap. 3 § i strafflagen tillämplig. I sig uppfyller gärningen rekvisitet för dataintrång, men dataintrånget kan i detta fall anses som en gärning av förberedelsekaraktär i förhållande till kränkningen av kommunikationshemlighet. Kränkningen av kommunikationshemlighet kan dessutom ha status av specialbestämmelse i förhållande till dataintrånget. Trots att tillämpningsområdet för kriminaliseringen av dataintrång är rätt brett, kan således ett särskilt gärningssätt, skyddsintresset, bestämmelsens karaktär av specialbestämmelse eller principen om att gärningar av förberedelsekaraktär får vika leda till att någon annan kriminalisering blir tillämplig. När det gäller paragrafen om dataintrång bör man dessutom notera att den innehåller en subsidiaritetsklausul, som inte föreslås bli upphävd.

Om gärningen även uppfyller rekvisitet för dataskadegörelse, systemstörning eller störande av post- och teletrafik, kan dataintrång få vika utifrån de allmänna principerna om lagkonkurrens och subsidiaritetsklausulen för dataintrång. Dataintrång är ofta också en gärning av förberedelsekaraktär i förhållande till dessa. Begränsningsbestämmelsen i 35 kap. 5 § i strafflagen saknar betydelse i detta fall, eftersom dataintrång inte förutsätter orsakande av skada.

Förhållandet mellan dataintrång och olovligt brukande enligt grundrekvisitet i 28 kap. 7 § i strafflagen kommer inte längre att bestämmas på basis av den subsidiaritetsklausul som gäller dataintrång. Maximistraffet för olovligt brukande är bara ett års fängelse och för den grova gärningsformen två års fängelse, medan maximistraffet för dataintrång är två års fängelse och för den grova gärningsformen tre års fängelse. Förhållandet mellan brotten ska bestämmas enligt de allmänna principerna om lagkonkurrens, och beroende på fallet kan en person dömas både för olovligt brukande och för dataintrång. Detta är motiverat, eftersom olovligt brukande skyddar objekt som egendomsskyddet och ett ekonomiskt intresse, medan skyddsobjektet för kriminaliseringen av dataintrång för sin del framför allt är ett informationssystems konfidentialitet. Å andra sidan bör man notera att dataintrång i vissa fall även kan få vika utifrån andra allmänna principer som gäller lagkonkurrens. Bestämmelsen om olovligt brukande ska t.ex. inte tillämpas, om brukandet är så obetydligt att det i praktiken är en följd av ett systemintrång som omfattas av dataintrång. För tydlighetens skull kan man även konstatera att användning av en internetanslutning via ett oskyddat trådlöst datanät inte anses som olovligt brukande, i enlighet med 28 kap. 7 § 3 mom.

Innehav av hjälpmedel vid nätbrott enligt 34 kap. 9 b § i strafflagen kan för sin del få vika för t.ex. dataintrång, i egenskap av en gärning av förberedelsekaraktär. I de fall när ett i sig straffbart innehav av ett föremål har samband med något annat allvarligare brott, har innehavet i allmänhet inte tillräknats särskilt i rättspraxis. Innehav av hjälpmedel vid nätbrott anses således i allmänhet inte som ett separat brott, om innehavaren vid användningen av hjälpmedlet, antingen som gärningsman eller medverkande, har gjort sig skyldig till något annat brott som bestraffas strängare. Även orsakande av fara för informationsbehandling enligt strafflagens 34 kap. 9 a § är i vissa fall en gärning av förberedelsekaraktär och får således vika för t.ex. dataskadegörelse, systemstörning och störande av post- och teletrafik. I den bestämmelsen finns det dessutom en uttrycklig subsidiaritetsklausul, som inte föreslås bli upphävd. Orsakande av fara för informationsbehandling (9 a §) står i samma förhållande som förut till olovligt brukande enligt 28 kap. 7 §, och maximistraffen för båda brotten är oförändrade. Trots att orsakande av fara för informationsbehandling ibland kan vara en gärning av förberedelsekaraktär, kan ett självständigt straff dömas ut för brottet i vissa fall. Det kan t.ex. handla om en situation där en gärning som avses i 9 a § riktar sig mot flera objekt eller annars är omfattande, och det olovliga brukandet t.ex. sker i bara ett informationssystem. Det är då motiverat att gärningsmannen ska kunna dömas inte bara för olovligt brukande utan också för orsakande av fara för informationsbehandling. Detta är befogat, eftersom kriminaliseringen av olovligt brukan-

de skyddar sådana objekt som t.ex. ett ekonomiskt intresse och databehandlingsfriden för ett enskilt system, medan 9 a § däremot framför allt skyddar säkerheten för databehandling och informationssystem rent allmänt, och gärningen kan äventyra flera informationssystem.

I vissa fall kan orsakande av fara för informationsbehandling, i egenskap av gärning av förberedelsekaraktär, även få vika för dataintrång, enligt de principer som anges ovan.

Förhållandet mellan dataskadegörelse, systemstörning och störande av post- och teletrafik kan å sin sida avgöras från fall till fall med hjälp av bestämmelsens särskilda karaktär. Genom kriminaliseringen av störande av post- och teletrafik (SL 38 kap. 5 §) skyddas framför allt post- och teletrafiken. Den har således status som specialbestämmelse i förhållande till systemstörning (SL 38 kap. 7 a §), om störningen riktar sig mot ett system som är väsentligt i synnerhet med tanke på post- och teletrafiken. Förhållandet mellan dessa två brott ändras således inte, trots att det av tekniska skäl föreslås att subsidiaritetsklausulen för systemstörning upphävs för att de ändringar i straffnivåerna som direktivet förutsätter inte ska leda till oändamålsenliga tillämpningssituationer, t.ex. mellan dataskadegörelse och systemstörning, då maximistraffen för dem kommer att sammanfalla i framtiden. Framöver ska tillämpningssituationerna lösas enligt de allmänna principerna om lagkonkurrens. Systemstörning har status som specialbestämmelse i förhållande till dataskadegörelse (SL, den nya 3 a § i 35 kap.), om man genom att skada data exempelvis hindrar ett informationssystems funktion eller orsakar allvarliga störningar i det. När det gäller möjligheterna att tillämpa dataskadegörelse bör man även beakta den allmänna begränsningsbestämmelsen i 35 kap. 5 §.

Om en persons handlande utöver rekvisitet för kränkning av kommunikationshemlighet även uppfyller rekvisitet för t.ex. olovligt brukande, dataskadegörelse, systemstörning eller störande av post- och teletrafik, är det möjligt att döma ut straff både för dessa brott och för kränkning av kommunikationshemlighet, eftersom skyddsobjektet för dem kan anses vara ett annat än för kränkning av kommunikationshemlighet.

I olovligt brukande kan det ingå en obetydlig mängd skadande av data, varvid rekvisitet för dataskadegörelse ännu inte kan anses vara uppfyllt.

I den föreslagna kriminaliseringen av identitetsstöld kan det handla om att någon obehörigen använder uppgifter som identifierar en juridisk person. I anslutning till detta kan man konstatera att också t.ex. förhållandet mellan vissa immaterialrättsliga brott och identitetsstöld ska avgöras enligt de sedvanliga principerna om lagkonkurrens. I en sådan situation som avses i 49 kap. 2 § i strafflagen kan exempelvis ett varumärke användas i strid med varumärkeslagen, på det sätt som anges i paragrafen. Enligt varumärkeslagen (7/1964) är det väsentliga dock att ett varumärke används obehörigen i näringsverksamhet. Om en identifieringsuppgift, dvs. ett varumärke, obehörigen används i näringsverksamhet, kan t.ex. brott mot industriell rättighet enligt 49 kap. 2 § i strafflagen ha ställning som särskild bestämmelse. Endast den bestämmelsen ska således tillämpas. Om uppgifter som identifierar en juridisk person används någon annanstans än i t.ex. näringsverksamhet, kan den föreslagna bestämmelsen om identitetsstöld för sin del bli tillämplig.

Av de orsaker som anges ovan är det inte möjligt att ange några absoluta konkurrensregler, och varje situation ska lösas med beaktande av omständigheterna i det enskilda fallet, i enlighet med de allmänna principerna om lagkonkurrens.

Artikel 4. *Olaglig systemstörning.* Enligt artikeln ska medlemsstaterna 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. Artikeln motsvarar i sak motsvarande artikel i rambeslutet. Konventionen innehåller en till sakinnehållet motsvarande artikel. Den skiljer sig från artiklarna i direktivet och rambeslutet endast i det avseendet att den inte innehåller någon uttrycklig undantagsbestämmelse om ringa fall. Till övriga delar är kraven i artiklarna

desamma i sak. Konventionen innehåller inte heller formuleringen ”göra det omöjligt att komma åt datorbehandlingsbara uppgifter” till skillnad från direktivet och rambeslutet, men detta saknar betydelse från Finlands synpunkt, eftersom vår nationella lagstiftning täcker även dessa situationer genom formuleringen ”eller på något annat med dessa jämförbart sätt”.

Innan man gjorde de ändringar av lagstiftningen som konventionen och rambeslutet förutsatte ingick de gällande bestämmelserna i Finland som motsvarade olaglig systemstörning som avses i artikeln främst i strafflagens 38 kap. 5 § om störande av post- och teletrafik, såsom framgår av regeringens proposition 153/2006 rd. Tillämpningsområdet för den bestämmelsen begränsade sig dock endast till kommunikation, dvs. överföring av meddelanden från ett ställe till ett annat. För att fullgöra skyldigheterna i konventionen och rambeslutet tog man därför in en ny kriminalisering som gäller systemstörning i 38 kap. 7 a § i strafflagen. Motiveringen till den bestämmelsen och till de motsvarande artiklarna finns i regeringens proposition 153/2006 rd. Enligt den nämnda paragrafen ska den som i syfte att orsaka någon annan olägenhet eller ekonomisk skada genom att mata in, överföra, skada, ändra eller undertrycka data eller på något annat med dessa jämförbart sätt obehörigen hindrar ett informationssystems funktion eller orsakar allvarliga störningar i det, om inte strängare eller lika strängt straff föreskrivs för gärningen någon annanstans i lag, för systemstörning dömas till böter eller fängelse i högst två år. I den nämnda 7 a § nämns inte särskilt gärningssätten radera och försämra, såsom i konventionen, rambeslutet och direktivet, men den öppna förteckningen över gärningssätt som finns i vår lagstiftning, ”eller på något annat med dessa jämförbart sätt”, täcker även dessa.

Enligt paragrafens 2 mom. är försök straffbart. Rekvisitet för grov systemstörning finns 38 kap. 7 b § i strafflagen.

Artikeln förutsätter inte ändringar i lagstiftningen.

Det föreslås dock att subsidiaritetsklausulen för systemstörning ska upphävas, på grund av konkurrenssituationer mellan olika brott. I annat fall kunde det uppstå oändamålsenliga tillämpningssituationer på grund av de ändringar av straffskalorna som direktivet förutsätter. Behovet av att slopa subsidiaritetsklausulen hänför sig bl.a. till att maximistraffet för dataskadegörelse (SL 35 kap. 3 a §) framöver kommer att vara detsamma som för systemstörning.

Artikel 5. *Olaglig datastörning.* Enligt artikeln ska medlemsstaterna 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. Artikeln motsvarar till sitt sakinnehåll den motsvarande artikeln i rambeslutet. Artikeln motsvarar till sitt sakinnehåll också den motsvarande artikeln i konventionen, även om också gärningssättet radera nämns i konventionen. Å andra sidan nämns inte gärningssättet göra det omöjligt att komma åt särskilt i konventionen. Det är dock endast fråga om olika uttryck, och gärningssätten kan anses täcka samma situationer. Artikeln i konventionen skiljer sig i sak från artiklarna i direktivet och rambeslutet endast i det avseendet att konventionen inte innehåller någon uttrycklig undantagsbestämmelse om ringa fall. Skillnaden har ingen praktisk betydelse från Finland synpunkt.

I den regeringsproposition som gällde genomförandet av rambeslutet och ikraftsättandet av konventionen (RP 153/2006 rd) redogörs det närmare för förhållandet mellan de situationer som avses i artikeln och den finska lagstiftningen. De gällande bestämmelserna i Finland om det brott som motsvarar den datastörning som avses här finns i strafflagens 35 kap. 1 §, som gäller skadegörelse. Enligt paragrafens 2 mom. ska för skadegörelse dömas den som för att skada någon orättmätigt förstör, skadar, döljer eller hemlighåller information som har upptagits på ett datamedium eller någon annan upptagning. Trots att förteckningen över gärningssätt i bestämmelsen inte till skrivningen motsvarar förteckningen i artikeln, konstateras det dock i den tidigare nämnda regeringspropositionen att samma gärningar omfattas av regleringen. Med att information skadas avses i bestäm-

melsen att informationen ändras antingen till innehållet eller så att den blir helt obegriplig eller obrukbar. Bestämmelsen täcker således varje slag av ingrepp i information som leder till att information som finns på en lagringsplattform antingen ändras eller utplånas.

Eftersom förteckningen över gärningssätt i paragrafens 2 mom. dock är uttömmande, föreslås det i propositionen att till förteckningen i momentet fogas gärningssätten försämrar, ändrar och gör det möjligt att komma åt, eftersom de gärningssätten inte nödvändigtvis innehållsmässigt helt och hållet täcker de gärningssätt som nu finns i momentet, trots att de delvis gäller samma slags situationer.

Enligt skrivningen i artikeln är föremålet för skadegörelsen datorbehandlingsbara uppgifter (dvs. data) i ett informationssystem. I bestämmelsen om skadegörelse i 35 kap. 1 § 2 mom. i strafflagen används dock den mer begränsade formuleringen information som har upptagits på ett datamedium eller någon annan upptagning. De data som finns i ett informationssystem kan emellertid också ha någon annan form än en permanent upptagning. De kan t.ex. överföras inom systemet. Av denna orsak och för att uppfylla förpliktelserna i direktivet föreslås det i propositionen att till förteckningen över gärningssätt i 2 mom. som föremål för skadegörelsen ska fogas data i ett informationssystem.

Eftersom den dataskadegörelse som avses i 2 mom. i praktiken är ett självständigt brott i förhållande till skadegörelse enligt grundformen i 1 mom., föreslås det i propositionen att 2 mom. om dataskadegörelse ska avskiljas till en självständig paragraf (den nya 3 a §). Detta möjliggör också en tydligare skrivning och reglering i anslutning till straffskalorna och kvalifikationsgrunderna för de grova gärningsformerna. Dessutom föreslås det att den grova gärningsformen av dataskadegörelse ska avskiljas till en självständig paragraf (den nya 3 b §), liksom även den lindriga gärningsformen av dataskadegörelse (den nya 3 c §). På grund av detta föreslås det att 2 och 3 mom. i 35 kap. 1 §, som gäller skadegörelse, ska upphävas.

Finland har inte gjort något sådant förbehåll som punkt 2 i den motsvarande artikeln i konventionen möjliggör, dvs. att man som krav för straffbarheten får uppställa att det handlande som anges i punkt 1 i artikeln i konventionen medför allvarlig skada.

Artikel 6. *Olaglig avlyssning.* Enligt artikeln ska medlemsstaterna 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.

Den motsvarande bestämmelsen i konventionen innehåller inte något uttryckligt undantag som gäller ringa fall. I övrigt är bestämmelserna likadana till sitt sakinnehåll. Enligt konventionen får parterna dessutom när det gäller straffbarheten uppställa krav på att brottet begås med brottsligt uppsåt eller mot ett datorsystem som är kopplat till ett annat datorsystem. Finland har inte uppställt några sådana tilläggskrav för straffbarheten som anges i artikeln.

I den regeringsproposition som gäller ikraftsättandet av konventionen (RP 153/2006 rd) redogörs det på ett heltäckande sätt för hur den bestämmelse som avses här förhåller sig till den finska lagstiftningen och konstateras att de gällande bestämmelserna motsvarar förpliktelserna i artikeln. De gällande bestämmelserna i Finland om det brott som motsvarar den gärning som avses i artikeln ingår i strafflagens 38 kap. 3 §, som gäller kränkning av kommunikationshemlighet, och, i fråga om den grova gärningsformen, i kapitlets 4 § och 8 § 2 mom. Enligt den nämnda 3 § 1 mom. ska den dömas för kränkning av kommunikationshemlighet som obehörigen öppnar ett brev eller ett annat tillslutet meddelande som är adresserat till någon annan eller genom att bryta ett säkerhetsarrangemang skaffar uppgifter om ett meddelande som har upptagits elektroniskt eller med någon annan sådan teknisk metod och som är skyddat mot utomstående, eller skaffar uppgifter om innehållet i samtal, telegram, text-, bild-, eller dataöverföring eller något annat motsvarande telemeddelande som förmedlas genom telenät eller om avsändande eller mottagande av ett sådant meddelande. För att gärningen ska anses som

grov krävs det enligt 4 § att gärningsmannen utnyttjar en särskild förtroendeställning, att brottet begås särskilt planmässigt eller att gärningen riktar sig mot synnerligen förtrolig information. Försök till båda gärningsformerna är straffbart.

Strafflagens 38 kap. 8 § 2 mom., som gäller avlyssning av elektromagnetisk strålning, behandlas i samband med artikel 3.

I den regeringsproposition som gäller ikraftsättandet av konventionen konstateras det att syftet med den motsvarande artikeln i konventionen enligt förklaranderapporten till konventionen är att trygga integritetsskyddet i varje slag av elektronisk kommunikation, oberoende av hur kommunikationen sker tekniskt. Artikelns tillämpningsområde omfattar endast gärningar som begås med tekniska hjälpmedel. Med tekniska hjälpmedel avses förutom apparater och program även användning av lösenord. Med icke allmänna överföringar avses kommunikation som sker i form av målgruppskommunikation. Det avgörande är dock inte arten av det medium som används utan själva meddelandets konfidentiella natur. Därför kan även ett konfidentiellt meddelande som förmedlats i ett medium för masskommunikation höra till artikelns tillämpningsområde. Det kan vara fråga om kommunikation mellan datorer, mellan olika delar i en dator eller mellan en dator och dess användare. Kommunikationen kan också ske genom förmedling av radiovågor. Artikeln omfattar också gärningar som begås genom avlyssning av s.k. elektromagnetiska emissioner. I artikeln förutsätts det att gärningen begås orättmätigt för att den ska utgöra brott. En gärning kan vara berättigad t.ex. på basis av erhållet samtycke av den andra parten eller en myndighets rätt att utreda brott. Artikeln gäller inte användningen av s.k. kakor för att spåra användare på internet.

Enligt regeringens proposition (RP 153/2006 rd) är tillämpningsområdet för bestämmelsen om kränkning av kommunikationshemlighet i strafflagen brett. Bestämmelsen omfattar förutom meddelanden i form av data också andra meddelanden, oberoende av deras form. Ett meddelande i form av data ska dock antingen vara skyddat mot utomstående eller förmedlas genom ett telenät. T.ex. ett e-postmeddelande är således skyddat enligt olika ställen i bestämmelsen beroende på var meddelandet finns. Ett e-postmeddelande åtnjuter skydd för meddelanden som förmedlas i ett telenät när det befinner sig i ett telenät men skydd för meddelanden som är skyddade mot utomstående när det är i en parts besittning, t.ex. när det har lagrats i en dator.

Enligt samma regeringsproposition avses med telenät i bestämmelsen förutom det allmänna telenätet också t.ex. företagsinterna telenät. Med telemeddelande avses varje slag av meddelande av sådan typ som anges i exempelförteckningen i bestämmelsen. Enligt förarbetena till lagen (RP 94/1993 rd) ska frågan om huruvida det föreligger motsvarighet avgöras speciellt med hänsyn till hur viktigt meddelandet är från integritetssynpunkt. Bestämmelsen gäller t.ex. inte masskommunikation i telenät. Förutom innehållet i ett meddelande skyddar bestämmelsen också uppgifter om sändning och mottagning av meddelanden. Det är således straffbart att t.ex. skaffa uppgifter om till vilket nummer någon har ringt från en viss telefon.

Enligt regeringens proposition (RP 153/2006 rd) skyddar bestämmelsen också meddelanden som utan överföring registreras i en dator för att bli lästa av en eller flera bestämda personer. En förutsättning för straffbarhet är dock att meddelandet genom någon teknisk metod har skyddats mot utomstående och att den som skaffar uppgifter om meddelandet bryter skyddet. I regeringens proposition hänvisas det till förarbetena till lagen (RP 94/1993 rd) och konstateras att detta kan ske på samma sätt som i fråga om datainträng.

Vidare konstateras det i samma proposition att gärningen ska begås obehörigen. En gärning kan vara berättigad t.ex. på basis av erhållet samtycke av den andra parten eller en myndighets rätt att utreda brott. I propositionen hänvisas det också till strafflagens 38 kap. 8 § 2 mom., som det konstateras att gäller avlyssning av elektromagnetiska emissioner. I propositionen konstateras det att slutsatsen är att de gällande bestämmelserna till dessa delar motsvarar skyldigheterna enligt artikeln.

Trots det som konstateras i den ovan nämnda regeringspropositionen kom arbets-

gruppen till den slutsatsen att de ovan nämnda bestämmelserna i strafflagen inte helt och hållet täcker syftena med och tillämpningsområdet för konventionen, eller nu direktivet. För det första förutsätts det i artikeln att den olagliga avlyssningen sker med tekniska hjälpmedel. Det är naturligtvis tillåtet att straffbelägga gärningen utan något sådant krav. I strafflagens 38 kap. 3 § 1 mom. 1 punkt förutsätts det dock att ett säkerhetsarrangemang bryts. Detta kriterium är mer begränsande än ”med tekniska hjälpmedel”. Med tekniska hjälpmedel hänvisas i den förklarande rapporten till konventionen till apparater, program och t.ex. användning av lösenord. Såsom det konstateras ovan sades det i förarbetena i samband med att konventionen sattes i kraft (RP 94/1993 rd) att brytandet av säkerhetsarrangemang kan ske på samma sätt som i fråga om dataintrång (8 §). Dessutom bör man notera att 8 § 2 mom., som gäller elektromagnetisk strålning, redan i sig uppfyller förpliktelsen i artikeln när det gäller utnyttjande av elektromagnetisk strålning. I fråga om 3 §, som gäller kränkning av kommunikationshemlighet, är det i viss mån oklart om den täcker alla de situationer enligt artikeln när ”tekniska hjälpmedel” används. I praktiken har det varit oklart huruvida den gällande 38 kap. 3 § täcker de avlyssningssituationer där data ännu inte förmedlas i ett telenät och inte heller har upptagits, och avlyssningen sker t.ex. med hjälp av ett sabotageprogram, som den som använder programmet antingen omedvetet eller genom att ha vilseletts själv har installerat i sin dator eller som annars har installerats med svikliga medel. Det har då inte heller nödvändigtvis skett något intrång i datasystemet i den bemärkelse som avses i bestämmelsen om dataintrång.

De omständigheter som nämns i det föregående stycket när det gäller strafflagens 38 kap. 3 § 1 mom. 1 punkt och information som har upptagits har dock inte särskilt stor betydelse med tanke på förpliktelserna i direktivet, eftersom dessa gäller avlyssning av överföringar data till, från eller inom ett informationssystem. Det är således som utgångspunkt inte fråga om information som har upptagits utan om avlyssning av icke-offentlig överföring av data. Denna förutsättning framgår tydligare av direktivets engelska text. Där används formuleringen ”intercepting non-public transmission of computer data”.

Förpliktelserna i artikeln gäller kommunikation såväl till och från som inom ett informationssystem. De oklarheter som nämns ovan gäller inte situationer där det är fråga om överföring av data till eller från ett informationssystem. Informationen förmedlas då i ett telenät, varvid bestämmelsen om kränkning av kommunikationshemlighet i 38 kap. 3 § 1 mom. 2 punkten i strafflagen blir tillämplig. Den punkten innehåller inte några tilläggskriterier utöver det att någon har skaffat uppgifter om innehållet i dataöverföring eller om avsändande eller mottagande av sådan. Oklarheterna gäller överföring av data inom ett informationssystem. Kapitlets 3 § 1 mom. 1 punkt gäller inte uttryckligen överföring av data inom ett informationssystem, t.ex. mellan användaren (tangentbordet) och informationssystemet eller mellan ett informationssystems olika delar. Den punkten gäller uttryckligen endast meddelanden som har upptagits, som förpliktelserna i artikeln inte kan anses gälla.

För att undanröja de oklarheter som nämns ovan föreslås det i propositionen att bestämmelsen om kränkning av kommunikationshemlighet i 3 § 1 mom. 2 punkten ska utvidgas till att gälla förutom dataöverföring som förmedlas genom ett telenät också dataöverföring inom ett informationssystem, på det sätt som skrivningen i konventionen och direktiver förutsätter. Enligt den ändring som görs i strafflagens 38 kap. 3 § 1 mom. 2 punkt ska också den dömas för kränkning av kommunikationshemlighet som obehörigen skaffar uppgifter om innehållet i samtal, telegram, text-, bild- eller dataöverföring eller något annat motsvarande telemeddelande som förmedlas genom telenät eller informationssystem eller om avsändande eller mottagande av ett sådant meddelande. Det är motiverat att skydda dataöverföring och annan icke-offentlig kommunikation på samma sätt, oberoende av var i kommunikationskedjan kränkningen av kommunikationshemlighet sker i respektive fall. Ändringen är också befogad av den anledningen att t.ex. många av de brott som riktar sig mot användningen av

nätbanker i dag begås genom att rikta åtgärder mot kommunikation i nätbankskundens personliga dator, dvs. inom ett informationssystem. En orsak till denna utvecklingstrend kan vara att själva telenäten och bankernas informationssystem i dag är så väl skyddade att det är kunden som är det mest sårbara objektet.

Icke-offentlig dataöverföring i den bemärkelse som avses i 1 mom. 2 punkten kan även inbegripa t.ex. lägesuppgifter som sänds från en teleterminalutrustning som en person administrerar, om data förmedlas på det sätt som avses i bestämmelsen.

Efter dessa ändringar motsvarar den finska lagstiftningen kraven i artikeln.

Artikel 7. *Verktyg som används för att begå brott.* Enligt artikeln ska medlemsstaterna 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 de verktyg som nämns i artikeln, 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. De verktygen är enligt artikelns led a) ett datorprogram som utformats eller anpassats i första hand för att begå något av de brott som avses i artiklarna 3–6 och 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 6 punkt 1 a i konventionen innehåller bestämmelser om samma frågor. Skillnaden är i sak att bestämmelsen i direktivet inte täcker andra verktyg än datorprogram och uppgifter. I direktivet finns det således inte något omnämnande av ”apparat” (device) som skulle hänvisa till s.k. ”hardware”, till skillnad från konventionens artikel 6 punkt 1 a i. Konventionen tillåter dock att man gör ett förbehåll till artikelns 1 punkt, dock under förutsättning att förbehållet inte gäller försäljning, spridning eller annat tillgängliggörande av föremål som avses i artikelns punkt 1 a ii. Punkt 1 a ii innehåller samma ”verktyg” som punkt b i artikeln i direktivet, dvs. ett datorlösenord, en åtkomstkod eller liknande uppgifter. Finland har inte gjort något sådant förbehåll som avses här. Konventionen innehåller dessutom bestämmelser om kriminalisering av innehav och, för tydlighetens skull, uteslutande av straffansvar i ett sådant fall när meningen är att behörig ordning testa eller skydda ett datorsystem.

Den bestämmelse som avses här behandlas på ett heltäckande sätt i den regeringsproposition som gäller ikraftsättandet av konventionen (RP 153/2006 rd). I samband med att konventionen sattes i kraft ändrades strafflagens 34 kap. 9 a § så att den motsvarar kraven i konventionen. I den gällande finska lagstiftningen motsvaras de situationer som avses i direktivet av orsakande av fara för informationsbehandling i strafflagens 34 kap. 9 a §. Enligt bestämmelsen döms den som för att orsaka olägenhet eller skada för informationsbehandling eller för ett informations- eller kommunikationssystems funktion eller säkerhet 1) för in i landet, tillverkar, säljer eller annars sprider eller ställer till förfogande a) sådana apparater, datorprogram eller programinstruktioner som har skapats eller anpassats för att äventyra eller skada informationsbehandling eller ett informations- eller kommunikationssystems funktion eller för att bryta eller avkoda det tekniska skyddet vid elektronisk kommunikation eller skyddet för ett informationssystem, eller b) andra personers lösenord eller åtkomstkoder eller andra motsvarande uppgifter om informationssystem, eller 2) sprider eller ställer till förfogande anvisningar för tillverkning av sådana datorprogram eller programinstruktioner som avses i 1 punkten. Bland gärningssätten i 9 a § ovan saknas det i artikeln i direktivet nämnda ”anskaffa i syfte att använda”. Bestämmelser om innehav av hjälpmedel vid nätbrott finns i strafflagens 34 kap. 9 b §. I den regeringsproposition som gäller ikraftsättandet av konventionen (RP 153/2006 rd) konstateras det att 9 b § täcker förpliktelserna enligt artikeln till den del de gäller anskaffning av hjälpmedel vid nätbrott utan att hjälpmedlet samtidigt sprids eller görs tillgängligt. I praktiken täcker straffbarheten för innehav även anskaffning, eftersom ett hjälpmedel till följd av anskaffningen alltid kommer i den persons besittning som har gjort anskaffningen.

Direktivet förutsätter emellertid också i fråga om ”anskaffning i syfte att använda” ett

maximistraff på två år. Maximistraffet för innehav av hjälpmedel vid nätbrott, dvs. den gärning som avses i strafflagens 34 kap. 9 b § är sex månaders fängelse. Enbart innehav av hjälpmedel vid nätbrott kan dock inte anses vara ett lika klandervärt brott som orsakande av fara för informationsbehandling, som avses i 9 a §. Det är således inte motiverat att höja maximistraffet i 9 b § till två års fängelse. Anskaffning i syfte att använda kan också anses vara mer klandervärt än enbart innehav och innebär inte samma sak, trots att hjälpmedlet som en följd av anskaffningen kommer i den persons besittning som har anskaffat det. Anskaffning i syfte att orsaka olägenhet eller skada förutsätter att en person vidtar aktiva åtgärder för att få hjälpmedlet i sin besittning till skillnad från när det gäller enbart ett innehav, då rekvisitet kan uppfyllas redan på basis av att en person helt enkelt innehar ett hjälpmedel, förutsatt att de övriga kriterierna i bestämmelsen, t.ex. att syftet varit att orsaka olägenhet eller skada, uppfylls. Anskaffning i syfte att använda kan för sin del förutsätta bl.a. aktivt letande, anskaffning av information och som en följd av detta t.ex. beställning av ett hjälpmedel via internet. Det väsentliga är således aktivt handlande för att skaffa ett hjälpmedel i syfte att använda det för att orsaka olägenhet eller skada.

I dag motsvarar 9 a och 9 b § i strafflagens 34 kap. inte till alla delar de krav i direktivet som gäller ”anskaffa i syfte att använda”. På grund av det som sägs ovan föreslås det i propositionen att även gärningssättet ”anskaffar i syfte att använda” fogas till kapitlets 9 a § 1 mom. 1 punkt. Rekvisitet för anskaffa i syfte att använda uppfylls först när personen i fråga har fått verktyget i sin besittning. Efter den föreslagna ändringen motsvarar lagstiftningen förpliktelserna i direktivet. Kriminaliseringen av anskaffning i syfte att använda ska, på det sätt som förutsätts i direktivet, också gälla anskaffning av andra personers datorlösenord, åtkomstkoder eller andra motsvarande uppgifter om informationssystem, i det fallet att de övriga kriterierna för straffbarheten, såsom ett syfte att orsaka olägenhet eller skada, är uppfyllda.

De förpliktelser som gäller s.k. botnät hänför sig till straffskärpningsgrunderna för de gärningar som avses i artiklarna 4 och 5, på det sätt som sägs nedan i samband med artikel 9. Det är dock skäl att konstatera att ett botnät också kan vara en sådan apparat eller ett sådant datorprogram som avses i 34 kap. 9 a och 9 b §.

Artikel 8. *Anstiftan, medhjälp och försök.* Enligt punkt 1 i artikeln ska medlemsstaterna se till att anstiftan av och medhjälp till de brott som avses i artiklarna 3—7 straffbeläggs. En motsvarande bestämmelse som gäller anstiftan och medhjälp finns också i konventionen och rambeslutet. I Finland finns bestämmelserna om straffbarhet för anstiftan och medhjälp i strafflagens 5 kap. 5 och 6 §. En anstiftare jämställs med en gärningsman i fråga om straffansvaret. En medhjälpare döms utifrån en lindrigare straffskala.

Till dessa delar motsvarar de gällande bestämmelserna förpliktelserna i artikeln. Artikeln förutsätter inte ändringar i lagstiftningen.

Enligt punkt 2 i artikeln ska medlemsstaterna se till att försök att begå de brott som avses i artiklarna 4 och 5 straffbeläggs. De artiklarna gäller olaglig systemstörning och olaglig datastörning. Även rambeslutet och konventionen innehåller artiklar om straffbarhet för försök. Förpliktelserna i rambeslutet är visserligen mer omfattande när det gäller straffbarheten för försök, eftersom rambeslutet förutsätter att försök straffbeläggs även i fråga om artikeln om olagligt intrång i informationssystem. Också förpliktelserna i konventionen är mer omfattande än förpliktelserna i direktivet, eftersom de förpliktelser i konventionen som gäller kriminalisering av försök även täcker artikeln om olaglig avlyssning. Å andra sidan tillåter konventionen att man gör ett förbehåll till de förpliktelser som gäller straffbarhet för försök.

De bestämmelser i strafflagen som motsvarar artikel 4 i direktivet är störande av post- och teletrafik i 5 §, grovt störande av post- och teletrafik i 6 §, lindrigt störande av post- och teletrafik i 7 §, systemstörning i 7 a § och grov systemstörning i 7 b § i strafflagens 38 kap. Försök är straffbart i fråga om samtliga ovan nämnda brott.

Artikel 5 i direktivet motsvaras i strafflagen av skadegörelse enligt 35 kap. 1 § 2 mom. Försök till det brottet är straffbart. Även försök till grov skadegörelse enligt

35 kap. 2 § är straffbart. På det sätt som anges ovan föreslås det i propositionen att bestämmelserna om dataskadegörelse ska avskiljas till självständiga paragrafer. De föreslagna nya bestämmelserna om dataskadegörelse (3 a §) och grov dataskadegörelse (3 b §) motsvarar till dessa delar de bestämmelser som nämns ovan, även när det gäller straffbarheten för försök. Försök till lindrig skadegörelse som avses i strafflagens 35 kap. 3 § är inte straffbart. Inte heller försök till lindrig dataskadegörelse enligt den föreslagna nya 3 c § ska vara straffbart. Förpliktelserna enligt artikel 5 i direktivet gäller dock inte ringa fall, och det är därför inte behövligt att utsträcka straffbarheten för försök till att gälla lindrig dataskadegörelse. Man stannade för en motsvarande lösning i rambeslutet, vars artikel om olaglig datastörning inte innehåller några förpliktelser om ringa fall. I samband med att konventionen sattes i kraft gjorde Finland också ett förbehåll enligt vilket man inte tillämpar den förpliktelse som hänför sig till kriminaliseringen av försök på lindrig skadegörelse.

Artikeln förutsätter inte ändringar i lagstiftningen till andra delar än när det gäller kriminalisering av försök i den föreslagna nya bestämmelsen om dataskadegörelse (38 kap. 3 a §) och grov dataskadegörelse (38 kap. 3 b §).

Artikel 9. *Påföljder.* Enligt artikel 9.1 ska medlemsstaterna 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. Artikelns 1 punkt är en standardbestämmelse om påföljder, och den förutsätter inte att man föreskriver om vissa särskilda straffnivåer. I praktiken gäller den dock enbart artikel 8, dvs. straffbarheten för anstiftan, medhjälp och försök, eftersom det i fråga om artiklarna 3–7 förutsätts vissa lägsta nivåer för maximistraffen, på det sätt som anges nedan.

Grundformerna av gärningarna

Enligt punkt 2 i artikeln ska medlemsstaterna 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. Den begränsning som gäller ringa fall är här främst ett informativt tillägg, eftersom samma begränsning nämns självständigt i alla de artiklar som avses här (artiklarna 3—7). Den förutsättning som gäller miniminivån riktar sig således i sin helhet till artiklarna 3—7.

På det sätt som konstateras i samband med artikel 3 ovan motsvaras den gärning som avses i artikel 3 i Finland av dataintrång enligt strafflagens 38 kap. 8 §. Maximistraffet för dataintrång är fängelse i högst ett år. Straffnivån för dataintrång måste alltså höjas till två års fängelse. Att straffnivån för dataintrång enligt grundformen höjs till två års fängelse har också betydelse när det gäller grovt dataintrång i strafflagens 38 kap. 8 a §. I dag är maximistraffet för grovt dataintrång två års fängelse. För att maximistraffen för grundformen och den grova gärningsformen av gärningen och inte ska vara identiska, föreslås det i propositionen att straffnivån för grovt dataintrång höjs till tre års fängelse. Förutom det som sägs ovan är det också för konsekvensens skull motiverat att höja maximistraffet för den grova gärningsformen av dataintrång, för att man ska förhålla sig lika allvarligt till nätbrotten som till de övriga brottstyperna som avses i direktivet. Artikel 9.2 i direktivet förutsätter således ändringar i lagstiftningen när det gäller bestämmelserna om dataintrång.

På det sätt som konstateras i samband med artikel 4 ovan ingår de bestämmelser som motsvarar den gärning som avses i artikel 4 i strafflagens 38 kap. 5 § om störande av post- och teletrafik och 38 kap. 7 a § om systemstörning. Maximistraffet för de gärningarna är redan i dag två års fängelse, varvid kravet på nivån på maximistraffet i artikel 9.2 uppfylls. Artikel 9.2 i direktivet förutsätter således inte ändringar i lagstiftningen när det gäller störande av post- och teletrafik och systemstörning.

På det sätt som konstateras i samband med artikel 5 ovan ingår de bestämmelser som motsvarar den gärning som avses i artikel 5 i strafflagens 35 kap. 1 § 2 mom. (dataskadegörelse). Maximistraffet för skadegörelsen är ett års fängelse. För att uppfylla kraven i direktivet bör maximistraffet för dataskadegö-

relse som utgångspunkt höjas till två års fängelse. Kriminaliseringen av den vanliga gärningsformen av skadegörelse i 1 mom. täcker emellertid ett så brett spektrum av olika fall att det inte är ändamålsenligt att höja straffnivån mer än vad direktivet förutsätter. Dataskadegörelse innebär i många fall en högre grad av uppsåt, och brottet kräver ofta en viss planmässighet. Därför är det motiverat att ha tillgång till ett högre maximistraff för dataskadegörelse än för skadegörelse enligt grundformen. Maximistraffet på två år bör således endast gälla dataskadegörelse som avses i 2 mom. Det föreslås att dataskadegörelse, på det sätt som anges ovan, ska avskiljas till en självständig paragraf, bl.a. för att bestämmelsen ska vara tekniskt tydlig. När dataskadegörelse avskiljs till en separat paragraf behöver man inte höja straffskalan för skadegörelse enligt grundformen i strafflagens 35 kap. 1 § till två års fängelse, utan det räcker att maximistraffet för den föreslagna nya kriminaliseringen av dataskadegörelse i 3 a § är två års fängelse.

I motsvarighet till skadegörelse föreslås det en ny lindrig gärningsform av den nya kriminaliseringen av dataskadegörelse, dvs. lindrig dataskadegörelse (3 c §), för vars del maximistraffet föreslås vara böter, på samma sätt som när det gäller lindrig skadegörelse. Det är motiverat att också stifta en lindrig gärningsform av det föreslagna nya brottet dataskadegörelse, för att man inte ska behöva tillämpa dataskadegörelse enligt grundformen, som bestraffas relativt strängt, på de allra lindrigaste fallen. Förpliktelserna i direktivet gäller inte ringa fall, och man får således besluta nationellt om maximistraffet för lindrig dataskadegörelse.

Artikel 9.2 i direktivet förutsätter således att lagstiftningen ändras när det gäller skadegörelse.

På det sätt som konstateras i samband med artikel 6 ovan, finns bestämmelser som motsvarar den gärning som avses i artikel 6 i strafflagens 38 kap. 3 § om kränkning av kommunikationshemlighet och 8 § 2 mom. om dataintrång. Maximistraffet för kränkning av kommunikationshemlighet är i dag ett års fängelse. Såsom det konstateras ovan är också maximistraffet för dataintrång i dag ett års fängelse. För att uppfylla kraven i artikel 9.2 i direktivet måste förutom maximistraffet för dataintrång även maximistraffet för kränkning av kommunikationshemlighet höjas till två års fängelse.

På det sätt som konstateras i samband med artikel 7 ovan ingår bestämmelser som motsvarar den gärning som avses i artikel 7 i strafflagens 34 kap. 9 a § om orsakande av fara för informationsbehandling och, när det gäller ”anskaffning i syfte att använda", i strafflagens 34 kap. 9 b § om innehav av hjälpmedel vid nätbrott. Maximistraffet för kriminaliseringen av orsakande av fara för informationsbehandling är redan i dag två års fängelse, och det finns alltså inte något behov av att höja nivån på maximistraffet för dess del. Maximistraffet för innehav av hjälpmedel vid nätbrott är sex månaders fängelse. I propositionen föreslås det dock att ”anskaffning i syfte att använda" ska tas in under kriminaliseringen av orsakande av fara för informationsbehandling. Kraven när det gäller den lägsta nivån på maximistraffen i artikel 9.2 i direktivet förutsätter således inte ändringar i lagstiftningen i och med den ändringen.

Maximistraffet på tre år

Enligt punkt 3 i artikeln ska medlemsstaterna 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.

Punkt 3 i artikeln gäller bl.a. situationer som är tänkta att täcka fall som gäller s.k. botnät. Syftet med direktivet har varit att täcka både skapande och användning av botnät, även om t.ex. en blockeringsattack där botnät utnyttjas riktar sig mot bara ett objekt. Såsom anges ovan är det i artiklarna 4 och 5, som avses i den nämnda 3 punkten, i den nationella lagstiftningen fråga om störande av post- och teletrafik enligt 5 § och systemstörning enligt 7 a § i strafflagens 38 kap. och om dataskadegörelse enligt 1 § 2 mom. eller det i denna proposition föreslagna nya

brottet dataskadegörelse (3 a §) i strafflagens 35 kap. Med verktyg enligt artikel 7 i direktivet avses för sin del de verktyg som nämns i strafflagens 34 kap. 9 a § 1 punkt.

Till vissa delar kunde det i de situationer som avses i 3 punkten vara fråga om ett sådant särskilt planmässigt brott som avses i 1 mom. 2 punkten i strafflagens 38 kap. 7 b §, som gäller grov systemstörning. Varken i bestämmelsen om grovt störande av post- och teletrafik i kapitlets 6 § eller i bestämmelsen om grov skadegörelse i 35 kap. 2 §, och inte heller i den föreslagna nya bestämmelsen om grov dataskadegörelse i 35 kap. 3 b §, finns det dock någon kvalifikationsgrund som gäller särskild planmässighet. På grund av detta och eftersom kvalifikationsgrunderna för grova gärningsformer som utgångspunkt ska tolkas snävt, föreslås det i propositionen att man, för att uppfylla kraven i direktivet, i grovt störande av post- och teletrafik i strafflagens 38 kap. 6 §, grov systemstörning i strafflagens 38 kap. 7 b § och grov dataskadegörelse i den nya 3 b § i strafflagens 35 kap. tar in en ny gärningsform som motsvarar artikel 9.3 i direktivet och som kvalificerar gärningarna i fråga som grova. En gärning kan kvalificera som grov, om brottet begås som ett led i verksamhet där ett betydande antal informationssystem har påverkats genom användning av sådana apparater, datorprogram eller programinstruktioner som avses i 34 kap. 9 a § 1 punkten underpunkt a eller sådana lösenord, åtkomstkoder eller andra motsvarande uppgifter som avses i 9 a § 1 punkten underpunkt b.

Kravet på en lägsta nivå på tre års fängelse för det maximistraff som förutsätts i artikel 9.3 i direktivet förutsätter inte någon höjning av straffnivåerna i den nationella lagstiftningen, eftersom maximistraffet för de ovan nämnda nu gällande grova gärningsformerna av brotten redan i dag är fyra års fängelse i finsk lag. Grov dataskadegörelse (38 kap. 3 b §) är en ny kriminalisering, men också maximistraffet för grov skadegörelse är fyra års fängelse redan i dag. Maximistraffen för de grova gärningsformerna i fråga måste dock höjas de orsaker som anges nedan i denna proposition.

Maximistraffet på fem år

Enligt punkt 4 i artikeln ska medlemsstaterna 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.

I de i punkten avsedda artiklarna 4 och 5 är det i den nationella lagstiftningen såsom anges ovan fråga om störande av post- och teletrafik enligt 5 § och systemstörning enligt 7 a § i strafflagens 38 kap. och om dataskadegörelse enligt 1 § 2 mom. eller, framöver, dataskadegörelse enligt 3 a § i strafflagens 35 kap. De gärningssätt som avses i punkten täcks i dag endast delvis av den nationella lagstiftningen i de grova gärningsformerna av de ovan nämnda brotten, dvs. grovt störande av post- och teletrafik enligt 38 kap. 6 §, grov systemstörning enligt 38 kap. 7 b § och grov skadegörelse enligt 35 kap. 2 § i strafflagen. För att uppfylla kraven i direktivet föreslås i propositionen att nya kvalifikationsgrunder som motsvarar punkt 4 ska tas in i de grova gärningsformerna av de brotten. När det gäller dataskadegörelse avskiljs grov dataskadegörelse från grov skadegörelse och blir en självständig paragraf (3 b §), på det sätt som anges ovan i propositionen. Dessutom är maximistraffet för de grova gärningsformerna som nämns ovan i dag fyra års fängelse enligt den nationella lagstiftningen. För att uppfylla kraven i direktivet föreslås ett maximistraff på fem års fängelse för dessa grova gärningsformer. Eftersom grov dataskadegörelse avskiljs till en egen paragraf, behöver maximistraffet för grov skadegörelse enligt strafflagens 35 kap. 2 § inte höjas.

Kriminell sammanslutning

Strafflagens 35 kap. 2 § 1 mom. 2 punkt innehåller i dag en kvalifikationsgrund om kriminella sammanslutningar som uttryckligen är begränsad till dataskadegörelse och som i sak uppfyller förpliktelserna i direkti-

vet. Kvalifikationsgrunden togs in i bestämmelsen i samband med de nationella åtgärderna för att genomföra rambeslutet. När det gäller grov dataskadegörelse förutsätter punkt 4 a således inte att lagstiftningen ändras annat än för maximistraffets del, som bör höjas till fem års fängelse såsom direktivet kräver. I propositionen föreslås det dock att det på det sätt som anges ovan stiftas en ny 3 b § om grov dataskadegörelse, som innehåller en kvalifikationsgrund som motsvarar 2 punkten. Maximistraffet i den föreslagna nya 3 b § är fem års fängelse. Den gällande bestämmelsen i 35 kap. 2 § 1 mom. 2 punkten i strafflagen upphävs.

Grovt störande av post- och teletrafik i 6 § och grov systemstörning 7 b § i strafflagens 38 kap. innehåller inte någon motsvarande kvalifikationsgrund som hänför sig till kriminella sammanslutningar. För att uppfylla kraven i direktivet föreslås att till de bestämmelserna fogas en motsvarande kvalifikationsgrund som den som i dag ingår i grov dataskadegörelse. En gärning kan således kvalificera som grov, om brottet begås som ett led i en i 17 kap. 1 a § 4 mom. avsedd kriminell sammanslutnings verksamhet. Dessutom föreslås det att maximistraffet för de nämnda brotten höjs till fem års fängelse.

Allvarlig skada

I skäl 5 i ingressen till direktivet konstateras det att medlemsstaterna får fastställa vad som utgör allvarlig skada enligt deras nationella rätt och praxis.

De situationer som avses i bestämmelsen om grov skadegörelse i strafflagens 35 kap. 2 § 1 mom. 1 punkt täcker i hög grad den allvarliga skada som avses i direktivet. Skadegörelsen kan kvalificera som grov, om skadegörelsen vållar a) synnerligen stor ekonomisk skada, b) synnerligen kännbar skada för den drabbade, med beaktande av dennes förhållanden eller c) avsevärd skada på egendom som är synnerligen värdefull i historiskt eller kulturellt hänseende. I propositionen föreslås det att grov dataskadegörelse ska avskiljas till en självständig paragraf (3 b §), i vilken man tar in en kvalifikationsgrund som motsvarar den som finns i 38 kap. 7 b § nedan. Maximistraffet för den föreslagna nya grova skadegörelsen är fem års fängelse.

I 1 mom. 1 punkten i strafflagens 38 kap. 7 b § om grov systemstörning finns det redan nu en kvalifikationsgrund som täcker de situationer där synnerligen kännbar olägenhet eller ekonomisk skada vållas. Till dessa delar förutsätter direktivet således inte att kriminaliseringen av grov systemstörning ändras, med undantag av att maximistraffet höjs till fem års fängelse.

Grovt störande av post- och teletrafik, som avses i 38 kap. 6 § i strafflagen, innehåller i dag inte någon kvalifikationsgrund som gäller allvarlig skada. I propositionen föreslås det att till den bestämmelsen, på samma sätt som när det gäller grov dataskadegörelse ovan (35 kap. 3 b §), fogas en kvalifikationsgrund som motsvarar 1 mom. 1 punkten i 7 b § om grov systemstörning och enligt vilken en gärning kan kvalificera som grov, om synnerligen kännbar olägenhet eller ekonomisk skada vållas. Kriteriet ”synnerligen kännbar” gäller även ekonomisk skada (RP 153/2006 rd, s. 69). Dessutom föreslås det att maximistraffet höjs till fem års fängelse.

Kritisk infrastruktur

Kritisk infrastruktur definieras inte i direktivet, och medlemsstaterna får således själva bestämma om saken. Skäl 4 i ingressen ger dock en fingervisning om prövningen till dessa delar. I skälet sägs det att ”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”.

När de brott som avses i artiklarna 4 och 5, dvs. i praktiken störande av post- och teletrafik, systemstörning och dataskadegörelse, riktar sig mot ett informationssystem som utgör kritisk infrastruktur kan i många fall också rekvisitet för sabotage i 34 kap. 1 § i strafflagen uppfyllas. Enligt den paragrafens

2 mom. döms för sabotage också den som genom att skada eller förstöra egendom eller genom att obehörigen ingripa i ett produktions-, distributions- eller datasystems funktion, förorsakar allvarlig fara för energiförsörjningen, den allmänna hälsovården, försvaret, rättsvården eller någon med dessa jämförbar viktig samhällsfunktion. Kriminaliseringen av sabotage räcker dock inte för att uppfylla kraven i direktivet till dessa delar. För det första krävs det i rekvisitet för sabotage att allvarlig fara förorsakas. Bestämmelserna i direktivet verkar inte tillåta denna begränsning, utan den nationella kriminaliseringen ska gälla brott enligt artiklarna 4 och 5 när de över huvud taget har riktat sig mot ett informationssystem som utgör kritisk infrastruktur. För det andra uppfyller maximistraffet på fyra år för sabotage inte kravet på ett maximistraff på minst fem år.

Eftersom det föreslås att maximistraffet för grovt störande av post- och teletrafik, grov systemstörning och grov dataskadegörelse höjs till fem års fängelse för att uppfylla förpliktelserna i direktivet, och för att tydligt täcka det handlande som ska kriminaliseras enligt kraven i direktivet på det sätt som avses i detta, föreslås det i propositionen att man i de grova gärningsformerna för de brott som nämns ovan tar in en ny kvalifikationsgrund, som delvis motsvarar rekvisitet för sabotage till den del det handlar om kritisk infrastruktur. När det gäller grov systemstörning föreslås det således en ny kvalifikationsgrund enligt vilken ett brott är grovt, om brottet riktar sig mot ett informationssystem vars skadande äventyrar energiförsörjningen, den allmänna hälso- och sjukvården, försvaret, rättsvården eller någon annan med dessa jämförbar viktig samhällsfunktion.

Ett exempel på ett sådant väsentligt informationssystem som nämns ovan är det säkerhetsnät som avses regeringens proposition (RP 54/2013 rd) med förslag till lag om verksamheten i den offentliga förvaltningens säkerhetsnät. Enligt den propositionen ska säkerhetsnätet användas i myndigheternas interna, inbördes och externa samarbete och kommunikation som ansluter sig till statens ledning och säkerhet, försvaret, den allmänna ordningen och säkerheten, gränssäkerheten, räddningsverksamheten, sjöräddningen, nödcentralsverksamheten, invandringen och den prehospitala akutsjukvården och där kraven på hög beredskap eller hög säkerhet iakttas. Också system som hänför sig till att trygga försörjningsberedskapen kan utgöra väsentliga system. I statsrådets beslut om målen med försörjningsberedskapen (5.12.2013) nämns som sektorer inom den väsentliga infrastrukturen systemen för produktion, överföring och distribution av energi; informations- och kommunikationssystem, -nät och –tjänster; tjänster inom finanssektorn; transporter och logistik; vattenförsörjning; byggande och underhåll av infrastrukturen och avfallshanteringen i exceptionella situationer. Också t.ex. livsmedelsförsörjningen kunde vara en sådan viktig funktion som avses i den nu föreslagna bestämmelsen. I statsrådets principbeslut (16.12.2010) om en säkerhetsstrategi för samhället konstateras det för sin del att de vitala funktionerna är tvärsektoriella funktionshelheter som är nödvändiga för samhället och som alltid måste vara tryggade. Det finska samhällets vitala funktioner är enligt principbeslutet ledning av staten, internationell verksamhet, Finlands försvarsförmåga, den inre säkerheten, ekonomins och infrastrukturens funktionsförmåga, befolkningens utkomstskydd och handlingsförmåga samt mental kristålighet. Också i statsrådets principbeslut om en strategi för cybersäkerheten i Finland (24.1.2013) hänvisas det till det finska samhällets vitala funktioner som anges ovan i statsrådets principbeslut (16.12.2010) och till statsrådets beslut om målen med försörjningsberedskapen (5.12.2013).

I grovt störande av post- och teletrafik föreslås det för sin del en ny kvalifikationsgrund som täcker de objekt som avses i grundformen av störande av post- och teletrafik och enligt vilken brottet är grovt, om vid störande av post- och teletrafik brottet riktar sig mot en apparat, ett informationssystem eller kommunikation vars skadande äventyrar energiförsörjningen, den allmänna hälso- och sjukvården, försvaret, rättsvården eller någon annan med dessa jämförbar viktig samhällsfunktion.

I enlighet med det som sägs ovan föreslås det att till grov dataskadegörelse för sin del fogas en grund som kvalificerar brottet som grovt, om brottet riktar sig mot ett informa-

tionssystem vars skadande äventyrar energiförsörjningen, den allmänna hälso- och sjukvården, försvaret, rättsvården eller någon annan med dessa jämförbar viktig samhällsfunktion.

De grova gärningsformer av de ovan nämnda brotten som föreslås nu kan ibland överlappa kriminaliseringen av sabotage. I vissa situationer är de ovan nämnda kriminaliseringarna mer heltäckande än sabotage, medan rekvisitet för sabotage för sin del kan uppfyllas i vissa situationer trots att rekvisitet för de kriminaliseringarna inte uppfylls. Om någon har förorsakat allvarlig fara genom att obehörigen ingripa i ett datasystems funktion på det sätt som avses i bestämmelsen om sabotage i strafflagens 34 kap. 1 § 2 mom., uppfylls inte nödvändigtvis rekvisitet för grov dataskadegörelse, om det inte föreligger ett sådant syfte att skada som förutsätts i 35 kap. 3 b § i strafflagen. På motsvarande sätt överlappar rekvisitet för sabotage i vissa situationer delvis kriminaliseringen av grovt störande av post- och teletrafik och grov systemstörning. Också i den gällande lagen överlappar rekvisiten för sabotage och grovt störande av post- och teletrafik samt grov systemstörning delvis varandra. Dataskadegörelse, systemstörning och störande av post- och teletrafik är dock särskilda bestämmelser i förhållande till sabotage, eftersom de förutsätter ett särskilt uppsåt eller gärningssätt. De kan således bli tillämpliga i stället för sabotage även om allvarlig fara har förorsakats. Sabotage kan i sin tur bli tillämpligt i situationer där det inte föreligger ett sådant särskilt uppsåt eller gärningssätt som avses ovan, men gärningen ändå förorsakar allvarlig fara. Det är inte möjligt att ange några absoluta konkurrensregler, och varje situation ska lösas med beaktande av omständigheterna i det enskilda fallet, enligt de allmänna principerna om lagkonkurrens.

Missbruk av personuppgifter

Enligt artikel 5 ska medlemsstaterna 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.

I den nationella lagstiftningen i Finland finns det inte några bestämmelser som uttryckligen skulle täcka de situationer som avses i punkt 5. I de situationer som avses där handlar det om s.k. identitetsstöld, dvs. missbruk av någon annans personuppgifter, när ett brott som avses i artikel 4 (olaglig systemstörning) eller artikel 5 (olaglig datastörning) begås. I typfallet kan det i dessa situationer handla om att dölja de datatekniska spåren efter gärningsmannen. Även utredningsåtgärderna och misstankarna kan då rikta sig mot den person vars identitets-, individualiserings- eller identifieringsuppgifter har använts. Också t.ex. en IP-adress till en persons dator kan vara en sådan identitetsuppgift som avses här.

Man kan välja mellan flera olika genomförandealternativ för att uppfylla förpliktelserna i direktivet. Det första alternativet är att göra användningen av någon annan persons identitet på det sätt som avses i punkt 5 till en kvalifikationsgrund utifrån vilken den föreslagna dataskadegörelsen (SL 35:3 a), störande av post- och teletrafik (SL 38:5) eller systemstörning (SL 38:7 a) i typfallet bedöms som grova. Det alternativet kan dock inte anses vara optimalt, eftersom det t.ex. för de brottens del torde vara mycket typiskt att gärningsmannen försöker dölja sina spår på det sätt som avses här. Vid bedömningen är det också av betydelse att man på grund av förpliktelserna i direktivet föreslår att straffnivån för de grova gärningsformerna av de brotten höjs till fem års fängelse. Inte heller i den nämnda punkt 5 i direktivet har avsikten varit att någon viss lägsta nivå på maximistraffet, t.ex. fem års fängelse, ska bli tillämplig i de situationer som avses där.

Av de allmänna straffskärpningsgrunderna i strafflagens 6 kap. 5 § motsvarar främst det kriterium som nämns i paragrafens 1 punkt, dvs. att den brottsliga verksamheten har varit planmässig, det missbruk av någon annans personuppgifter som avses i punkt 5 i artikeln. Detta är också det andra alternativet

för att uppfylla förpliktelserna i direktivet. Också i själva punkt 5 i artikeln sägs det att medlemsstaterna ska se till att de situationer som avses i punkten ”i enlighet med nationell rätt kan anses som en försvårande omständighet”. Skrivningen ger det nationella genomförandet stort spelrum. Det nationella spelrummet betonas vidare också i skäl 19 i ingressen, där det sägs följande: ”Medlemsstaternas nationella rätt bör innehålla regler om försvårande omständigheter i enlighet med de tillämpliga regler om försvårande omständigheter som fastställts genom deras rättsystem. De bör se till att rätten vid påföljdsbestämningen har möjlighet ta hänsyn till dessa försvårande omständigheter. Det är upp till rätten att bedöma dessa omständigheter, tillsammans med övriga faktiska sakomständigheter i det enskilda fallet.” Det är dock motiverat att de förpliktelser i punkt 5 som hänför sig till identitetsstölder trots det genomförs genom att man, delvis på grund av nationella behov, tar in uttryckliga bestämmelser om saken i den nationella lagstiftningen.

Ett tredje alternativ för genomförandet är att de situationer som avses i punkt 5 skulle utgöra en ny allmän straffskärpningsgrund i strafflagens 6 kap. 5 §. Den situation enligt punkt 5 som avses här kan dock anses vara alltför specifik, och det är inte motiverat att den tas in som en ny allmän straffskärpningsgrund.

Ett fjärde genomförandealternativ kunde vara att i fråga om den aktuella punkten hänvisa till strafflagens 6 kap. 4 §, enligt vilken straffet ska mätas ut så att det står i ett rättvist förhållande till hur skadligt och farligt brottet är, motiven till gärningen samt gärningsmannens av brottet framgående skuld i övrigt. Detta genomförandealternativ kan dock inte bedömas vara optimalt med beaktande av de nationella behoven.

Förpliktelserna enligt direktivet kan på det sätt som framgår av punkt 5 även uppfyllas så att de situationer som avses i punkten täcks i rekvisitet för något annat brott, dvs. det görs en självständig kriminalisering i fråga om dem (det femte genomförandealternativet). I propositionen föreslås det också att i strafflagens 38 kap. tas in en ny 9 b §, som motsvarar bestämmelserna i direktivet, dock utan att man begränsar sig till de brott som avses i artiklarna 4 och 5 i direktivet. I paragrafen sägs att "Den som i syfte att vilseleda en tredje part obehörigen använder någon annans personuppgifter eller identifieringsuppgifter eller andra motsvarande uppgifter som identifierar personen, och därmed orsakar ekonomisk skada eller mer än ringa olägenhet för den som uppgifterna gäller, ska för identitetsstöld dömas till böter”. Straffet för de gärningar som avses i artiklarna 4 och 5 i direktivet kunde då vid behov skärpas i enlighet med punkt 5 genom ett gemensamt straff, om personen även döms för en gärning som avses i den nya 9 b §. Skyddsobjektet för den gärning som avses i den nya 9 b § är identitetens okränkbarhet (för den person vars personuppgifter har använts), medan skyddsobjektet för de gärningar som avses i artiklarna 4 och 5 i direktivet och de nationella kriminaliseringar som motsvarar dem för sin del är informationssystem eller data. Enligt konkurrenslärorna är det således möjligt att döma till straff för båda brotten. Å andra sidan kräver direktivet inte ens att straffet skärps, om en gärning som avses i punkt 5 täcks av en kriminalisering i nationell lag, som den som nu föreslås i propositionen.

Det är t.ex. möjligt att en person genom att använda någon annans personuppgifter har gjort sig skyldig till bedrägeri enligt 36 kap. 1 § i strafflagen. I detta fall är den som har vilseletts en person som t.ex. bestämmer över en ekonomisk förmån och det centrala skyddsobjektet skyddet för den vilseledda personens egendom. I den nu föreslagna kriminaliseringen av identitetsstöld är skyddsobjektet för sin del okränkbarheten av den persons identitet vars personuppgifter har använts vid bedrägeriet. Gärningsmannen kan således dömas för båda brotten. Å andra sidan kan gärningsmannen dömas för identitetsstöld trots att han eller hon inte döms för bedrägeri, om det finns förutsättningar för att döma för identitetsstöld. På motsvarande sätt är det centrala skyddsobjektet t.ex. vid systemstörning (SL 38:7 a) ett informationssystems störningsfria funktion. Också brottsoffret är ofta en annan person. Det är således möjligt att döma samtidigt också för systemstörning och identitetsstöld. Detsamma gäller

också t.ex. dataskadegörelse (SL 35:3 a), där skyddsobjektet är dataintegriteten och offret ofta är en annan person än vid identitetsstölden. Den föreslagna nya kriminaliseringen av identitetsstöld klarlägger t.ex. för bedrägeribrottens del målsägandeställningen för den vars personuppgifter har använts.

För att uppfylla kraven i direktivet skulle det räcka att man begränsar den ovan nämnda kriminaliseringen till att enbart gälla situationer där någon samtidigt har gjort sig skyldig till störande av post- och teletrafik enligt 5 §, grovt störande av post- och teletrafik enligt 6 §, systemstörning enligt 7 a § eller grov systemstörning enligt 7 b § i strafflagens 38 kap. eller dataskadegörelse enligt 3 a § eller den grova gärningsformen av det brottet enligt 3 b § i strafflagens 35 kap. eller till straffbart försök till de brotten. En sådan begränsning är dock inte motiverad, eftersom ett motsvarande och i sak lika klandervärt döljande av spår och därmed orsakande av olägenhet för den person som identitetsuppgifterna gäller även kan förekomma vid andra brott. I punkt 5 i artikeln och i den nya 9 b § som nu föreslås koncentrerar man sig på den person vars identitetsuppgifter har missbrukats. I detta fall är denna person offer för identitetsstöld, och syftet med den föreslagna nya bestämmelsen är att förbättra hans eller hennes ställning. Om kriminaliseringen av missbruk av någon annans personuppgifter skulle kopplas till fullbordade gärningsformer för vissa andra av de angivna brotten, kunde detta i en del fall orsaka problem för att målsägandena i de brotten av en eller annan orsak inte vill att åtal väcks. Då skulle man inte heller kunna väcka åtal enligt den föreslagna 9 b §, trots att den vars personuppgifter har missbrukats skulle ha förorsakats olägenhet. Denna situation kunde uppstå bl.a. för att den dataskadegörelse som föreslås i strafflagens 35 kap. 3 a § och systemstörning enligt strafflagens 38 kap. 7 a § är målsägandebrott. I den föreslagna 9 b § kan man inte heller begränsa sig till enbart kommunikation i internetmiljön eller i telenät för att uppfylla kraven i direktivet, eftersom ett informationssystem och post- och teletrafiken kan störas eller data skadas också fysiskt och i den reella världen. För den föreslagna nya 9 b § talar, utöver att uppfylla kraven i direktivet, även det att en kriminalisering som täcker identitetsstöld och särskilt ställningen för offret för identitetsstöld, dvs. för den person vars identitetsuppgifter har använts, under den senaste tiden har fått uppmärksamhet på det nationella planet (se t.ex. projektet rörande skapande av identitet (identitetsprogrammet), arbetsgruppens slutrapport, inrikesministeriets publikationer 32/2010 och justitieministeriets bedömningspromemoria om identitetsstöld, OM 4/41/2013, samt remissammandraget över promemorian, Betänkanden och utlåtanden 47/2013).

Den föreslagna nya kriminaliseringen ska vara begränsad till situationer där ekonomisk skada eller mer än ringa olägenhet har orsakats. En sådan begränsning är tillåten i direktivet, eftersom kriminaliseringsförpliktelsen i artiklarna 4 och 5 i direktivet endast gäller situationer som inte är ringa. Den straffskärpningsgrund som avses i artikel 9.5 i direktivet och som gäller missbruk av någon annan persons personuppgifter kan således begränsas till att täcka situationer som inte är ringa.

Artikel 10. *Juridiska personers ansvar.* Enligt punkt 1 i artikeln ska medlemsstaterna 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.

Enligt punkt 2 i artikeln ska medlemsstaterna 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.

Enligt punkt 3 i artikeln ska juridiska personers ansvar enligt punkterna 1 och 2 inte

utesluta lagföring av fysiska personer som begår, anstiftar eller medverkar till något av de brott som avses i artiklarna 3—8.

Artikeln är en standardbestämmelse om juridiska personers ansvar som finns i många av Europeiska unionens författningar. Rambeslutet innehåller en till sakinnehållet motsvarande artikel, som behandlas i den regeringsproposition som gäller ikraftsättandet av konventionen och genomförandet av rambeslutet (RP 153/2006 rd), och det är inte ändamålsenligt att analysera de allmänna förutsättningarna för juridiska personers ansvar i detta sammanhang. Konventionen innehåller också bestämmelser som till sitt sakinnehåll är av motsvarande slag.

I Finland finns de gällande allmänna bestämmelserna om straffansvar för juridiska personer i strafflagens 9 kap. För de enskilda straffbestämmelsernas del förutsätts det att det finns en straffbestämmelse om saken i strafflagen för att juridiska personers straffansvar ska bli tillämpligt.

Enligt strafflagens 9 kap. 2 § 1 mom. döms en juridisk person till samfundsbot, om någon som hör till ett av dess lagstadgade organ eller annars hör till dess ledning eller utövar faktisk beslutanderätt inom den juridiska personen har varit delaktig i brottet eller tillåtit att brottet har begåtts eller om i den juridiska personens verksamhet inte har iakttagits den omsorg och försiktighet som krävs för att förebygga brottet. Enligt samma paragrafs 2 mom. döms samfundsbot ut även om det inte kan utredas vem gärningsmannen är eller om gärningsmannen av någon annan anledning inte döms till straff. Enligt kapitlets 3 § anses ett brott begånget i en juridisk persons verksamhet, om gärningsmannen har handlat på den juridiska personens vägnar eller till dess förmån och gärningsmannen hör till den juridiska personens ledning eller står i tjänste- eller arbetsförhållande till denna eller har handlat på uppdrag av en representant för den juridiska personen.

Straffansvaret för juridiska personer utsträcker sig i dag till följande brott som avses i direktivet:

1. orsakande av fara för informationsbehandling (SL 34:9 a)
2. (data)skadegörelse (SL 35:1.2) och den föreslagna nya kriminaliseringen av dataskadegörelse (SL 35:3 a)
3. grov (data)skadegörelse (SL 35:2) och den föreslagna nya kriminaliseringen av grov dataskadegörelse (SL 35:3 b)
4. kränkning av kommunikationshemlighet (SL 38:3)
5. grov kränkning av kommunikationshemlighet (SL 38:4)
6. störande av post- och teletrafik (SL 38:5)
7. grovt störande av post- och teletrafik (SL 38:6)
8. systemstörning (SL 38:7 a)
9. grov systemstörning (SL 38:7 b)
10. dataintrång (SL 38:8)
11. grovt dataintrång (SL 38:8 a)

Straffansvaret för juridiska personer täcker inte lindrig skadegörelse, lindrigt störande av post- och teletrafik, lindrig systemstörning eller innehav av hjälpmedel vid nätbrott. Det ska inte heller täcka den föreslagna kriminaliseringen av lindrig dataskadegörelse (SL 35:3 c). Det är inte motiverat att utsträcka straffansvaret för juridiska personer till de ovan nämnda lindriga gärningsformerna. Arrangemanget står i samklang med direktivet, eftersom den internationella förpliktelsen inte gäller ringa fall. Däremot bör man, för uppfylla förpliktelserna i direktivet, utsträcka straffansvaret för juridiska personer till innehav av hjälpmedel vid nätbrott (SL 34:9 b), om ”anskaffning i syfte att använda" inte täcks på ett uttömmande sätt i SL 34 kap. 9 a § i stället för den nuvarande 9 b §. I propositionen föreslås det dock att ”anskaffning i syfte att använda" täcks i 9 a §. I samband med den regeringsproposition som gäller ikraftsättandet av konventionen och genomförandet av rambeslutet (RP 153/2006 rd, s. 28) var det ännu inte nödvändigt att utsträcka straffansvaret för juridiska personer till innehav av hjälpmedel vid nätbrott, eftersom ansvaret enligt konventionen även kunde innebära privaträttsligt skadeståndsansvar. Rambeslutet förutsatte däremot böter eller administrativa avgifter, men dess tillämpningsområde omfattade inte hjälpmedel vid brott.

Artikeln förutsätter att straffansvaret för juridiska personer utsträcks till de i propositionen föreslagna nya kriminaliseringarna av dataskadegörelse (SL 35:3 a) och grov data-

skadegörelse (SL 35:3 b), genom vilka dataskadegörelse och grov dataskadegörelse avskiljs från rekvisitet för grundformen av skadegörelse.

Artikel 11. *Påföljder för juridiska personer.* Också artikeln om påföljder mot juridiska personer är en standardbestämmelse. Den motsvarar artikeln i rambeslutet. Enligt artikeln ska medlemsstaterna 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. På det sätt som sades vid den föregående artikeln har ansvaret för juridiska personer täckts i Finland eller ska täckas genom straffansvar för juridiska personer och samfundsbot enligt strafflagens 9 kap. i fråga om de brott som avses i direktivet.

I punkt 1 i artikeln finns det också en exempelförteckning över alternativa påföljder, av vilka en del är främmande för rättssystemet i Finland. Detta saknar dock betydelse, eftersom bestämmelsen inte är förpliktande till dessa delar. I punkt 2 i artikeln finns dessutom en bestämmelse enligt vilken 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.

Artikeln förutsätter inte ändringar i lagstiftningen.

Artikel 12. *Behörighet.* Enligt punkt 1 i artikeln ska medlemsstaterna 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. Enligt punkt 2 i artikeln ska en medlemsstat i de fall som avses i 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.

Enligt punkt 3 i artikeln ska en medlemsstat 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.

Också konventionen och rambeslutet innehåller bestämmelser om behörighet, även om förpliktelserna i dem avviker något från förpliktelserna i direktivet till sin omfattning.

I Finland finns de gällande bestämmelserna om strafflagens tillämpningsområde i strafflagens 1 kap.

Den bestämmelse som motsvarar punkt 1 a i artikeln är kapitlets 1 §, enligt vilken finsk lag tillämpas på brott som har begåtts i Finland. Punkt 2 i artikeln motsvaras av 10 § 1 mom., enligt vilket ett brott anses vara begånget såväl där den brottsliga handlingen företogs som där den rekvisitsenliga följden av brottet framträdde.

Punkt 1 b i artikeln motsvaras av 6 §, enligt vilken finsk lag tillämpas på brott som en finsk medborgare har begått utomlands. I kapitlets 11 § finns som en ytterligare förutsättning också det s.k. kravet på dubbel straffbarhet.

Punkt 3 i artikeln har inte någon omedelbar betydelse med tanke på lagstiftningen, eftersom den endast innehåller en underrättelseskyldighet som gäller en eventuell mer omfattande behörighet. Av betydelse när det gäller punkt 3 a är dock strafflagens 1 kap. 6 § 3 mom. 1 punkt, enligt vilken med finsk medborgare jämställs den som vid gärningstidpunkten eller när rättegången inleds är varaktigt bosatt i Finland. Kommissionen ska underrättas om den bestämmelsen i samband med meddelandet om genomförande. När det gäller punkt 3 b i artikeln om gärningar som har begåtts till förmån för en juridisk person finns det ingen motsvarande behörighetsbestämmelse i Finland.

De gällande bestämmelserna motsvarar förpliktelserna i artikeln. Artikeln förutsätter inte ändringar i lagstiftningen.

Artikel 13. *Informationsutbyte.* I punkt 1 i artikeln sägs det att 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.

Enligt punkt 2 i artikeln ska medlemsstaterna 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.

I artikel 35 i konventionen och artikel 11 i rambeslutet finns det redan bestämmelser om den kontaktpunkt och det nät som avses i artikeln. Konventionen har satts i kraft i Finland genom republikens presidents förordning 768/2007. I artikeln åläggs medlemsstaterna också endast att se till att de har en sådan kontaktpunkt och att använda det befintliga nätet. Punkt 1 i artikeln i direktivet motsvarar i sak artikeln i rambeslutet. Det enda relevanta tillägget är att kontaktpunkterna enligt punkt 1 i artikeln i direktivet i brådskande fall inom högst åtta timmar efter att ha tagit emot en begäran ska kunna ange huruvida begäran kommer att besvaras samt formen och den beräknade tidpunkten för svaret. I dag är centralkriminalpolisen kontaktpunkt i Finland. Kommissionen ska underrättas om detta i samband med meddelandet om genomförande av direktivet, i enlighet med punkt 2 i artikeln. Åttatimmarsregeln i artikeln förutsätter inte författningsändringar. Polisens interna anvisningar kommer att uppdateras så att en kvittering kan ges inom åtta timmar.

Enligt punkt 3 i artikeln ska medlemsstaterna 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.

Punkten är en uppmaning av allmän natur, och de lämpliga rapporteringskanalerna definieras inte närmare. I praktiken är det klart att det finns rapporteringskanaler för att rapportera brott. Deras lämplighet bestäms för sin del nationellt. Sådana rapporteringskanaler som avses i punkten är i Finland bl.a. polisanmälan, som i vissa fall även kan göras elektroniskt, e-postanmälningar eller telefonsamtal till en myndighet, den s.k. ”blåa knappen” på polisens webbplats, dvs. nättips, samt anmälan till Kommunikationsverkets cybersäkerhetscenter (cert-fi), för vilket ändamål det bl.a. finns en länk, ”anmäl kränkningar av informationssäkerheten”, på Kommunikationsverkets webbplats. Punkten förutsätter inte författningsändringar.

Artikel 14. *Övervakning och statistik.* Enligt punkt 1 i artikeln ska medlemsstaterna se till att det finns ett system för registrering, insamling och tillhandahållande av statistiska uppgifter om de brott som avses i artiklarna 3—7. I punkt 2 sägs det att de statistiska uppgifterna åtminstone ska 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.

Enligt punkt 3 ska medlemsstaterna 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.

De befintliga uppgifter som avses i direktivet kan fås och översändas på det sätt som förutsätts i direktivet utan författningsändringar. Statistikföringen underlättas dessutom av den nya självständiga kriminaliseringen av dataskadegörelse som föreslås i propositionen, vilket betyder att uppfyllandet av de internationella förpliktelserna inte längre grundar sig på 2 mom. i grundformen av skadegörelse. Detta relevant, eftersom brottsrubriceringen är väsentlig vid statistikföringen. Om inte dataskadegörelse skulle avskiljas till ett särskilt brott, skulle ett stort antal fall av skadegörelse som inte har någon anknytning till nätbrott statistikföras under kriminaliseringen av skadegörelse.

Artiklarna 15—19. Artiklarna 15—19 innehåller sedvanliga slutbestämmelser om ersättande av det tidigare rambeslutet 2005/222/RIF, införlivande av förpliktelserna i direktivet med den nationella lagstiftningen, rapportering, ikraftträdande och adressater.

2 Lagförslag

2.1 Strafflagen

34 kap. **Om allmänfarliga brott**

9 a §. *Orsakande av fara för informationsbehandling.* På det sätt som anges i detaljmotiveringen till artikel 7 ovan föreslås det att till 1 mom. 1 punkten i den kriminalisering som gäller s.k. hjälpmedel vid nätbrott fogas ett nytt gärningssätt, *anskaffning i syfte att använda*. Enligt 1 mom. 1 punkten kan även den dömas för orsakande av fara för informationsbehandling som i syfte att orsaka olägenhet eller skada för informationsbehandling eller för ett informations- eller kommunikationssystems funktion eller säkerhet

1) för in i landet, *anskaffar i syfte* att använda, tillverkar, säljer eller annars sprider eller ställer till förfogande

a) sådana apparater, datorprogram eller programinstruktioner som har skapats eller anpassats för att äventyra eller skada informationsbehandling eller ett informations- eller kommunikationssystems funktion eller för att bryta eller avkoda det tekniska skyddet vid elektronisk kommunikation eller skyddet för ett informationssystem, eller

b) andra personers lösenord eller åtkomstkoder eller andra motsvarande uppgifter om informationssystem.

Tillägget behövs för att genomföra direktivets artikel 7, som gäller verktyg som används för att begå brott, artikel 9.2, som förutsätter ett maximistraff på minst två års fängelse, och artikel 10, som gäller juridiska personers ansvar. Innehav av hjälpmedel vid nätbrott kriminaliseras i dag i kapitlets 9 b §, som gäller innehav av hjälpmedel vid nätbrott. Den kriminaliseringen uppfyller dock inte kraven i direktivet, eftersom anskaffning i syfte att använda som avses i direktivet och å andra sidan innehav delvis är olika gärningssätt, på det sätt som anges i detaljmotiveringen till artikel 7 och nedan, och de gärningssätten också har skiljts åt i konventionen. Enligt kapitlets 13 § tillämpas inte heller straffansvar för juridiska personer på den gällande 9 b §, till skillnad från när det gäller orsakande av fara för informationsbehandling enligt 9 a §.

Direktivet förutsätter ett maximistraff på två år i fråga om ”anskaffning i syfte att använda”. Maximistraffet för innehav av hjälpmedel vid nätbrott, dvs. den gärning som avses i strafflagens 34 kap. 9 b §, är sex månaders fängelse. Enbart innehav av hjälpmedel vid nätbrott kan dock inte anses vara ett lika klandervärt brott som orsakande av fara för informationsbehandling enligt 9 a §. Det är således inte motiverat att höja maximistraffet i 9 b § till två års fängelse. Anskaffning i syfte att använda kan också anses vara mer klandervärt än enbart innehav och innebär inte samma sak, trots att hjälpmedlet som en följd av anskaffningen kommer i den persons besittning som har anskaffat det. Anskaffning i syfte att orsaka olägenhet eller skada förutsätter att en person vidtar aktiva åtgärder för att få hjälpmedlet i sin besittning, till skillnad från vid innehav, då rekvisitet kan uppfyllas redan på den grunden att en person helt enkelt innehar ett hjälpmedel, förutsatt att de övriga kriterierna i bestämmelsen, t.ex. att syftet varit att orsaka olägenhet eller skada, uppfylls. Anskaffning i syfte att använda kan för sin del förutsätta bl.a. aktivt letande, anskaffning av information och som en följd av detta t.ex. beställning av ett hjälpmedel via internet. Det väsentliga är således ett aktivt handlande för att skaffa ett hjälpmedel i syfte att använda det för att orsaka olägenhet eller skada. Rekvisitet för anskaffar i syfte att använda uppfylls först när personen i fråga har fått verktyget i sin besittning.

14 §. *Definitioner.* Av de orsaker som anges i detaljmotiveringen till artikel 2 och i motiveringen till 38 kap. 13 § nedan föreslås det att till kapitlet ska fogas en ny definitionsbestämmelse, där det i fråga om 34 kap. 9 a och 9 b § ingår en hänvisning till definitionen av informationssystem i den föreslagna 13 § i 38 kap.

35 kap. **Om skadegörelse**

1 §. *Skadegörelse.* Det föreslås att 2 och 3 mom., som gäller s.k. dataskadegörelse, i paragrafen om skadegörelse upphävs av de orsaker som anges i detaljmotiveringen till artikel 5. Motsvarande reglering överförs, preciserad genom de ändringar som direktivet förutsätter, till en självständig 3 a § om dataskadegörelse. Då behöver maximistraffet för vanlig skadegörelse inte höjas på grund av kraven i artikel 9.2 i direktivet. Genom den föreslagna lösningen försöker man också förtydliga bestämmelserna i skrivtekniskt avseende, eftersom regleringssättet även påverkar regleringen av den grova gärningsformen av skadegörelse. När skadegörelse och dataskadegörelse skiljs åt möjliggörs också en bättre statistikföring av de gärningar som utgör dataskadegörelse, på det sätt som artikel 14 förutsätter.

2 §. *Grov skadegörelse.* Det föreslås att 2 punkten, som hänför sig till dataskadegörelse, i 1 mom. i paragrafen om grov skadegörelse upphävs. Den regleringen föreslås bli överförd till den nya 3 b § om grov dataskadegörelse, på det sätt som anges i detaljmotiveringen till artikel 5 och artikel 9.3 och 9.4, kompletterad med de tillägg som direktivet förutsätter. Detta motsvarar den lösning som valts när det gäller skadegörelse enligt grundformen.

3 a §. *Dataskadegörelse.* Av de orsaker som anges vid 1 § ovan och i detaljmotiveringen till artikel 5 föreslås det att till kapitlet fogas en ny paragraf om dataskadegörelse, varvid dataskadegörelserna flyttas från den gällande 1 § om skadegörelse. Enligt 1 mom. kriminaliseras det som dataskadegörelse att en person i syfte att skada någon annan obehörigen förstör, försämrar, döljer, skadar, ändrar, gör det omöjligt att komma åt eller hemlighåller information som har upptagits på ett datamedium eller någon annan upptagning eller data i ett informationssystem.

I sak är den nya paragrafen i princip innehållsmässigt densamma som den gällande 1 § 2 och 3 mom., som upphävs. För att uppfylla förpliktelserna i artikel 5 i direktivet utökas gärningssätten dock med försämra, ändra och göra det omöjligt att komma åt. Dessutom kan gärningen i enlighet med kraven i direktivet rikta sig förutom mot information som har upptagits på ett datamedium eller någon annan upptagning även mot data i ett informationssystem. Det tillägget är väsentligt, eftersom data som finns i ett informationssystem inte behöver ha upptagits permanent utan även kan finnas i någon annan form. Data kan t.ex. överföras inom ett informationssystem. I enlighet med kraven i direktivet ska straffskalan för den föreslagna nya kriminaliseringen dataskadegörelse vara böter eller fängelse i högst två år. Dataskadegörelse ådagalägger i många fall en högre grad av uppsåt, och brottet förutsätter således ofta en viss eller större planmässighet än skadegörelse enligt grundrekvisitet. Det är därför motiverat att man kan tillämpa ett högre maximistraff vid dataskadegörelse än vid skadegörelse enligt grundrekvisitet.

I samband med regeringens proposition 153/2006 rd föreslogs det att maximistraffet för skadegörelse enligt grundrekvisitet i 1 § skulle höjas till två års fängelse för att uppfylla kraven i rambeslutet. Lagutskottet noterade då i sitt betänkande (LaUB 23/2006 rd) att förpliktelsen i artikel 7 i rambeslutet att föreskriva ett maximistraff på fängelse i minst två år inte gäller andra skadegörelsebrott än skadegörelse som riktar sig mot information enligt paragrafens 2 mom. Förpliktelserna i rambeslutet gällde vid den tidpunkten dessutom bara om brottet hade begåtts inom ramen för en organiserad kriminell sammanslutnings verksamhet. Utskottet såg ingen anledning att ändra straffskalan för skadegörelse i den utsträckning som föreslogs bara för att genomföra den ytterst snäva förpliktelsen i rambeslutet. Utskottet ansåg att ändringen skulle ha kunnat få oförutsebara kriminalpolitiska konsekvenser, med hänsyn till hur allmänna skadegörelsebrott är och till att det handlar om en typisk form av ungdomsbrottslighet. En annan synpunkt som utskottet ansåg att talade mot den höjning av maximistraffet som föreslogs då var att skadegörelse därigenom skulle ha blivit ett strängare bestraffat brott än stöld. I första fasen av den totala strafflagsreformen konstaterades det i samband med att bestämmelserna om egendomsbrott sågs över att skadegörelsebrott i snitt ådagalägger mindre skuld än de flesta andra egendomsbrott och att det inte är motiverat att ställa sig lika strängt till dem som t.ex. till stöldbrott (RP 66/1988 rd). Ut-

skottet ansåg att den här uppfattningen fortfarande gällde. De synpunkter som nämns ovan är fortfarande av betydelse vid genomförandet av detta direktiv. Därför föreslås det i propositionen att dataskadegörelse ska avskiljas till ett självständigt brott.

Enligt paragrafens 2 mom. ska försök till dataskadegörelse vara straffbart, på samma sätt som i 1 § 3 mom. i dag. Även artikel 8 i direktivet förutsätter detta.

3 b §. *Grov dataskadegörelse.* Till kapitlet fogas en ny paragraf om grov dataskadegörelse, på det sätt som anges i samband med 1, 2 och 3 a § ovan och i detaljmotiveringen till artikel 5 och artikel 9.3 och 9.4. Dataskadegörelse kvalificerar som grov för det första om det vid dataskadegörelse vållas synnerligen kännbar olägenhet eller ekonomisk skada. På den grunden uppfylls kraven i artikel 9.4 b i direktivet, vilka hänför sig till förorsakande av allvarlig skada. Kvalifikationsgrunden motsvarar kvalifikationsgrunden i 1 mom. 1 punkten i den gällande bestämmelsen om systemstörning (38 kap. 7 b §). En motsvarande grund föreslås även i den grova gärningsformen av störande av post- och teletrafik (38 kap. 6 §) för att uppfylla förpliktelserna i direktivet. Kvalifikationsgrunden avviker till sina detaljer något från kvalifikationsgrunderna för grov skadegörelse i den gällande 2 § 1 mom. 1 punkten, men innehållet i dem är i stor utsträckning detsamma, och den kvalifikationsgrund som nu föreslås och som överensstämmer med den formulering som i dag finns i bestämmelsen om grov systemstörning kan anses lämpa sig bättre för dataskadegörelse. I kvalifikationsgrunden för grov dataskadegörelse nämns inte nu uttryckligen avsevärd skada på egendom som är synnerligen värdefull i historiskt eller kulturellt hänseende. Om dataskadegörelsen orsakar avsevärd skada på sådan synnerligen värdefull egendom, ska den nu föreslagna kvalifikationsgrunden om synnerligen kännbar olägenhet eller ekonomisk skada i allmänhet bli tillämplig i praktiken.

Den kvalifikationsgrund som gäller kriminella sammanslutningar ingår även i grov dataskadegörelse, såsom anges i detaljmotiveringen till artikel 9 och 2 § ovan. En identisk grund finns redan i dag i 2 § 2 punkten, som föreslås bli upphävd. Enligt den kan brottet kvalificera som grovt, om det begås som ett led i en i 17 kap. 1 a § 4 mom. avsedd kriminell sammanslutnings verksamhet. För att uppfylla kraven i direktivet föreslås det att en motsvarande grund också ska fogas till grovt störande av post- och teletrafik (38 kap. 6 §) och grov systemstörning (38 kap. 7 b §).

I grov dataskadegörelse ingår också en kvalifikationsgrund som gäller s.k. botnät, såsom anges i detaljmotiveringen till artikel 9.3. Enligt den kan gärningen kvalificera som grov, om brottet begås som ett led i verksamhet där ett betydande antal informationssystem har påverkats genom användning av sådana apparater, datorprogram eller programinstruktioner som avses i 34 kap. 9 a § 1 punkten underpunkt a eller sådana lösenord, åtkomstkoder eller andra motsvarande uppgifter som avses i 9 a § 1 punkten underpunkt b. En motsvarande kvalifikationsgrund fogas också till grovt störande av post- och teletrafik och grov systemstörning.

I grov dataskadegörelse ingår också, i enlighet med kraven i direktivet och så som anges i detaljmotiveringen till artikel 9, en kvalifikationsgrund som gäller s.k. kritisk infrastruktur. Enligt den kan gärningen kvalificera som grov, om brottet riktar sig mot ett informationssystem vars skadande äventyrar energiförsörjningen, den allmänna hälso- och sjukvården, försvaret, rättsvården eller någon annan med dessa jämförbar viktig samhällsfunktion. En motsvarande kvalifikationsgrund fogas också till grovt störande av post- och teletrafik och grov systemstörning.

I enlighet med kraven i artikel 8 i direktivet ska försök vara straffbart, på samma sätt som vid grov skadegörelse i dag.

3 c §. *Lindrig dataskadegörelse.* På samma sätt som när det gäller kriminaliseringen av vanlig skadegörelse föreslås det, i enlighet med vad som sägs i detaljmotiveringen till artikel 5, att till kapitlet fogas en ny paragraf om lindrig dataskadegörelse. Paragrafen är till sitt innehåll likadan som den gällande kriminaliseringen av lindrig skadegörelse. Den blir tillämplig, om dataskadegörelsen, med beaktande av att skadan är liten eller andra omständigheter vid brottet, bedömd som en helhet är ringa. Påföljden är böter.

6 §. *Åtalsrätt.* Det föreslås att i paragrafen ska tas in hänvisningar till den föreslagna

nya paragrafen om dataskadegörelse (3 a §) och lindrig dataskadegörelse (3 c §). Det är fråga om en teknisk ändring som följer av att dataskadegörelse och lindrig dataskadegörelse avskiljs till självständiga kriminaliseringar. Även i fråga om dessa brott får åklagaren väcka åtal endast om målsäganden anmäler brottet till åtal, om enbart enskild egendom har varit föremål för brottet. Paragrafen ändras i skrivtekniskt avseende så att den motsvarar gällande rekommendationer.

7 §. *Åtgärdseftergift.* Det föreslås att i paragrafen ska tas in hänvisningar till den föreslagna nya paragrafen om dataskadegörelse (3 a §) och lindrig dataskadegörelse (3 c §). Det är fråga om en teknisk ändring som följer av att dataskadegörelse och lindrig dataskadegörelse avskiljs till självständiga kriminaliseringar. Även i fråga om dessa brott får eftergift ske i fråga om anmälan, åtal eller straff, om gärningsmannen har ersatt skadan och skadestånd prövas vara en tillräcklig påföljd.

8 §. *Straffansvar för juridiska personer.* Det föreslås en teknisk ändring i paragrafen om straffansvar för juridiska personer, så att paragrafen motsvarar den ändring genom vilken dataskadegörelse och lindrig dataskadegörelse avskiljs till självständiga paragrafer. I dag hänför sig straffansvaret för juridiska personer till 1 § 2 mom., som föreslås bli upphävt. Artikel 10 i direktivet förutsätter, såsom anges i allmänna motiveringen, att straffansvaret för juridiska personer utsträcks till dataskadegörelse och grov dataskadegörelse.

9 §. *Definitioner.* Av de orsaker som anges i detaljmotiveringen till artikel 2 och i motiveringen till 38 kap. 13 § nedan, föreslås det att till kapitlet fogas en ny definitionsbestämmelse som i fråga om de föreslagna 3 a och 3 b § i 35 kap. innehåller en hänvisning till definitionerna av informationssystem och data i den föreslagna nya 13 § i 38 kap.

38 kap. Om informations- och kommunikationsbrott

3 §. *Kränkning av kommunikationshemlighet.* För att uppfylla kraven i direktivet föreslås det att till 1 mom. 2 punkten fogas en hänvisning till dataöverföring som förmedlas genom informationssystem, på det sätt som anges i detaljmotiveringen till artikel 6. Direktivet förutsätter att man kriminaliserar avlyssning (interception) med tekniska hjälpmedel, som sker uppsåtligen och orättmätigt, av icke-offentliga överföringar av datorbehandlingsbara uppgifter (data) till, från eller inom ett informationssystem. I dag täcker paragrafens 1 mom. 2 punkt icke-offentliga överföringar av data mellan, men inte inom, informationssystem. Paragrafens 1 mom. 1 punkt täcker endast meddelanden som har upptagits, och också i fråga om dem är kriteriet för att gärningen ska fullbordas, att bryta ett säkerhetsarrangemang, alltför begränsande för att kraven i direktivet ska uppfyllas. Kraven i direktivet kan dock inte anses gälla meddelanden som har upptagits. Efter den föreslagna ändringen motsvarar lagstiftningen kraven i direktivet så att den bl.a. täcker situationer där någon avlyssnar icke-offentliga överföringar av data inom ett informationssystem, t.ex. meddelanden som användaren matar in via tangentbordet.

Det föreslås att maximistraffet för kränkning av kommunikationshemlighet ska höjas från nuvarande ett års fängelse till två års fängelse i enlighet med kraven i direktivet.

6 §. *Grovt störande av post- och teletrafik.* Såsom anges i detaljmotiveringen till artikel 9 och i motiveringen ovan till grov dataskadegörelse (35 kap. 3 b §), föreslås det att till paragrafen fogas motsvarande kvalifikationsgrunder om användning av botnät, organiserade kriminella sammanslutningar, allvarlig skada och kritisk infrastruktur som i fråga om grov dataskadegörelse. Det föreslås att maximistraffet för grovt störande av post- och teletrafik ska höjas från fyra till fem års fängelse, i enlighet med kraven i artikel 9 i direktivet.

7 a §. *Systemstörning.* Beroende på konkurrenssituationer mellan olika brott föreslås det att subsidiaritetsklausulen för systemstörning ska upphävas. I annat fall kunde det uppstå oändamålsenliga tillämpningssituationer på grund av ändringarna av straffskalorna. Behovet av att slopa subsidiaritetsklausulen hänför sig bl.a. till att maximistraffet för dataskadegörelse (SL 35 kap. 3 a §) framöver är detsamma som för systemstörning. I detaljmotiveringen till artikel 3, som

gäller olagligt intrång i informationssystem, redogörs det för konkurrenssituationer mellan olika brott.

7 b §. *Grov systemstörning.* Såsom anges i detaljmotiveringen till artikel 9, föreslås det att till paragrafen fogas motsvarande kvalifikationsgrunder om botnät, organiserade kriminella sammanslutningar och kritisk infrastruktur som vad som föreslås ovan i fråga om grov dataskadegörelse (35 kap. 3 b §) och grovt störande av post- och teletrafik. Grov systemstörning innehåller redan i dag en kvalifikationsgrund som gäller allvarlig skada (”vållas synnerligen kännbar olägenhet eller ekonomisk skada”), och en motsvarande kvalifikationsgrund föreslås i fråga om grov dataskadegörelse och grovt störande av post- och teletrafik.

Det föreslås att maximistraffet ska höjas från fyra till fem års fängelse, i enlighet med kraven i artikel 9 i direktivet.

8 §. *Dataintrång.* Såsom anges i detaljmotiveringen till artikel 3 föreslås det att 2 mom. ändras så att momentet i mer omfattande grad än i dag täcker fall där någon med tekniska medel skaffar sig tillgång till eller avlyssnar data i ett informationssystem. I dag täcker 2 mom. endast situationer där någon tar reda på information som finns i ett system med tekniska specialanordningar. Genom det gällande 2 mom. har man genomfört bestämmelsen om elektromagnetiska emissioner från datorsystem i artikel 3, som gäller olaglig avlyssning, i konventionen. En motsvarande förpliktelse ingår också i artikel 6 i direktivet.

Enligt förslaget ska straff dömas ut förutom för det gärningssätt som gäller tekniska specialanordningar också när någon utan att tränga in i ett informationssystem eller en del av ett sådant annars med tekniska metoder genom att ta sig förbi säkerhetsarrangemangen, utnyttja informationssystemets sårbarhet eller annars med uppenbart svikliga medel obehörigen tar reda på information eller data som finns i ett sådant informationssystem som avses i 1 mom.

Det föreslagna 2 mom. är teknikneutralt. Meningen är således att momentet ska täcka bl.a. situationer där någon genom att mata in data får ett informationssystem att fungera felaktigt så att det lämnar ut information (t.ex. så kallade SQL-injektioner) och situationer där någon tar reda på information eller data som finns i systemet med hjälp av ett sabotageprogram, som innehavaren av systemet t.ex. har vilseletts till att installera. Frågan om huruvida kriterierna i det föreslagna 2 mom. 2 punkt är uppfyllda och om uppenbart svikliga medel har använts ska bedömas från fall till fall. Det är klart att bestämmelsen inte täcker fall där någon i praktiken får informationen i misstag. Rekvisitet uppfylls ofta inte heller om det inte krävs särskilda datatekniska kunskaper för att få tillgång till de data som finns i ett system eller om dessa inte har skyddats genom särskilda säkerhetsarrangemang. Det svikliga förfarandet ska också vara uppenbart. T.ex. sedvanlig skötsel av ärenden på internet och annan normal användning där man prövar sig fram eller ställer frågor på nätet omfattas inte av tillämpningsområdet för punkten. Det svikliga handlande som avses i punkten ska av gärningsmannen riktas direkt mot ett informationssystem som är i hans eller hennes kommando eller användning. Om gärningen gäller användning av ett informationssystem, ska det svikliga handlandet i allmänhet synas direkt i systemets gränssnitt. För tydlighetens skull kan man konstatera att t.ex. användningen av ett informationssystem via Tornätet eller andra förfaranden eller programvaror som förbättrar användarens integritetsskydd som utgångspunkt inte innebär ett svikligt handlande.

Det svikliga handlandet ska också annars i allmänhet rikta sig direkt mot ett informationssystem eller innehavaren av systemet eller dess administration. Att vilseleda någon som använder ett informationssystem kommer i allmänhet att bedömas som något annat brott. I allmänhet innebär inte heller att t.ex. utnyttja en cross site scripting-sårbarhet (XSS) eller en cross site request forgery-attack (CSRF) att ta reda på information eller data som finns i ett informationssystem, utan det ska bedömas som t.ex. orsakande av fara för informationsbehandling, olovligt brukande, dataskadegörelse, bedrägeri eller betalningsmedelsbedrägeri i stället för som dataintrång, beroende på det aktuella fallet.

Obehörigen i paragrafens 2 mom. hänför sig till användningen av ett informationssy-

stem. Enbart det att informationen är tillgänglig på något annat sätt, t.ex. för att den är offentlig, innebär i sig inte att användningen är behörig.

Det föreslås dessutom att man i 1 mom. i paragrafen om dataintrång vid sidan av ordet ”data” tar in ordet ”information”, för att förtydliga det som man vill reglera i paragrafen. Det föreslås att begreppet data (datorbehandlingsbara uppgifter) definieras såsom förutsätts i direktivet. Paragrafens 1 mom. innebär dock inte i och med definitionen av informationssystem någon allmän kriminalisering av att bryta en kryptering. Att bryta en kryptering är t.ex. inte en del av rekvisitet för denna gärning. Paragrafens 1 mom. gäller dock med stöd av definitionsbestämmelsen i 13 § också att "göra intrång i data” för att uppfylla de tekniska kraven i direktivet. Ordet ”data” i 1 mom. är tänkt att klarlägga att också en innehavare av data och inte bara ägaren av en apparat kan vara målsägande.

Det föreslås att maximistraffet för dataintrång ska höjas från ett till två års fängelse, i enlighet med kraven i artikel 9 i direktivet.

8 a §. *Grovt dataintrång.* I dag är maximistraffet för grovt dataintrång två års fängelse. I enlighet med vad som förutsätts i direktivet ska maximistraffet för dataintrång enligt grundrekvisitet höjas till fängelse i två år. Av den anledningen måste också maximistraffet för grovt dataintrång höjas. I propositionen föreslås det att det nya maximistraffet ska vara tre års fängelse. Det är också annars motiverat att höja maximistraffet, med beaktande av skärpningen av maximistraffnivåerna för de andra motsvarande nätbrotten. Det är dock motiverat att maximistraffet ska vara lägre än vid t.ex. grov dataskadegörelse, grovt störande av post- och teletrafik eller grov systemstörning liksom i dag. Dessutom är ett lägre maximistraff motiverat, eftersom kriminaliseringen av dataintrång också täcker obehöriga handlingar som begåtts s.a.s. för nöjes skull. Om någon efter att ha gjort intrång i ett informationssystem skadar data, hindrar informationssystemets funktion eller hindrar kommunikationen, kan andra kriminaliseringar som eventuellt bestraffas strängare bli tillämpliga.

9 b §. *Identitetsstöld.* I kapitlet föreslås en ny paragraf om identitetsstöld. Förslaget behandlas mer ingående i detaljmotiveringen till artikel 9.5. Enligt förslaget ska den dömas för identitetsstöld som i syfte att vilseleda en tredje part obehörigen använder någon annans personuppgifter eller identifieringsuppgifter eller andra motsvarande uppgifter som identifierar personen, och därmed orsakar ekonomisk skada eller mer än ringa olägenhet för den som uppgifterna gäller. Som påföljd föreslås bötesstraff.

Den föreslagna 9 b § förutsätter för det första att gärningsmannens syfte med att använda uppgifterna har varit att vilseleda en tredje part. Det kriteriet ingår också i direktivet. Det kan också vara ett informationssystem som skapats eller administreras av en person som vilseleds. Det väsentliga för vilseledandets del är att en tredje person vilseleds uttryckligen om någons person eller identitet. En ytterligare förutsättning för straffbarhet är att personen handlar obehörigen. En person handlar inte obehörigen om han eller hon t.ex. har rätt att använda IP-adressen i fråga eller om han eller hon använder sitt namn som också är hans eller hennes eget namn. I den föreslagna kriminaliseringen förutsätts det att någon annans personuppgifter eller identifieringsuppgifter eller andra motsvarande uppgifter som identifierar personen används. Meningen har varit att täcka alla de uppgifter på basis av vilka en tredje part kan vilseledas till att tro att den som använder uppgifterna är samma person som den som uppgifterna gäller. Med personuppgifter avses t.ex. enligt 3 § 1 punkten i personuppgiftslagen (523/1999) alla slags anteckningar som beskriver en fysisk person eller hans egenskaper eller levnadsförhållanden som kan hänföras till honom själv eller till hans familj eller någon som lever i gemensamt hushåll med honom. Med identifieringsuppgifter avses t.ex. enligt 10 kap. 6 § i tvångsmedelslagen (806/2011) uppgifter om ett meddelande vilka kan förknippas med en abonnent eller användare och behandlas i kommunikationsnäten för att överföra, distribuera eller tillhandahålla meddelanden. Bl.a. IP-adresser är sådana uppgifter. Vilka som helst lösryckta uppgifter kommer emellertid inte i fråga, utan det väsentliga är att uppgifterna hänför sig till eller kan kopplas till identifiering och möjliggör identifiering av

en person och således vilseledande. Även om uppgifterna i sig är personuppgifter, saknar de betydelse i den situation som avses här, om de inte förekommer i ett sammanhang eller tillsammans med andra uppgifter som möjliggör identifiering.

”Någon annans” som avses i paragrafen kan också avse en juridisk person. Trots att man med personuppgifter avser personuppgifter enligt personuppgiftslagen som möjliggör identifiering av en fysisk person, är det meningen att skrivningen i den föreslagna bestämmelsen om andra uppgifter som identifierar en person även ska täcka t.ex. uppgifter som identifierar en juridisk person.

Det är dock klart att brottet inte fullbordas, om användningen av uppgifter som rör en annan person är så obetydligt eller som helhet gäller en så lösryckt omständighet eller annars är sådan att det inte finns någon faktisk möjlighet att missta sig. Detta gäller t.ex. om det tydligt framgår att det handlar om satir.

I de fall när någon uppträder under pseudonym, t.ex. ”Matti Meikäläinen” är det klart att personen inte nödvändigtvis använder sitt eget namn i den aktuella situationen och att det högst sannolikt också är fråga om en annan persons namn. Gärningen är dock inte straffbar, om det inte finns något vilseledandesyfte eller om avsikten snarare är att framföra en kommentar anonymt. För att rekvisitet ska uppfyllas är det också väsentligt att avsikten är att vilseleda en tredje person så att han eller hon tror att den som använder uppgifterna är en eller flera andra personer. Väsentligt med tanke på straffansvaret är även, såsom också sagts tidigare, bedömningen av om huruvida det finns risk för att missta sig i den konkreta situationen.

Den användning av personuppgifter som avses i paragrafen gäller inte heller sådan behandling av personuppgifter som har karaktären av förberedelse.

Gärningen ska dessutom ha orsakat ekonomisk skada eller mer än ringa olägenhet. Ekonomisk skada kan uppstå t.ex. i form av utredningskostnader för att rätta till situationen. Begränsningen till ringa situationer gäller endast andra situationer än sådana där ekonomisk skada har uppstått, dvs. olägenhet. I praktiken överlappar olägenhet delvis den förutsättning som gäller ekonomisk skada, men olägenhet täcker även fall där det inte har uppstått någon direkt ekonomisk skada. Sådan olägenhet kunde uppstå t.ex. i en situation där det krävs stor möda för att reda ut och rätta till saken eller detta över huvud taget inte lyckas. Om någon t.ex. har gjort sig skyldig till bedrägerier genom att använda någon annans personuppgifter kan det vara mycket arbetskrävande för denna person att reda ut situationen och de obefogade fakturorna. Olägenhet har också anknytning till skyddet av en persons rätt att använda sig av yttrandefriheten i sitt eget namn. En sådan situation kan i vissa fall föreligga t.ex. när någon har skapat en falsk profil på ett socialt medium i internet genom att använda någon annans personuppgifter. I vissa fall kan det vara svårt att radera en sådan profil. Dessutom kan det krävas att man kontaktar ett stort antal personer som har trott att de kommunicerat med den som identitetsuppgifterna gäller. Utmärkande för uttryckligen de handlingar som begås på internet är det att det är både svårt och orsakar olägenhet att få bort de uppgifter som laddats upp på nätet. Å andra sidan orsakar det i allmänhet inte mer än ringa olägenhet att skicka en enstaka reklamation per e-post i de fall när detta lyckas. Om vilseledandet bildar en till motivationsunderlaget sakligt och tidsmässigt enhetlig helhet där samma persons identitetsuppgifter har använts, ska gärningen betraktas som en enda identitetsstöld också i det fallet att flera tredje parter har vilseletts. Detta betyder att trots att en person exempelvis bara behöver skicka en reklamation per e-post till var och en av de tredje parter som har vilseletts, handlar det inte längre om bara en sådan enstaka lyckad reklamation som nämns ovan. Å andra sidan kan också en enstaka reklamation orsaka mer än ringa olägenhet med beaktande av omständigheterna, t.ex. om en person blir föremål för flera enstaka identitetsstölder från flera olika gärningsmäns sida. Saken ska således bedömas från fall till fall.

Vid brottsutredningen blir de utrednings- och tvångsmedel som kommer i fråga i respektive fall tillämpliga. Det är t.ex. möjligt att i enlighet med 17 § i lagen om yttrandefrihet i masskommunikation (460/2003) utre-

da ett nätmeddelandes identifieringsuppgifter, om det föreligger sannolika skäl att misstänka att innehållet i meddelandet är sådant att det är straffbart att göra det tillgängligt för allmänheten. Det kan vara fråga om en sådan situation t.ex. när en identitetsstöld som avses i den föreslagna paragrafen sker i form av blogginlägg. Vid utredningen av en identitetsstöld blir även sådan teleövervakning med samtycke av den som innehar en teleadress eller teleterminalutrustning som avses i 10 kap. 7 § i tvångsmedelslagen tillämplig i de fall när gärningen har begåtts med användning av en teleadress eller teleterminalutrustning. Även de medel för att skaffa information som avses i 4 kap. 3 § i polislagen kan användas vid utredningen av en identitetsstöld. Enligt den paragrafens 2 mom. har en polisman i enskilda fall på begäran rätt att av teleföretag och av sammanslutningsabonnenter få kontaktuppgifter för teleadresser som inte är upptagna i en offentlig katalog eller information som specificerar en teleadress eller teleterminalutrustning, om informationen behövs för ett polisuppdrag.

Man bör dock lägga märke till att en gärning, beroende på det konkreta gärningssättet, också kan uppfylla rekvisitet för något annat brott, t.ex. ärekränkning eller spridande av information som kränker privatlivet, varvid de tvångsmedel som är tillämpliga på dem blir aktuella. Vidare bör man notera att den identitetsstöld som avses i den föreslagna paragrafen ofta kan begås i samband med något annat brott som är allvarligare, t.ex. bedrägeri. Vid utredningen av bedrägeriet kan man då använda de tvångsmedel som är möjliga vid utredningen av det brottet. Av betydelse till dessa delar är också det syfte med förslaget enligt vilket avsikten med att kriminalisera identitetsstöld är att förtydliga ställningen som målsägande för offret för identitetsstöld t.ex. vid bedrägeribrott.

10 §. *Åtalsrätt.* I paragrafen föreslås ett nytt 4 mom., enligt vilket åklagaren får väcka åtal för identitetsstöld endast om målsäganden anmäler brottet till åtal. I den föreslagna nya 9 b § om identitetsstöld skyddas framför allt okränkbarheten av identiteten för den person vars personuppgifter har använts. Om målsäganden inte upplever att hans eller hennes identitet har kränkts eller av någon annan orsak inte vill att saken ska behandlas och åtal väckas, är det inte motiverat att göra detta mot målsägandens vilja. Det är möjligt att målsäganden i förhållandevis ringa fall också kunde uppleva att handläggningen av åtalsärendet orsakar större olägenhet än själva brottet.

11 §. *Förverkandepåföljd.* Det föreslås att hänvisningen i paragrafen till avkodningssystem som avses i 8 a § ändras till en hänvisning till 8 b §. Förslaget hänför sig inte till genomförandet av direktivet. Det är fråga om en rättelse av ett skrivfel, eftersom det avkodningssystemsbrott som i dag finns i 8 b § tidigare fanns i 8 a §. I samband med den tidigare ändringen av paragrafnumreringen ändrades inte hänvisningen i 11 §.

13 §. *Definitioner.* I kapitlet föreslås en ny paragraf, som innehåller definitioner av informationssystem och data, i enlighet med vad som anges i detaljmotiveringen till artikel 2. I 34 och 35 kap. hänvisas det också till den föreslagna paragrafen såsom anges ovan.

I den föreslagna paragrafens 1 mom. tar man in definitionen av informationssystem i artikel 2 a i direktivet för de brotts del som motsvarar kriminaliseringsförpliktelserna i detta direktiv. Definitionen är öppen och teknikneutral, så att begreppet informationssystem inte heller i fråga om de bestämmelser i strafflagen som det hänvisas till ska begränsas till den definition som finns i direktivet, utan med informationssystem ska även avses det som i direktivet avses med informationssystem och data (datorbehandlingsbara uppgifter) i ett informationssystem. Genom detta uppfylls minimikraven i direktivet. Det är väsentligt att ta in definitionen i paragrafen, eftersom med informationssystem i direktivet avses också data i ett informationssystem. Eftersom det endast handlar om en öppen definition som föreskrivs för att säkerställa att förpliktelserna i direktivet kan genomföras, föreslås det i propositionen att den endast ska täcka de kriminaliseringar som är avsedda att täcka minimiförpliktelserna i direktivet.

Enligt det föreslagna 1 mom. avses vid tillämpningen av 3, 6, 7 a, 7 b och 8 § med informationssystem också i artikel 2 a i Europaparlamentets och rådets direktiv 2013/40/EU om angrepp mot informations-

system och om ersättande av rådets rambeslut 2005/222/RIF avsedda

1) apparater eller grupper av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program automatiskt behandlar data, samt

2) data 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.

För tydlighetens skull och eftersom definitionen av data i enlighet med vad som sägs ovan vid punkt a hör nära samman med definitionen av informationssystem, föreslås det i propositionen att i 2 mom. på motsvarande sätt som när det gäller begreppet informationssystem ska tas in en öppen definition, som motsvarar definitionen i artikel 2 b i direktivet och enligt vilken med data också avses sådana datorbehandlingsbara uppgifter som avses i direktivet i fråga om de brott som motsvarar kriminaliseringsförpliktelserna i direktivet. Genom detta uppfylls minimikraven i direktivet. Eftersom det endast handlar om en öppen definition som föreskrivs för att säkerställa att förpliktelserna i direktivet kan genomföras, föreslås det i propositionen att den endast ska täcka de kriminaliseringar som är avsedda att täcka minimiförpliktelserna i direktivet.

Enligt det föreslagna 2 mom. avses vid tillämpningen av 3, 7 a och 8 § med data också i artikel 2 b i nätbrottsdirektivet 2013/40/EU avsedda

1) framställningar av fakta, information eller begrepp i en form som lämpar sig för behandling i ett informationssystem, samt

2) program som lämpar sig för att få ett informationssystem att utföra en viss uppgift.

2.2 Tvångsmedelslagen

3 §. *Teleavlyssning och dess förutsättningar.* Eftersom grov dataskadegörelse avskiljs från grov skadegörelse och blir en särskild brottsrubricering, bör man göra en ändring som gäller detta i 12 punkten i tvångsmedelslagens 10 kap. 3 §, som gäller teleavlyssning och dess förutsättningar. I punkten nämns från förut grov skadegörelse. Bestämmelsen ändras så att tillstånd till teleavlyssning får ges också när en misstänkt är skäligen misstänkt för grov dataskadegörelse.

6 §. *Teleövervakning och dess förutsättningar.* Det föreslås att i paragrafen görs ändringar av teknisk natur som beror på de föreslagna ändringarna i strafflagen. Enligt 2 mom. 3 punkten i den gällande paragrafen är teleövervakning möjlig i fråga om olovligt brukande, skadegörelse, kränkning av kommunikationshemlighet eller dataintrång som riktat sig mot ett automatiskt databehandlingssystem och som begåtts med användning av en teleadress eller teleterminalutrustning. Det har varit behövligt att förteckna de brotten i 3 punkten, eftersom teleövervakning för deras del i dag inte kan användas i enlighet med 2 punkten, eftersom det i den punkten förutsätts ett maximistraff på två års fängelse.

Enligt momentets 2 punkt är teleövervakning möjlig i fråga om ett brott som begåtts med användning av en teleadress eller teleterminalutrustning och för vilket det föreskrivna strängaste straffet är fängelse i minst två år. Genom de ändringar i strafflagen som föreslås nu stiger maximistraffet för dataintrång och kränkning av kommunikationshemlighet till fängelse i två år, varvid 2 punkten kan tillämpas. Dataintrång och kränkning av kommunikationshemlighet kan därför strykas ur förteckningen i 3 punkten. Även skadegörelse som har begåtts genom det gärningssätt som anges i 3 punkten kan strykas ur förteckningen, eftersom s.k. ”dataskadegörelse” genom de ändringar i strafflagen som föreslås i propositionen avskiljs från kriminaliseringen av skadegörelse i 35 kap. 1 § i strafflagen och blir en självständig kriminalisering som gäller dataskadegörelse i 35 kap. 3 a § i strafflagen. På motsvarande föreslås det att bestämmelserna om skadegörelse i 1 § 2 och 3 mom. upphävs. Maximistraffet för den nya gärningen dataskadegörelse ska vara två års fängelse, vilket betyder att 10 kap. 6 § 2 mom. 2 punkten i tvångsmedelslagen kan tillämpas.

2.3 Polislagen

8 §. *Teleövervakning och dess förutsättningar.* I paragrafen görs motsvarande tekniska ändringar som i tvångsmedelslagen, be-

roende på de föreslagna ändringarna i strafflagen. Enligt 2 mom. 3 punkten i den gällande paragrafen är teleövervakning möjlig i fråga om olovligt brukande, skadegörelse, kränkning av kommunikationshemlighet eller dataintrång som riktar sig mot ett automatiskt databehandlingssystem och som begåtts med användning av en teleadress eller teleterminalutrustning. Det har varit behövligt att förteckna de brotten i 3 punkten, eftersom teleövervakning för deras del i dag inte kan användas i enlighet med 2 punkten, eftersom det i den punkten förutsätts ett maximistraff på två års fängelse.

Enligt momentets 2 punkt är teleövervakning möjlig i fråga om ett brott som begåtts med användning av en teleadress eller teleterminalutrustning och för vilket det föreskrivna strängaste straffet är fängelse i minst två år. Genom de ändringar i strafflagen som föreslås nu stiger maximistraffet för dataintrång och kränkning av kommunikationshemlighet till fängelse i två år, varvid 2 punkten kan tillämpas. Dataintrång och kränkning av kommunikationshemlighet kan därför strykas ur förteckningen i 3 punkten. Även skadegörelse som har begåtts genom det gärningssätt som avses i 3 punkten kan strykas ur förteckningen, eftersom s.k. ”dataskadegörelse” genom de ändringar i strafflagen som föreslås i propositionen avskiljs från kriminaliseringen av skadegörelse i 35 kap. 1 § i strafflagen och blir en självständig kriminalisering som gäller dataskadegörelse i 35 kap. 3 a § i strafflagen. På motsvarande föreslås det att bestämmelserna om skadegörelse i 1 § 2 och 3 mom. upphävs. Maximistraffet för den nya gärningen dataskadegörelse ska vara två års fängelse, vilket betyder att 5 kap. 8 § 2 mom. 2 punkten i polislagen kan tillämpas.

2.4 Militära rättegångslagen

Enligt 2 § 2 mom. i militära rättegångslagen (326/1983) handläggs såsom militärt rättegångsärende även åtal mot krigsman för en gärning för vilken straff bestäms i 21 kap. 1—3 eller 5—14 §, 25 kap. 7 eller 8 §, 28, 31—33 eller 35 kap., 36 kap. 1—3 §, 37 kap. 8–10 §, 38 kap. 1—7, 7 a, 7 b, 8 eller 8 a § eller 40 kap. 1—3 eller 5 § i strafflagen (39/1889). Detta förutsätter att gärningen har riktat sig mot försvarsmakten eller mot någon annan krigsman. Såsom militärt rättegångsärende handläggs också åtal för en gärning för vilken straff bestäms i 118 § i värnpliktslagen (1438/2007). Identitetsstöld som i propositionen föreslås i 38 kap. 9 b § i strafflagen kan bli brottsrubricering vid utredningen i samband med t.ex. tjänstgöringsbrott eller egendoms- eller förfalskningsbrott. På det sätt som konstateras i propositionen utgör identitetsstöld sannolikt ofta en del av något annat straffbart beteende. För resursanvändningens del kan det då inte anses motiverat att försvarsmakten tvingas överföra förundersökningen till polisen när det gäller brottsrubriceringen identitetsstöld. Av den orsak som anges ovan tas den föreslagna kriminaliseringen av identitetsstöld in i förteckningen i 2 § 2 mom. i militära rättegångslagen.

3 Ikraftträdande

Lagarna föreslås träda i kraft den 4 september 2015, då direktivet ska genomföras.

4 Förhållande till grundlagen samt lagstiftningsordning

Enligt grundlagens 10 § 1 mom. är vars och ens privatliv, heder och hemfrid tryggade. Flera av de kriminaliseringar av nätbrott som avses i propositionen är av betydelse med tanke på bestämmelsen och utvidgar indirekt det skydd för privatlivet som föreskrivs i det momentet.

Enligt grundlagens 10 § 2 mom. är brev- och telefonhemligheten samt hemligheten i fråga om andra förtroliga meddelanden okränkbar. Bestämmelsen är utformad så att den är neutral när det gäller medel och teknik, och genom bestämmelsen tryggas allmänt hemligheten i fråga om all slags förtrolig kommunikation (RP 309/1993 rd, s. 57). De ändringar som i propositionen föreslås i fråga om kränkning av kommunikationshemlighet enligt strafflagens 38 kap. 3 § utvidgar skyddet för förtrolig kommunikation.

Enligt grundlagens 10 § 3 mom. kan det genom lag bestämmas om sådana begränsningar i meddelandehemligheten som är nödvändiga vid utredning av brott som även-

tyrar individens eller samhällets säkerhet eller hemfriden. Den föreslagna ändringen i 10 kap. 3 § 2 mom. 12 punkten i tvångsmedelslagen som gäller teleavlyssning innebär inte någon ändring i sak. Ändringen behövs för att grov dataskadegörelse blir ett självständigt brott och avskiljs från den gällande bestämmelsen om grov skadegörelse, för vars del teleavlyssning redan är möjlig enligt den gällande lagen. Teletvångsmedlen har fått allt större betydelse vid utredningen av allvarliga brott som har begåtts i informationsnät, och grov dataskadegörelse kan anses vara ett brott som äventyrar individens eller samhällets säkerhet på samma sätt som grov skadegörelse. Enligt grundlagsutskottet (GrUU 36/2002 rd, s. 4) är det av central betydelse att möjligheten till teleavlyssning med tanke på kriteriet för en nödvändig begränsning i grundlagens 10 § 3 mom. endast är bunden till grova brott. Grov dataskadegörelse kan anses som ett sådant grovt brott. Maximistraffet för grov dataskadegörelse är fem års fängelse, och brottet är således till sin allvarlighet på samma nivå som eller bestraffas strängare än många andra brott vid vars utredning teleavlyssning får användas i dag enligt tvångsmedelslagens 10 kap. 3 § 2 mom.

De ändringar i anslutning till teleövervakning som föreslås i 10 kap. 6 § i tvångsmedelslagen och 5 kap. 8 § i polislagen är inte ändringar i sak. På grund av de i propositionen föreslagna ändringarna i strafflagen och höjningen av straffnivåerna är det inte längre behövligt att uttryckligen förteckna skadegörelse, kränkning av kommunikationshemlighet eller dataintrång som riktar sig mot ett automatiskt databehandlingssystem och som begåtts med användning av en teleadress eller teleterminalutrustning som brott som berättigar till teleövervakning i de paragraferna.

De föreslagna straffbestämmelserna om informationssystem och informationsnät, särskilt grovt störande av post- och teletrafik enligt 6 § och grov systemstörning enligt 7 b § i strafflagens 38 kap., skyddar indirekt även den i grundlagens 12 § tryggade yttrandefriheten. Enligt bestämmelsen hör till yttrandefriheten rätten att framföra, sprida och ta emot information, åsikter och andra meddelanden utan att någon i förväg hindrar detta. På grund av de tekniska lösningarna vid kommunikation på nätet är det också behövligt att med hjälp av lagstiftning främja en friktionsfri funktion i kommunikationssystemen (GrUU 9/2004 rd).

Också den föreslagna nya kriminaliseringen av identitetsstöld i 38 kap. 9 b § i strafflagen är av relevans med tanke på den i grundlagens 12 § tryggade yttrandefriheten. Straffbestämmelsen begränsar i obetydlig mån yttrandefriheten, men genom kriminaliseringen skyddas samtidigt den i grundlagens 10 § tryggade rätten till privatlivet. Rätten till personlig identitet omfattas av skyddet för privatlivet i grundlagen (se GrUU 25/2006 rd, s. 2, GrUU 16/2006 rd, s. 3, GrUU 59/2002 rd, s. 3). Den föreslagna kriminaliseringen är proportionell, den riktar sig inte mot kärnan i yttrandefriheten och innebär inte att man i förväg ingriper i utövandet av yttrandefriheten.

Regeringen anser att lagförslagen kan godkännas i vanlig lagstiftningsordning.

Med stöd av vad som anförts ovan föreläggs Riksdagen följande lagförslag:

Lagförslag

1.

Lag

om ändring av strafflagen

I enlighet med riksdagens beslut

upphävs i strafflagen (39/1889) 35 kap. 1 § 2 och 3 mom., sådana de lyder, 1 § 2 mom. i lag 769/1990 och 1 § 3 mom. i lag 540/2007,

ändras 34 kap. 9 a §, 35 kap. 2 och 6—8 § och 38 kap. 3 §, 6 § 1 mom. sista stycket samt 7 a, 7 b, 8, 8 a och 11 §,

sådana de lyder, 34 kap. 9 a §, 35 kap. 8 § och 38 kap. 7 a, 7 b och 8 a § i lag 540/2007, 35 kap. 2 § i lagarna 769/1990, 17/2003 och 540/2007, 35 kap. 6 § i lag 441/2011, 35 kap 7 § i lag 769/1990, 38 kap. 3 § i lag 531/2000, 38 kap. 6 § 1 mom. sista stycket och 8 § i lag 578/1995 och 38 kap. 11 § i lag 1118/2001, samt

fogas till 34 kap. en ny 14 §, till 35 kap. nya 3 a—3 c och 9 §, till 38 kap. 6 § 1 mom., sådant det lyder i lag 578/1995, nya 3—6 punkter, till 38 kap. en ny 9 b §, till 38 kap. 10 §, sådan den lyder i lag 441/2011, ett nytt 4 mom. och till 38 kap. en ny 13 § som följer:

34 kap.

Om allmänfarliga brott

9 a §

Orsakande av fara för informationsbehandling

Den som i syfte att orsaka olägenhet eller skada för informationsbehandling eller för ett informations- eller kommunikationssystems funktion eller säkerhet

1) för in i landet, anskaffar i syfte att använda, tillverkar, säljer eller annars sprider eller ställer till förfogande

a) sådana apparater, datorprogram eller programinstruktioner som har skapats eller anpassats för att äventyra eller skada informationsbehandling eller ett informations- eller kommunikationssystems funktion eller för att bryta eller avkoda det tekniska skyddet vid elektronisk kommunikation eller skyddet för ett informationssystem, eller

b) andra personers lösenord eller åtkomstkoder eller andra motsvarande uppgifter om informationssystem, eller

2) sprider eller ställer till förfogande anvisningar för tillverkning av sådana datorprogram eller programinstruktioner som avses i 1 punkten,

ska, om inte strängare eller lika strängt straff föreskrivs för gärningen någon annanstans i lag, för *orsakande av fara för informationsbehandling* dömas till böter eller fängelse i högst två år.

14 §

Definitioner

Vad som i 38 kap. 13 § 1 mom. föreskrivs om definitionen av informationssystem, tillämpas också på 9 a och 9 b §.

35 kap.

Om skadegörelse

2 §

Grov skadegörelse

Om skadegörelsen vållar

1) synnerligen stor ekonomisk skada,

2) synnerligen kännbar skada för den drabbade, med beaktande av dennes förhållanden, eller

3) avsevärd skada på egendom som är synnerligen värdefull i historiskt eller kulturellt hänseende,

och skadegörelsen även bedömd som en helhet är grov, ska gärningsmannen för *grov skadegörelse* dömas till fängelse i minst fyra månader och högst fyra år.

Försök är straffbart.

3 a §

Dataskadegörelse

Den som i syfte att skada någon annan obehörigen förstör, försämrar, döljer, skadar, ändrar, gör det omöjligt att komma åt eller hemlighåller information som har upptagits på ett datamedium eller någon annan upptagning eller data i ett informationssystem, ska för *dataskadegörelse* dömas till böter eller fängelse i högst två år.

Försök är straffbart.

3 b §

Grov dataskadegörelse

Om vid dataskadegörelse

1) vållas synnerligen kännbar olägenhet eller ekonomisk skada,

2) brottet begås som ett led i en i 17 kap. 1 a § 4 mom. avsedd organiserad kriminell sammanslutnings verksamhet,

3) brottet begås som ett led i verksamhet där ett betydande antal informationssystem har påverkats genom användning av sådana apparater, datorprogram eller programinstruktioner som avses i 34 kap. 9 a § 1 punkten underpunkt a eller sådana lösenord, åtkomstkoder eller andra motsvarande uppgifter som avses i 9 a § 1 punkten underpunkt b, eller

4) brottet riktar sig mot ett informationssystem vars skadande äventyrar energiförsörjningen, den allmänna hälso- och sjukvården, försvaret, rättsvården eller någon annan med dessa jämförbar viktig samhällsfunktion,

och dataskadegörelsen även bedömd som en helhet är grov, ska gärningsmannen för *grov dataskadegörelse* dömas till fängelse i minst fyra månader och högst fem år.

Försök är straffbart.

3 c §

Lindrig dataskadegörelse

Om dataskadegörelsen, med beaktande av att skadan är liten eller andra omständigheter vid brottet, bedömd som en helhet är ringa, ska gärningsmannen för *lindrig dataskadegörelse* dömas till böter.

6 §

Åtalsrätt

Om enbart enskild egendom är föremål för ett brott som avses i 1, 3, 3 a eller 3 c §, får åklagaren väcka åtal endast om målsäganden anmäler brottet till åtal.

7 §

Åtgärdseftergift

Vid skadegörelse, dataskadegörelse, lindrig skadegörelse och lindrig dataskadegörelse får eftergift ske i fråga om anmälan, åtal eller straff, om gärningsmannen har ersatt skadan och skadestånd prövas vara en tillräcklig påföljd.

8 §

Straffansvar för juridiska personer

På dataskadegörelse och grov dataskadegörelse tillämpas vad som föreskrivs om straffansvar för juridiska personer.

9 §

Definitioner

Vad som i 38 kap. 13 § 1 mom. föreskrivs om definitionen av informationssystem, tillämpas också på 3 a och 3 b §.

Vad som i 38 kap. 13 § 2 mom. föreskrivs om definitionen av data, tillämpas också på 3 a §.

38 kap.

Om informations- och kommunikationsbrott

3 §

Kränkning av kommunikationshemlighet

Den som obehörigen

1) öppnar ett brev eller ett annat tillslutet meddelande som är adresserat till någon annan eller genom att bryta ett säkerhetsarrangemang skaffar uppgifter om ett meddelande som har upptagits elektroniskt eller med någon annan sådan teknisk metod och som är skyddat mot utomstående, eller

2) skaffar uppgifter om innehållet i samtal, telegram, text-, bild- eller dataöverföring eller något annat motsvarande telemeddelande som förmedlas genom telenät eller informationssystem eller om avsändande eller mottagande av ett sådant meddelande,

ska för *kränkning av kommunikationshemlighet* dömas till böter eller fängelse i högst två år.

Försök är straffbart.

6 §

Grovt störande av post- och teletrafik

Om vid störande av post- och teletrafik

— — — — — — — — — — — — — — —

3) brottet begås som ett led i verksamhet där ett betydande antal informationssystem har påverkats genom användning av sådana apparater, datorprogram eller programinstruktioner som avses i 34 kap. 9 a § 1 punkten underpunkt a eller sådana lösenord, åtkomstkoder eller andra motsvarande uppgifter som avses i 9 a § 1 punkten underpunkt b,

4) brottet begås som ett led i en i 17 kap. 1 a § 4 mom. avsedd organiserad kriminell sammanslutnings verksamhet,

5) genom brottet vållas synnerligen kännbar olägenhet eller ekonomisk skada, eller

6) brottet riktar sig mot en apparat, ett informationssystem eller kommunikation vars skadande äventyrar energiförsörjningen, den allmänna hälso- och sjukvården, försvaret, rättsvården eller någon annan med dessa jämförbar viktig samhällsfunktion,

och störandet av post- och teletrafiken även bedömt som en helhet är grovt, ska gärningsmannen för *grovt störande av post- och teletrafik* dömas till fängelse i minst fyra månader och högst fem år.

— — — — — — — — — — — — — — —

7 a §

Systemstörning

Den som i syfte att orsaka någon annan olägenhet eller ekonomisk skada genom att mata in, överföra, skada, ändra eller undertrycka data eller på något annat med dessa jämförbart sätt obehörigen hindrar ett informationssystems funktion eller orsakar allvarliga störningar i det, ska för *systemstörning* dömas till böter eller fängelse i högst två år.

Försök är straffbart.

7 b §

Grov systemstörning

Om vid systemstörning

1) vållas synnerligen kännbar olägenhet eller ekonomisk skada,

2) brottet begås särskilt planmässigt,

3) brottet begås som ett led i verksamhet där ett betydande antal informationssystem har påverkats genom användning av sådana apparater, datorprogram eller programinstruktioner som avses i 34 kap. 9 a § 1 punkten underpunkt a eller sådana lösenord, åtkomstkoder eller andra motsvarande uppgifter som avses i 9 a § 1 punkten underpunkt b,

4) brottet begås som ett led i en i 17 kap. 1 a § 4 mom. avsedd organiserad kriminell sammanslutnings verksamhet, eller

5) brottet riktar sig mot ett informationssystem vars skadande äventyrar energiförsörjningen, den allmänna hälso- och sjukvården, försvaret, rättsvården eller någon annan med dessa jämförbar viktig samhällsfunktion,

och systemstörningen även bedömd som en helhet är grov, ska gärningsmannen för *grov systemstörning* dömas till fängelse i minst fyra månader och högst fem år.

Försök är straffbart.

8 §

Dataintrång

Den som genom att göra bruk av en användaridentifikation som han eller hon inte har rätt till eller genom att annars bryta säkerhetsarrangemang obehörigen tränger in i ett informationssystem där information eller data behandlas, lagras eller överförs elektroniskt eller med någon annan sådan teknisk metod eller i en särskilt skyddad del av ett sådant system, ska för *dataintrång* dömas till böter eller fängelse i högst två år.

För dataintrång döms också den som utan att tränga in i ett informationssystem eller en del av ett sådant

1) med hjälp av tekniska specialanordningar, eller

2) annars med tekniska metoder genom att ta sig förbi säkerhetsarrangemangen, utnyttja informationssystemets sårbarhet eller använda annars uppenbart svikliga medel

obehörigen tar reda på information eller data som finns i ett sådant informationssystem som avses i 1 mom.

Försök är straffbart.

Denna paragraf tillämpas endast på gärningar för vilka inte föreskrivs strängare eller lika strängt straff på något annat ställe i lag.

8 a §

Grovt dataintrång

Om dataintrång görs

1) som ett led i en i 17 kap. 1 a § 4 mom. avsedd organiserad kriminell sammanslutnings verksamhet, eller

2) särskilt planmässigt,

och dataintrånget även bedömt som en helhet är grovt, ska gärningsmannen för *grovt dataintrång* dömas till böter eller fängelse i högst tre år.

Försök är straffbart.

9 b §

Identitetsstöld

Den som i syfte att vilseleda en tredje part obehörigen använder någon annans personuppgifter eller identifieringsuppgifter eller andra motsvarande uppgifter som identifierar personen, och därmed orsakar ekonomisk skada eller mer än ringa olägenhet för den som uppgifterna gäller, ska för *identitetsstöld* dömas till böter.

10 §

Åtalsrätt

— — — — — — — — — — — — — — —

Åklagaren får väcka åtal för identitetsstöld endast om målsäganden anmäler brottet till åtal.

11 §

Förverkandepåföljd

Avkodningssystem som avses i 8 b § ska dömas förverkade till staten.

13 §

Definitioner

Vid tillämpningen av 3, 6, 7 a, 7 b och 8 § avses med informationssystem också i artikel 2 a i Europaparlamentets och rådets direktiv 2013/40/EU om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF, nedan *nätbrottsdirektivet*, avsedda

1) apparater eller grupper av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program automatiskt behandlar data, samt

2) data 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.

Vid tillämpningen av 3, 7 a och 8 § avses med data också i artikel 2 b i nätbrottsdirektivet avsedda

1) framställningar av fakta, information eller begrepp i en form som lämpar sig för behandling i ett informationssystem, samt
2) program som lämpar sig för att få ett informationssystem att utföra en viss uppgift.

Denna lag träder i kraft den 20 .

2.

Lag

om ändring av 10 kap. 3 och 6 § i tvångsmedelslagen

I enlighet med riksdagens beslut
ändras i tvångsmedelslagen (806/2011) 10 kap. 3 § 2 mom. 12 punkten och 6 § 2 mom., sådana de lyder i lag 1146/2013, som följer:

10 kap.

Hemliga tvångsmedel

3 §

Teleavlyssning och dess förutsättningar

— — — — — — — — — — — — — — —

Förundersökningsmyndigheten kan ges tillstånd att rikta teleavlyssning mot en teleadress eller teleterminalutrustning som en misstänkt innehar eller annars kan antas använda, om den misstänkte är skäligen misstänkt för

— — — — — — — — — — — — — — —

12) grov skadegörelse eller grov dataskadegörelse,

— — — — — — — — — — — — — — —

6 §

Teleövervakning och dess förutsättningar

— — — — — — — — — — — — — — —

Förundersökningsmyndigheten kan ges tillstånd att rikta teleövervakning mot en teleadress eller teleterminalutrustning som en misstänkt innehar eller annars kan antas använda, om den misstänkte är skäligen misstänkt för

1) ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst fyra år,
2) ett brott som begåtts med användning av en teleadress eller teleterminalutrustning och för vilket det föreskrivna strängaste straffet är fängelse i minst två år,
3) olovligt brukande som riktat sig mot ett automatiskt databehandlingssystem och som begåtts med användning av en teleadress eller teleterminalutrustning
4) utnyttjande av person som är föremål för sexhandel, lockande av barn i sexuella syften eller koppleri,
5) narkotikabrott,
6) förberedelse till brott som begås i terroristiskt syfte,
7) grovt tullredovisningsbrott,
8) grovt döljande av olagligt byte,
9) förberedelse till tagande av gisslan, eller
10) förberedelse till grovt rån.

— — — — — — — — — — — — — — —

Denna lag träder i kraft den 20 .

3.

Lag

om ändring av 5 kap. 8 § i polislagen

I enlighet med riksdagens beslut
ändras i polislagen (872/2011) 5 kap. 8 § 2 mom., sådant det lyder i lag 1168/2013, som följer:

5 kap.

Hemliga metoder för inhämtande av information

8 §

Teleövervakning och dess förutsättningar

— — — — — — — — — — — — — — —

För att förhindra brott kan polisen ges tillstånd att rikta teleövervakning mot en teleadress eller teleterminalutrustning som innehas eller sannolikt används av en person, om personen på grund av sina yttranden, hotelser eller uppträdande eller annars med fog kan antas göra sig skyldig till

1) ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst fyra år,

2) ett brott som begåtts med användning av en teleadress eller teleterminalutrustning och för vilket det föreskrivna strängaste straffet är fängelse i minst två år,

3) olovligt brukande som riktar sig mot ett automatiskt databehandlingssystem och som begåtts med användning av en teleadress eller teleterminalutrustning,

4) utnyttjande av en person som är föremål för sexhandel, lockande av barn i sexuella syften eller koppleri,

5) narkotikabrott,

6) förberedelse till brott som begås i terroristiskt syfte, eller

7) grovt tullredovisningsbrott.

— — — — — — — — — — — — — — —

Denna lag träder i kraft den 20 .

4.

Lag

om ändring av 2 § i militära rättegångslagen

I enlighet med riksdagens beslut

ändras i militära rättegångslagen (326/1983) 2 § 2 mom., sådant det lyder i lag 1442/2007, som följer:

2 §

— — — — — — — — — — — — — — — —

Såsom militärt rättegångsärende handläggs även åtal mot krigsman för en gärning för vilken straff bestäms i 21 kap. 1—3 eller 5—14 §, 25 kap. 7 eller 8 §, 28, 31—33 eller 35 kap., 36 kap. 1—3 §, 37 kap. 8—10 §, 38 kap. 1—7, 7 a, 7 b, 8, 8 a eller 9 b § eller 40 kap. 1—3 eller 5 § i strafflagen (39/1889). Detta förutsätter att gärningen har riktat sig mot försvarsmakten eller mot någon annan krigsman. Såsom militärt rättegångsärende handläggs också åtal för en gärning för vilken straff bestäms i 118 § i värnpliktslagen (1438/2007).

— — — — — — — — — — — — — — — —

Denna lag träder i kraft den 20 .

Helsingfors den 13 november 2014

Statsminister

ALEXANDER STUBB

Justitieminister *Anna-Maja Henriksson*

Bilaga
Parallelltexter

1.

Lag

om ändring av strafflagen

I enlighet med riksdagens beslut

upphävs i strafflagen (39/1889) 35 kap. 1 § 2 och 3 mom., sådana de lyder, 1 § 2 mom. i lag 769/1990 och 1 § 3 mom. i lag 540/2007,

ändras 34 kap. 9 a §, 35 kap. 2 och 6—8 § och 38 kap. 3 §, 6 § 1 mom. sista stycket samt 7 a, 7 b, 8, 8 a och 11 §,

sådana de lyder, 34 kap. 9 a §, 35 kap. 8 § och 38 kap. 7 a, 7 b och 8 a § i lag 540/2007, 35 kap. 2 § i lagarna 769/1990, 17/2003 och 540/2007, 35 kap. 6 § i lag 441/2011, 35 kap 7 § i lag 769/1990, 38 kap. 3 § i lag 531/2000, 38 kap. 6 § 1 mom. sista stycket och 8 § i lag 578/1995 och 38 kap. 11 § i lag 1118/2001, samt

fogas till 34 kap. en ny 14 §, till 35 kap. nya 3 a—3 c och 9 §, till 38 kap. 6 § 1 mom., sådant det lyder i lag 578/1995, nya 3—6 punkter, till 38 kap. en ny 9 b §, till 38 kap. 10 §, sådan den lyder i lag 441/2011, ett nytt 4 mom. och till 38 kap. en ny 13 § som följer:

Gällande lydelse	*Föreslagen lydelse*
34 kap.	
Om allmänfarliga brott	
9 a §	9 a §
Orsakande av fara för informationsbehandling	*Orsakande av fara för informationsbehandling*
Den som för att orsaka olägenhet eller skada för informationsbehandling eller för ett informations- eller kommunikationssystems funktion eller säkerhet	Den som i syfte att orsaka olägenhet eller skada för informationsbehandling eller för ett informations- eller kommunikationssystems funktion eller säkerhet
1) för in i landet, tillverkar, säljer eller annars sprider eller ställer till förfogande	1) för in i landet, *anskaffar i syfte att använda*, tillverkar, säljer eller annars sprider eller ställer till förfogande
a) sådana apparater, datorprogram eller programinstruktioner som har skapats eller anpassats för att äventyra eller skada informationsbehandling eller ett informations- eller kommunikationssystems funktion eller för att bryta eller avkoda det tekniska skyddet vid elektronisk kommunikation eller skyddet för ett informationssystem, eller	a) sådana apparater, datorprogram eller programinstruktioner som har skapats eller anpassats för att äventyra eller skada informationsbehandling eller ett informations- eller kommunikationssystems funktion eller för att bryta eller avkoda det tekniska skyddet vid elektronisk kommunikation eller skyddet för ett informationssystem, eller
b) andra personers lösenord eller åtkomstkoder eller andra motsvarande uppgifter om	b) andra personers lösenord eller åtkomstkoder eller andra motsvarande uppgifter om

Gällande lydelse	*Föreslagen lydelse*
informationssystem, eller 2) sprider eller ställer till förfogande anvisningar för tillverkning av sådana datorprogram eller programinstruktioner som avses i 1 punkten, skall, om inte strängare eller lika strängt straff föreskrivs för gärningen någon annanstans i lag, för *orsakande av fara för informationsbehandling* dömas till böter eller fängelse i högst två år.	informationssystem, eller 2) sprider eller ställer till förfogande anvisningar för tillverkning av sådana datorprogram eller programinstruktioner som avses i 1 punkten, ska, om inte strängare eller lika strängt straff föreskrivs för gärningen någon annanstans i lag, för *orsakande av fara för informationsbehandling* dömas till böter eller fängelse i högst två år.
(ny)	14 § *Definitioner* *Vad som i 38 kap. 13 § 1 mom. föreskrivs om definitionen av informationssystem, tillämpas också på 9 a och 9 b §.*

35 kap.

Om skadegörelse

1 §	1 §
Skadegörelse	*Skadegörelse*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
För skadegörelse döms också den som för att skada någon orättmätigt förstör, skadar, döljer eller hemlighåller information som har upptagits på ett datamedium eller någon annan upptagning.	(2 mom. upphävs)
Försök till skadegörelse enligt 2 mom. är straffbart.	(3 mom. upphävs)
2 §	2 §
Grov skadegörelse	*Grov skadegörelse*
Om *1)* skadegörelsen vållar a) synnerligen stor ekonomisk skada, b) synnerligen kännbar skada för den drabbade, med beaktande av dennes förhållanden, c) avsevärd skada på egendom som är synnerligen värdefull i historiskt eller kulturellt hänseende, *eller* *2) skadegörelse enligt 1 § 2 mom. begås som ett led i en i 17 kap. 1 a § 4 mom. avsedd*	Om skadegörelsen vållar *1)* synnerligen stor ekonomisk skada, *2)* synnerligen kännbar skada för den drabbade, med beaktande av dennes förhållanden, *eller* *3)* avsevärd skada på egendom som är synnerligen värdefull i historiskt eller kulturellt hänseende,

Gällande lydelse	*Föreslagen lydelse*
organiserad kriminell sammanslutnings verksamhet,	
och skadegörelsen även bedömd som en helhet är grov, skall gärningsmannen för *grov skadegörelse* dömas till fängelse i minst fyra månader och högst fyra år.	och skadegörelsen även bedömd som en helhet är grov, ska gärningsmannen för *grov skadegörelse* dömas till fängelse i minst fyra månader och högst fyra år.
Försök är straffbart.	Försök är straffbart.
(ny)	3 a §
	Dataskadegörelse
	Den som i syfte att skada någon annan obehörigen förstör, försämrar, döljer, skadar, ändrar, gör det omöjligt att komma åt eller hemlighåller information som har upptagits på ett datamedium eller någon annan upptagning eller data i ett informationssystem, ska för ***dataskadegörelse*** *dömas till böter eller fängelse i högst två år.*
	Försök är straffbart.
(ny)	3 b §
	Grov dataskadegörelse
	Om vid dataskadegörelse
	1) vållas synnerligen kännbar olägenhet eller ekonomisk skada,
	2) brottet begås som ett led i en i 17 kap. 1 a § 4 mom. avsedd organiserad kriminell sammanslutnings verksamhet,
	3) brottet begås som ett led i verksamhet där ett betydande antal informationssystem har påverkats genom användning av sådana apparater, datorprogram eller programinstruktioner som avses i 34 kap. 9 a § 1 punkten underpunkt a eller sådana lösenord, åtkomstkoder eller andra motsvarande uppgifter som avses i 9 a § 1 punkten underpunkt b, eller
	4) brottet riktar sig mot ett informationssystem vars skadande äventyrar energiförsörjningen, den allmänna hälso- och sjukvården, försvaret, rättsvården eller någon annan med dessa jämförbar viktig samhällsfunktion,
	och dataskadegörelsen även bedömd som en helhet är grov, ska gärningsmannen för ***grov dataskadegörelse*** *dömas till fängelse i minst fyra månader och högst fem år.*

Gällande lydelse	*Föreslagen lydelse*
	Försök är straffbart.
(ny)	3 c §
	Lindrig dataskadegörelse
	Om dataskadegörelsen, med beaktande av att skadan är liten eller andra omständigheter vid brottet, bedömd som en helhet är ringa, ska gärningsmannen för ***lindrig dataskadegörelse*** *dömas till böter.*
6 §	6 §
Åtalsrätt	*Åtalsrätt*
Är enbart enskild egendom föremål för ett brott som avses i 1 eller 3 §, får åklagaren väcka åtal endast om målsäganden anmäler brottet till åtal.	Om enbart enskild egendom är föremål för ett brott som avses i 1, 3, *3 a eller 3 c* §, får åklagaren väcka åtal endast om målsäganden anmäler brottet till åtal.
7 §	7 §
Åtgärdseftergift	*Åtgärdseftergift*
Vid skadegörelse och lindrig skadegörelse får eftergift ske i fråga om anmälan, åtal eller straff, om gärningsmannen har ersatt skadan och skadestånd prövas vara en tillräcklig påföljd.	Vid skadegörelse, *dataskadegörelse*, lindrig skadegörelse och *lindrig dataskadegörelse* får eftergift ske i fråga om anmälan, åtal eller straff, om gärningsmannen har ersatt skadan och skadestånd prövas vara en tillräcklig påföljd.
8 §	8 §
Straffansvar för juridiska personer	*Straffansvar för juridiska personer*
På skadegörelse som avses i 1 § 2 mom. samt på grov skadegörelse som avses i 2 §, när den har skett på det sätt som avses i 1 § 2 mom., tillämpas vad som föreskrivs om straffansvar för juridiska personer.	På *dataskadegörelse* och *grov dataskadegörelse* tillämpas vad som föreskrivs om straffansvar för juridiska personer.
(ny)	9 §
	Definitioner
	Vad som i 38 kap. 13 § 1 mom. föreskrivs

Gällande lydelse	*Föreslagen lydelse*
	om definitionen av informationssystem, tillämpas också på 3 a och 3 b §. *Vad som i 38 kap. 13 § 2 mom. föreskrivs om definitionen av data, tillämpas också på 3 a §.*
38 kap.	
Om informations- och kommunikationsbrott	
3 §	3 §
Kränkning av kommunikationshemlighet	*Kränkning av kommunikationshemlighet*
Den som obehörigen 1) öppnar ett brev eller ett annat tillslutet meddelande som är adresserat till någon annan eller genom att bryta ett säkerhetsarrangemang skaffar uppgifter om ett meddelande som har upptagits elektroniskt eller med någon annan sådan teknisk metod och som är skyddat mot utomstående, eller 2) skaffar uppgifter om innehållet i samtal, telegram, text-, bild-, eller dataöverföring eller något annat motsvarande telemeddelande som förmedlas genom telenät eller om avsändande eller mottagande av ett sådant meddelande, skall för *kränkning av kommunikationshemlighet* dömas till böter eller fängelse i högst ett år. Försök är straffbart.	Den som obehörigen 1) öppnar ett brev eller ett annat tillslutet meddelande som är adresserat till någon annan eller genom att bryta ett säkerhetsarrangemang skaffar uppgifter om ett meddelande som har upptagits elektroniskt eller med någon annan sådan teknisk metod och som är skyddat mot utomstående, eller 2) skaffar uppgifter om innehållet i samtal, telegram, text-, bild- eller dataöverföring eller något annat motsvarande telemeddelande som förmedlas genom telenät *eller informationssystem* eller om avsändande eller mottagande av ett sådant meddelande, *ska* för *kränkning av kommunikationshemlighet* dömas till böter eller fängelse i högst två år. Försök är straffbart.
6 §	6 §
Grovt störande av post- och teletrafik	*Grovt störande av post- och teletrafik*
Om vid störande av post- och teletrafik	Om vid störande av post- och teletrafik
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
(nya 3–6 punkter)	*3) brottet begås som ett led i verksamhet där ett betydande antal informationssystem har påverkats genom användning av sådana apparater, datorprogram eller programinstruktioner som avses i 34 kap. 9 a § 1 punkten underpunkt a eller sådana lösenord, åtkomstkoder eller andra motsvarande uppgifter som avses i 9 a § 1 punkten underpunkt b,* *4) brottet begås som ett led i en i 17 kap. 1 a § 4 mom. avsedd organiserad kriminell sammanslutnings verksamhet,*

Gällande lydelse	*Föreslagen lydelse*
	5) genom brottet vållas synnerligen kännbar olägenhet eller ekonomisk skada, eller
	6) brottet riktar sig mot en apparat, ett informationssystem eller kommunikation vars skadande äventyrar energiförsörjningen, den allmänna hälso- och sjukvården, försvaret, rättsvården eller någon annan med dessa jämförbar viktig samhällsfunktion,
och störandet av post- och teletrafiken även bedömt som en helhet är grovt, skall gärningsmannen för *grovt störande av post- och teletrafik* dömas till fängelse i minst fyra månader och högst fyra år.	och störandet av post- och teletrafiken även bedömt som en helhet är grovt, ska gärningsmannen för *grovt störande av post- och teletrafik* dömas till fängelse i minst fyra månader och högst *fem* år.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
7 a §	7 a §
Systemstörning	*Systemstörning*
Den som i syfte att orsaka någon annan olägenhet eller ekonomisk skada genom att mata in, överföra, skada, ändra eller undertrycka data eller på något annat med dessa jämförbart sätt obehörigen hindrar ett informationssystems funktion eller orsakar allvarliga störningar i det skall, *om inte strängare eller lika strängt straff föreskrivs för gärningen någon annanstans i lag*, för *systemstörning* dömas till böter eller fängelse i högst två år.	Den som i syfte att orsaka någon annan olägenhet eller ekonomisk skada genom att mata in, överföra, skada, ändra eller undertrycka data eller på något annat med dessa jämförbart sätt obehörigen hindrar ett informationssystems funktion eller orsakar allvarliga störningar i det, *ska* för *systemstörning* dömas till böter eller fängelse i högst två år.
Försök är straffbart.	Försök är straffbart.
7 b §	7 b §
Grov systemstörning	*Grov systemstörning*
Om vid systemstörning	Om vid systemstörning
1) vållas synnerligen kännbar olägenhet eller ekonomisk skada, eller	1) vållas synnerligen kännbar olägenhet eller ekonomisk skada,
2) brottet begås särskilt planmässigt,	2) brottet begås särskilt planmässigt,
(nya 3—5 punkter)	*3) brottet begås som ett led i verksamhet där ett betydande antal informationssystem har påverkats genom användning av sådana apparater, datorprogram eller programinstruktioner som avses i 34 kap. 9 a § 1 punkten underpunkt a eller sådana lösenord, åtkomstkoder eller andra motsvarande uppgifter som avses i 9 a § 1 punkten underpunkt b,*
	4) brottet begås som ett led i en i 17 kap. 1 a § 4 mom. avsedd organiserad kriminell

Gällande lydelse	Föreslagen lydelse
	sammanslutnings verksamhet, eller
	5) brottet riktar sig mot ett informationssystem vars skadande äventyrar energiförsörjningen, den allmänna hälso- och sjukvården, försvaret, rättsvården eller någon annan med dessa jämförbar viktig samhällsfunktion,
och systemstörningen även bedömd som en helhet är grov, skall gärningsmannen för grov systemstörning dömas till fängelse i minst fyra månader och högst fyra år.	och systemstörningen även bedömd som en helhet är grov, *ska* gärningsmannen för *grov systemstörning* dömas till fängelse i minst fyra månader och högst *fem* år.
Försök är straffbart.	Försök är straffbart.
8 §	8 §
Dataintrång	*Dataintrång*
Den som genom att göra bruk av en användaridentifikation som han inte har rätt till eller genom att annars bryta säkerhetsarrangemang obehörigen tränger in i ett datasystem där data behandlas, lagras eller överförs elektroniskt eller med någon annan sådan teknisk metod eller i en särskilt skyddad del av ett sådant system, skall för *dataintrång* dömas till böter eller fängelse i högst ett år.	Den som genom att göra bruk av en användaridentifikation som han *eller hon* inte har rätt till eller genom att annars bryta säkerhetsarrangemang obehörigen tränger in i ett *informations*system där *information eller* data behandlas, lagras eller överförs elektroniskt eller med någon annan sådan teknisk metod eller i en särskilt skyddad del av ett sådant system, ska för *dataintrång* dömas till böter eller fängelse i högst två år.
För dataintrång döms också den som utan att tränga in i datasystemet eller en del av detta med tekniska specialanordningar obehörigen tar reda på information som finns i ett sådant datasystem som avses i 1 mom.	För dataintrång döms också den som utan att tränga in i ett *informations*system eller en del av *ett sådant*
	1) med *hjälp av* tekniska specialanordningar, *eller*
	2) annars med tekniska metoder genom att ta sig förbi säkerhetsarrangemangen, utnyttja informationssystemets sårbarhet eller använda annars uppenbart svikliga medel
	obehörigen tar reda på information *eller data* som finns i ett sådant *informations*system som avses i 1 mom.
Försök är straffbart.	Försök är straffbart.
Denna paragraf tillämpas endast på gärningar för vilka inte stadgas strängare eller lika strängt straff på något annat ställe i lag.	Denna paragraf tillämpas endast på gärningar för vilka inte *föreskrivs* strängare eller lika strängt straff på något annat ställe i lag.
8 a §	8 a §
Grovt dataintrång	*Grovt dataintrång*
Om dataintrång görs	Om dataintrång görs
1) som ett led i en i 17 kap. 1 a § 4 mom. avsedd organiserad kriminell sammanslut-	1) som ett led i en i 17 kap. 1 a § 4 mom. avsedd organiserad kriminell sammanslut-

Gällande lydelse	*Föreslagen lydelse*
nings verksamhet, eller 2) särskilt planmässigt, och dataintrånget även bedömt som en helhet är grovt, skall gärningsmannen för *grovt dataintrång* dömas till böter eller fängelse i högst två år. Försök är straffbart.	nings verksamhet, eller 2) särskilt planmässigt, och dataintrånget även bedömt som en helhet är grovt, *ska* gärningsmannen för *grovt dataintrång* dömas till böter eller fängelse i högst *tre* år. Försök är straffbart.
(ny)	9 b § *Identitetsstöld* *Den som i syfte att vilseleda en tredje part obehörigen använder någon annans personuppgifter eller identifieringsuppgifter eller andra motsvarande uppgifter som identifierar personen, och därmed orsakar ekonomisk skada eller mer än ringa olägenhet för den som uppgifterna gäller, ska för* ***identitetsstöld*** *dömas till böter.*
10 § *Åtalsrätt* — — — — — — — — — — — — — — (nytt 4 mom.)	10 § *Åtalsrätt* — — — — — — — — — — — — — — *Åklagaren får väcka åtal för identitetsstöld endast om målsäganden anmäler brottet till åtal.*
11 § *Förverkandepåföljd* Avkodningssystem som avses i 8 a § ska dömas förverkade till staten.	11 § *Förverkandepåföljd* Avkodningssystem som avses i 8 *b* § ska dömas förverkade till staten.
(ny)	13 § *Definitioner* *Vid tillämpningen av 3, 6, 7 a, 7 b och 8 § avses med informationssystem också i artikel 2 a i Europaparlamentets och rådets direktiv 2013/40/EU om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF, nedan* ***nätbrottsdirektivet****, avsedda*

Gällande lydelse	Föreslagen lydelse
	1) apparater eller grupper av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program automatiskt behandlar data, samt *2) data 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.* *Vid tillämpningen av 3, 7 a och 8 § avses med data också i artikel 2 b i nätbrottsdirektivet avsedda* *1) framställningar av fakta, information eller begrepp i en form som lämpar sig för behandling i ett informationssystem, samt* *2) program som lämpar sig för att få ett informationssystem att utföra en viss uppgift.*
	Denna lag träder i kraft den 20 .

2.

Lag

om ändring av 10 kap. 3 och 6 § i tvångsmedelslagen

I enlighet med riksdagens beslut

ändras i tvångsmedelslagen (806/2011) 10 kap. 3 § 2 mom. 12 punkten och 6 § 2 mom., sådana de lyder i lag 1146/2013, som följer:

Gällande lydelse	*Föreslagen lydelse*
10 kap.	
Hemliga tvångsmedel	
3 §	3 §
Teleavlyssning och dess förutsättningar	*Teleavlyssning och dess förutsättningar*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Förundersökningsmyndigheten kan ges tillstånd att rikta teleavlyssning mot en teleadress eller teleterminalutrustning som en misstänkt innehar eller annars kan antas använda, om den misstänkte är skäligen misstänkt för	Förundersökningsmyndigheten kan ges tillstånd att rikta teleavlyssning mot en teleadress eller teleterminalutrustning som en misstänkt innehar eller annars kan antas använda, om den misstänkte är skäligen misstänkt för
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
12) grov skadegörelse	12) grov skadegörelse *eller grov dataskadegörelse,*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
6 §	6 §
Teleövervakning och dess förutsättningar	*Teleövervakning och dess förutsättningar*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Förundersökningsmyndigheten kan ges tillstånd att rikta teleövervakning mot en teleadress eller teleterminalutrustning som en misstänkt innehar eller annars kan antas använda, om den misstänkte är skäligen misstänkt för	Förundersökningsmyndigheten kan ges tillstånd att rikta teleövervakning mot en teleadress eller teleterminalutrustning som en misstänkt innehar eller annars kan antas använda, om den misstänkte är skäligen misstänkt för
1) ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst fyra år,	1) ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst fyra år,
2) ett brott som begåtts med användning av en teleadress eller teleterminalutrustning och för vilket det föreskrivna strängaste straffet är fängelse i minst två år,	2) ett brott som begåtts med användning av en teleadress eller teleterminalutrustning och för vilket det föreskrivna strängaste straffet är fängelse i minst två år,

Gällande lydelse	*Föreslagen lydelse*
3) olovligt brukande, *skadegörelse, kränkning av kommunikationshemlighet eller dataintrång* som riktat sig mot ett automatiskt databehandlingssystem och som begåtts med användning av en teleadress eller teleterminalutrustning	3) olovligt brukande som riktat sig mot ett automatiskt databehandlingssystem och som begåtts med användning av en teleadress eller teleterminalutrustning
4) utnyttjande av person som är föremål för sexhandel, lockande av barn i sexuella syften eller koppleri,	4) utnyttjande av person som är föremål för sexhandel, lockande av barn i sexuella syften eller koppleri,
5) narkotikabrott,	5) narkotikabrott,
6) förberedelse till brott som begås i terroristiskt syfte,	6) förberedelse till brott som begås i terroristiskt syfte,
7) grovt tullredovisningsbrott,	7) grovt tullredovisningsbrott,
8) grovt döljande av olagligt byte,	8) grovt döljande av olagligt byte,
9) förberedelse till tagande av gisslan, eller	9) förberedelse till tagande av gisslan, eller
10) förberedelse till grovt rån.	10) förberedelse till grovt rån.
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —

Denna lag träder i kraft den 20 .

3.

Lag

om ändring av 5 kap. 8 § i polislagen

I enlighet med riksdagens beslut
ändras i polislagen (872/2011) 5 kap. 8 § 2 mom., sådant det lyder i lag 1168/2013, som följer:

Gällande lydelse	*Föreslagen lydelse*
5 kap.	
Hemliga metoder för inhämtande av information	
8 §	8 §
Teleövervakning och dess förutsättningar	*Teleövervakning och dess förutsättningar*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
För att förhindra brott kan polisen ges tillstånd att rikta teleövervakning mot en teleadress eller teleterminalutrustning som innehas eller sannolikt används av en person, om personen på grund av sina yttranden, hotelser eller uppträdande eller annars med fog kan antas göra sig skyldig till	För att förhindra brott kan polisen ges tillstånd att rikta teleövervakning mot en teleadress eller teleterminalutrustning som innehas eller sannolikt används av en person, om personen på grund av sina yttranden, hotelser eller uppträdande eller annars med fog kan antas göra sig skyldig till
1) ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst fyra år,	1) ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst fyra år,
2) ett brott som begåtts med användning av en teleadress eller teleterminalutrustning och för vilket det föreskrivna strängaste straffet är fängelse i minst två år,	2) ett brott som begåtts med användning av en teleadress eller teleterminalutrustning och för vilket det föreskrivna strängaste straffet är fängelse i minst två år,
3) olovligt brukande, *skadegörelse, kränkning av kommunikationshemlighet eller dataintrång* som riktar sig mot ett automatiskt databehandlingssystem och som begåtts med användning av en teleadress eller teleterminalutrustning,	3) olovligt brukande som riktar sig mot ett automatiskt databehandlingssystem och som begåtts med användning av en teleadress eller teleterminalutrustning,
4) utnyttjande av en person som är föremål för sexhandel, lockande av barn i sexuella syften eller koppleri,	4) utnyttjande av en person som är föremål för sexhandel, lockande av barn i sexuella syften eller koppleri,
5) narkotikabrott,	5) narkotikabrott,
6) förberedelse till brott som begås i terroristiskt syfte, eller	6) förberedelse till brott som begås i terroristiskt syfte, eller
	7) grovt tullredovisningsbrott.

Gällande lydelse	*Föreslagen lydelse*
ristiskt syfte, eller 7) grovt tullredovisningsbrott.	
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
	Denna lag träder i kraft den 20 .

4.

Lag

om ändring av 2 § i militära rättegångslagen

I enlighet med riksdagens beslut

ändras i militära rättegångslagen (326/1983) 2 § 2 mom., sådant det lyder i lag 1442/2007, som följer:

Gällande lydelse	*Föreslagen lydelse*
2 §	2 §
Såsom militärt rättegångsärende handläggs även åtal mot krigsman för en gärning för vilken straff bestäms i 21 kap. 1—3 eller 5—14 §, 25 kap. 7 eller 8 §, 28, 31—33 eller 35 kap., 36 kap. 1—3 §, 37 kap. 8—10 §, 38 kap. 1—7, 7 a, 7 b, 8 eller 8 a § eller 40 kap. 1—3 eller 5 § i strafflagen (39/1889). Detta förutsätter att gärningen har riktat sig mot försvarsmakten eller mot någon annan krigsman. Såsom militärt rättegångsärende handläggs också åtal för en gärning för vilken straff bestäms i 118 § i värnpliktslagen (1438/2007).	Såsom militärt rättegångsärende handläggs även åtal mot krigsman för en gärning för vilken straff bestäms i 21 kap. 1—3 eller 5—14 §, 25 kap. 7 eller 8 §, 28, 31—33 eller 35 kap., 36 kap. 1—3 §, 37 kap. 8—10 §, 38 kap. 1—7, 7 a, 7 b, 8, 8 a eller 9 b § eller 40 kap. 1—3 eller 5 § i strafflagen (39/1889). Detta förutsätter att gärningen har riktat sig mot försvarsmakten eller mot någon annan krigsman. Såsom militärt rättegångsärende handläggs också åtal för en gärning för vilken straff bestäms i 118 § i värnpliktslagen (1438/2007).

Denna lag träder i kraft den 20 .