EUROOPA LIIDU NÕUKOGU

Brüssel, 30. mai 2011 (06.06)
(OR. en)

10751/11

Institutsioonidevaheline dokument: 2010/0273 (COD)

DROIPEN 47
TELECOM 82
CODEC 915

MÄRKUS

Saatja:	Eesistujariik
Saaja:	COREPER / nõukogu
Eelm dok nr:	10357/11 DROIPEN 42 TELECOM 74 CODEC 851
Teema:	Ettepanek: Euroopa Parlamendi ja nõukogu direktiiv, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega asendatakse nõukogu raamotsus 2005/222/JSK - Üldine lähenemisviis

I. TAUSTTEAVE

Komisjon esitas 30. septembril 2010 Euroopa Parlamendile ja nõukogule järgmise ettepaneku: Euroopa Parlamendi ja nõukogu direktiiv, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega tunnistatakse kehtetuks nõukogu raamotsus 2005/222/JSK.

Vastavalt aluslepingu protokolli (nr 21) artikli 3 lõikele 1 teavitasid Ühendkuningriik ja Iirimaa nõukogu sellest, et nad sooviksid osaleda direktiivi vastuvõtmisel ja kohaldamisel. Aluslepingu protokolli (nr 22) kohaselt Taani nimetatud õigusakti vastuvõtmisel ei osale.

UK ja FR esitasid parlamentaarse analüüsi reservatsiooni. DE, SI, FR ja SE esitasid üldise analüüsi reservatsiooni ettepaneku suhtes.

Ettepanek esitati nõukogule 8.–9. novembri 2010. aasta istungil.

Kriminaalasjades tehtava politsei- ja õigusalase koostöö kooskõlastuskomiteel (CATS) paluti kolmel korral anda strateegilisi juhtnööre aruteludeks kriminaalõiguse töörühmas (edaspidi DROIPEN). CATS andis läbirääkimiste alguses, 13. detsembril 2010 üldsuunised edasiseks aruteluks. 11. veebruaril 2011 analüüsis CATS komisjoni ettepaneku artikli 10 lõiget 3, millega kehtestatakse uus raskendav asjaolu küberrünnakute puhul, mis on toime pandud tegeliku omaniku identiteediandmete väärkasutamise kaudu. Lõpetuseks konsulteeriti CATSiga 22. märtsil nelja lahendamata küsimuse osas: vähemolulisi juhtumeid väljajätvate sätete kohaldamisala, artiklis 3 sätestatud süüteo koosseis, karistusmäärad ja kodakondsusel põhinev jurisdiktsioon.

DROIPEN arutas ettepanekut oma koosolekutel, mis toimusid 13.–14. ja 28. jaanuaril 2011 ning 2.-3. ja 29. märtsil 2011. DROIPEN viis oma 29. märtsi 2011. aasta koosolekul lõpule teksti kolmanda lugemise.

Nõukogu võttis 25. veebruaril 2011 teadmiseks arutelude hetkeolukorra. Nõukogu võttis 12. aprillil 2011 teadmiseks esialgse kokkuleppe, mis oli saavutatud direktiivi eelnõu artiklite 1–6 ja 11–19 osas. Samuti andis nõukogu suuniseid mitme lahendamata küsimuse osas, määratledes sellega poliitilise raamistiku, mille alusel jätkati nõukogu ettevalmistavates organites ettepaneku osas tehtavat tööd.

II. KOMPROMISSPAKETI ETTEPANEK

Lisas esitatud tekst on kompromissettepanek, mis koostati justiits- ja siseküsimuste nõunike 13. mai 2011. aasta koosoleku ning eesistujariigi sõprade rühma 24. mai 2011. aasta koosoleku tulemusel.

Arutelude käigus tehti komisjoni esialgsesse ettepanekusse mitmeid kohandusi, et arvestada delegatsioonide väljendatud seisukohti nii palju kui võimalik. Eesistujariik on samuti püüdnud säilitada tasakaalu komisjoni ettepaneku aluseks olnud põhjustega, milleks on eelkõige vajadus sätestada ELi tasandil tõhusam kriminaalõiguslik reageerimine küberkuritegevusest tulenevatele uutele ohtudele, nagu näiteks suuremahulised küberründed.

A. Sellega seoses soovib eesistujariik tuletada meelde kompromisspaketi põhielemente, mille nõukogu esialgselt kinnitas oma 12. aprilli 2011. aasta istungil.

1. Kriminaliseerimise kohaldamisala (artiklid 3–7)

- Viidet „vähemolulistele juhtumitele" on laiendatud kõigile direktiivis viidatud süütegudele (artiklid 3–7). Seega on vähemolulised juhtumid direktiivi kohaldamisalast täielikult välja jäetud. Vähemolulise juhtumi mõiste määratlemine toimub siseriikliku õiguse ja praktika alusel (vt põhjendus 6a) ning samuti on lisatud vastavad näited.
- Artikli 3 „Ebaseaduslik sisenemine infosüsteemi" kohaldamisala piirdub juhtumitega, mille puhul turvameetme rikkumine moodustab süüteo koosseisu. Võimalus selleks on ette nähtud Budapesti konventsioonis valikuvõimalusena, kuid see ei sisaldunud esialgses komisjoni ettepanekus.
- Küberrünnakute toimepanemisel kasutatud vahendite omamine on artikli 7 kohaldamisalast välja jäetud.
- Süüteo toimepanemise katse kriminaliseerimine on piiratud artiklites 4 ja 5 osutatud süütegudega.

2. Karistused (artikkel 9)

- Säilitatud on komisjoni ettepanek, mis on seotud kergemate süütegude karistusmääradega (vt artikli 9 lõiget 2), st maksimaalselt vähemalt kaheaastane vangistus. Selle põhjuseks on eelkõige kriminaliseerimise piiratud kohaldamisala, mis tulenes nõukogu ettevalmistavates organites asetleidnud aruteludest. Sätte kohaldamisala on veelgi piiratud, see hõlmab artikleid 3–6, seega ei ole enam kohustust sätestada seda konkreetset karistusmäära artiklis 7.
- Kompromissettepanekuga kehtestatakse suurem paindlikkus seoses raskendavatel asjaoludel toimepandud süütegude karistusmääradega: sõltuvalt süüteo raskusest maksimaalselt vähemalt kolme- ja viieaastane vangistus (vastavalt artikli 9 lõige 3 ja lõige 4) ning lisaks on sätete kohaldamine kompromissi alusel piiratud artiklitega 4 ja 5.

3. Jurisdiktsioon (artikkel 13)

- Enda kodanike suhtes jurisdiktsiooni kehtestamine on seotud positiivse topeltkaristatavuse kontrolliga (artikli 13 lõike 1 punkt b).
- Direktiivi sätteid ei kohaldata riikliku jurisdiktsiooni kohaldamise tingimuste suhtes (vt preambul, põhjendus 10a).

4. Direktiivi eelnõus sätestatud süütegudega seonduv teabevahetus (artikkel 14)

- Säilitatakse kiireloomulistele taotlustele vastamiseks ettenähtud tähtaeg, milleks on 8 tundi, samas on teksti muudetud, et täpsustada taotluse saanud riigi kohustuse olemust, eelkõige seda, et ettenähtud tähtaja jooksul teatab pädev asutus vähemalt seda, kas ta saab abitaotlusele vastata ning juhul kui ta seda saab, märgib täiendavalt eeldatava vastuse mõned esialgsed elemendid, nagu näiteks vastuse vorm ja eeldatav vastamise aeg.

B. Ettepaneku osas jätkati tööd, võttes arvesse nõukogu poolt 12. aprillil 2011 antud poliitilisi suuniseid. Selle tulemusel tuleks üldises kompromisspaketis käsitleda ka järgmisi uusi elemente:

1. Süüteo toimepanemisel kasutatud vahendid - artikkel 7

- Artikli 7 kohaldamisala on täiendavalt piiratud. Selle tulemusel on ettepaneku kohaldamisalast samuti välja jäetud selliste seadmete tootmine või kättesaadavaks tegemine, mida saab kasutada küberrünnete toimepanemiseks.
- Direktiivis kasutatakse „seadme” mõiste kitsast tõlgendust, millele on osutatud artiklis 7, ning mis erineb komisjoni ettepanekust, mis põhines kõnealuse mõiste laiemal tõlgendusel ja hõlmas nt eririistvara, mida kasutatakse küberrünnete toimepanemiseks.

2. Suuremahulised küberründed kui raskendavad asjaolud - artikkel 9

- Säilitatud on komisjoni ettepaneku põhielement, mis käsitles raskendavate asjaoludena suuremahulisi küberründeid, kuigi seda on märkimisväärselt muudetud. Rõhutada tuleks, et suuremahuliste küberrünnetena käsitatakse kaht alternatiivset süütegu - need on kas ründed suure hulga infosüsteemide vastu või suurt kahju põhjustavad ründed. Kõnealust kaht aspekti käsitletakse vastavalt artikli 9 lõikes 3 ja lõike 4 punktis b.

- Selleks, et leida lahendus mitme delegatsiooni murele, mille kohaselt esineb vajadus luua selge seos praeguste ohtudega, mida kujutavad kurjategijate kasutatavad teatud meetodid suuremahuliste küberrünnete toimepanemiseks, nagu näiteks „robotivõrgu”[1] loomine ja kasutamine, on ettepaneku põhjendustesse lisatud asjakohane sõnastus (vt põhjendused 3 ja 7). Eesistujariik on valinud selle lähenemisviisi, et säilitada direktiivi regulatiivosas paindlikkus ja tehniline neutraalsus suuremahuliste küberrünnete toimepanemisel kasutatavate meetodite küsimuses. See on eriti oluline, võttes arvesse tehnoloogia pidevat arengut ja kõnealuse kuriteoliigi pidevalt arenevat olemust.

- Kompromissina jäeti välja artikli 9 lõige 5, mis käsitleb teise isiku isikuandmete väärkasutamist eesmärgiga võita kolmanda isiku usaldus, mis lihtsustab küberründe toimepanemist. Selle tingis mõne delegatsiooni poolt korduvalt väljendatud seisukoht, mille kohaselt on tegemist fenomeniga, mida tuleks käsitleda terviklikult spetsiaalses õigusaktis, mis käsitleb identiteedivarguse vastast võitlust.

[1] Nn „robotivõrgu” kasutamist iseloomustavad kuriteo teineteisele järgnevad etapid, mis ka eraldiseisvalt võivad kujutada endast tõsist ohtu üldistele huvidele. Sellega seoses on direktiivi üheks eesmärgiks kehtestada kriminaalsanktsioonid seoses „robotivõrgu” loomise etapiga, milleks on kaugkontroll märkimisväärse arvu arvutite üle, mis saadakse selle kaudu, et nakatatakse eesmärgipäraste küberrünnete abil kõnealused arvutid kurivaraga. Hilisemas etapis saab „robotivõrgu” moodustavad nakatatud arvutid aktiveerida arvutikasutaja teadmata, et panna toime suuremahulisi küberründeid, mis üldjuhul võivad põhjustada suurt kahju.

3. Jurisdiktsioon (põhjendus 10a)

- Põhjenduse 10a sõnastuse muutmisega eristati selgesõnaliselt artiklis 13 osutatud tingimused jurisdiktsiooni kehtestamiseks ja tingimused jurisdiktsiooni kohaldamiseks.

COREPERi palutakse a) analüüsida kompromissi uusi elemente kui lahutamatut osa üldisest kompromisspaketi ettepanekust ning b) kinnitada, et lisas esitatud tekst tuleks edastada nõukogule, et saavutada ettepaneku osas üldine lähenemisviis, nii et lisatud tekst oleks Euroopa Parlamendiga toimuvate edasiste arutelude aluseks vastavalt Euroopa Liidu toimimise lepingu artiklile 294.

2010/0273 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV,

milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega asendatakse nõukogu raamotsus 2005/222/JSK

EUROOPA PARLAMENT JA EUROOPA LIIDU NÕUKOGU,
võttes arvesse Euroopa Liidu toimimise lepingut,
eriti selle artikli 83 lõiget 1,
võttes arvesse Euroopa Komisjoni ettepanekut[2],
olles edastanud seadusandliku akti eelnõu riikide parlamentidele,
võttes arvesse Euroopa Majandus- ja Sotsiaalkomitee arvamust,
võttes arvesse Regioonide Komitee arvamust,
toimides seadusandliku tavamenetluse kohaselt
ning arvestades järgmist:

(1) Käesoleva direktiivi eesmärk on ühtlustada liikmesriikide kriminaalõigust infosüsteemide vastu suunatud rünnete valdkonnas, kehtestada miinimumeeskirjad kuritegude määratlemise ja sanktsioonide kohta ning arendada koostööd pädevate asutuste, sealhulgas liikmesriikide politsei- ja muude spetsialiseeritud õiguskaitseasutuste vahel.

(2) Infosüsteemide vastu suunatud, eelkõige organiseeritud kuritegevuse ohust tulenevate rünnete oht aina suureneb ning seega mure infosüsteemide kui liikmesriikide ja ELi elutähtsa infrastruktuuri osa vastu suunatud võimalike terrori- või poliitiliselt ajendatud rünnakute pärast kasvab. See on ohuks nii infoühiskonna turvalisemaks muutmisele kui ka vabadusel, turvalisusel ja õigusel rajaneva ala saavutamisele ning nõuab seega Euroopa Liidu tasandi meedet.

[2] ELT C […], […], lk […].

(2a) Liidus on teatav arv elutähtsaid infrastruktuure, mille kahjustada saamisel või hävimisel oleks olulised piiriülesed mõjud. Vajadusest tõsta Euroopas elutähtsate infrastruktuuride kaitsevõimet johtub see, et infosüsteemide vastu suunatud rünnete vastast võitlust tuleks täiendada rangete kriminaalsanktsioonidega, mis kajastavad selliste rünnete raskusastet. Elutähtsa infrastruktuurina võib käsitada liikmesriikides asuvat vara, süsteemi või selle osa, mis on hädavajalik näiteks eluliselt tähtsate ühiskondlike toimingute, tervishoiu, turvalisuse, julgeoleku, inimeste majandusliku ja sotsiaalse heaolu toimimiseks ning mille kahjustada saamine või hävimine mõjutaks nimetatud toimingute toimimishäire tulemusena oluliselt liikmesriiki.

(3) On tõendeid, et üha ohtlikumaid ja korduvaid suuremahulisi ründeid suunatakse järjest enam infosüsteemide vastu, mis võivad sageli olla riikidele või avaliku või erasektori toimimise seisukohalt äärmiselt olulised. Selle tendentsiga kaasneb üha keerukamate meetodite arendamine, nagu näiteks nn „robotivõrkude" loomine ja kasutamine. „Robotivõrku" iseloomustavad kuriteo teineteisele järgnevad etapid, mis ka eraldiseisvalt võivad kujutada endast tõsist ohtu üldistele huvidele. Sellega seoses on direktiivi üheks eesmärgiks kehtestada kriminaalsanktsioonid seoses „robotivõrgu" loomise etapiga, milleks on kaugkontroll märkimisväärse arvu arvutite üle, mis saadakse selle kaudu, et nakatatakse eesmärgipäraste küberrünnete abil kõnealused arvutid kurivaraga. Hilisemas etapis saab „robotivõrgu" moodustava nakatatud arvutite võrgu aktiveerida arvutikasutaja teadmata, et panna toime suuremahulisi küberründeid, mis üldjuhul võivad põhjustada suurt kahju, nagu sellele on osutatud käesolevas direktiivis. Liikmesriigid võivad vastavalt oma riiklikule õigusele ja praktikale määratleda suure kahju mõiste, mis võib hõlmata märkimisväärset üldist huvi kujutavate teenuste osutamise häirimist või suurt rahalist kahju või isikuandmete kaotsiminekut.

(4) Ühised eeskirjad selles valdkonnas, eelkõige seoses infosüsteemide ja arvutiandmetega, on olulised tagamaks liikmesriikides järjekindlat lähenemisviisi käesoleva direktiivi kohaldamisel.

(5) Tuleb tagada ühine lähenemisviis kuriteokoosseisu suhtes, kriminaliseerides selleks kõikjal ELis ebaseadusliku infosüsteemi sisenemise, ebaseadusliku süsteemi häirimise, ebaseadusliku andmetesse sekkumise ja teabe ebaseadusliku pealtkuulamise.

(6) Liikmesriigid peaksid infosüsteemide vastu suunatud rünnete eest ette nägema karistused. Sätestatavad karistused peaksid olema tõhusad, proportsionaalsed ja hoiatavad.

(6a) Direktiiviga sätestatakse kriminaalsanktsioonid vähemalt oluliste juhtumite puhul. Liikmesriigid võivad vastavalt oma riiklikule õigusele ja praktikale määratleda vähemolulise juhtumi mõiste. Juhtumit võidakse käsitada vähemolulisena näiteks siis, kui kahju ja/või oht, mida see võib põhjustada avalikele või erahuvidele, näiteks arvutisüsteemi või arvutiandmete puutumatusele, või isiku puutumatusele, õigustele ja muudele huvidele ei ole märkimisväärne või ei ole sellise iseloomuga, et kriminaalkaristuse kohaldamine õigusaktidega sätestatud piirmäärade raames või kriminaalvastutuse kohaldamine oleks vajalik.

(7) Asjakohane on näha ette keskmisest rangemad karistused juhuks, kui infosüsteemide vastu suunatud ründe on toime pannud kuritegelik ühendus, nagu see on määratletud nõukogu 24. oktoobri 2008. aasta raamotsuses 2008/841/JSK (organiseeritud kuritegevuse vastase võitluse kohta)[3] või kui rünne on suuremahuline, mõjutades seega märkimisväärset arvu infosüsteeme või põhjustades suurt kahju, sealhulgas kui ründe eesmärgiks oli luua „robotivõrk" või kui see pandi toime „robotivõrgu" abil, põhjustades seeläbi suurt kahju.

(8) Nõukogu 27.–28. novembri 2008. aasta järeldustes märgiti, et liikmesriigid ja komisjon peaksid välja töötama uue strateegia, võttes arvesse Euroopa Nõukogu küberkuritegevuse 2001. aasta konventsiooni. Nimetatud konventsiooniga on kehtestatud küberkuritegevuse, sealhulgas infosüsteemide vastu suunatud rünnete vastase võitluse õiguslik raamistik. Käesolev direktiiv tugineb nimetatud konventsioonile.

(9) Arvestades rünnete erinevaid toimepaneku viise ning tark- ja riistvara kiiret arengut, viidatakse käesolevas direktiivis vahenditele, mille abil on võimalik käesolevas direktiivis loetletud kuritegusid toime panna. Vahendite all mõistetakse näiteks kurivara, sealhulgas sellist kurivara, mille abil on võimalik luua robotivõrke, mida kasutatakse küberrünnete toimepanemiseks. Kuna käesoleva direktiiviga kehtestatakse miinimumeeskirjad, võivad liikmesriigid sätestada kriminaalsanktsioonid teist liiki süütegude suhtes, mis seonduvad süütegude toimepanemiseks kasutatavate vahenditega, nagu näiteks selliste vahendite omamine või mis tahes teiste seadmete, sealhulgas riistvara, mis on loodud või kohandatud eelkõige direktiivis osutatud süütegude toimepanemiseks, tootmine, müük, kasutamiseks hankimine, importimine, levitamine ja muul viisil kättesaadavaks tegemine.

(10) Käesoleva direktiiviga ei nähta ette kriminaalvastutust juhul, kui süütegu on toime pandud kriminaalse tahtluseta, näiteks infosüsteemide volitatud testimise ja kaitsmise korral või kui isik ei olnud teadlik, et juurdepääs ei ole lubatud.

(10a) Käesoleva direktiiviga ei sätestata tingimusi, mis tuleb täita selleks, et (…) teostada jurisdiktsiooni artiklites 3–8 viidatud süütegude üle, näiteks ohvri avaldus süüteo toimepanemise asukohas või süüteo toimepanemise asukohariigi avaldus, või asjaolu, et süüteo toimepanijale ei ole esitatud süüdistust süüteo toimepanemise asukohas.

(11) Käesoleva direktiiviga tugevdatakse võrgustike, näiteks G8 ning teabevahetuseks loodud Euroopa Nõukogu seitse päeva nädalas ööpäev läbi töötava kontaktpunktide võrgustiku tähtsust, et tagada olemasoleva asjakohase teabe andmine seoses infosüsteemide ja andmetega seotud kuritegude uurimise ja menetlusega, kaasates taotlevaid liikmesriike. Arvestades suuremahuliste rünnete leviku võimalikku kiirust, peaksid liikmesriigid olema võimelised viivitamata vastama nimetatud kontaktpunktide võrgustiku kaudu esitatud kiireloomulistele taotlustele. Sellistel juhtudel võib olla otstarbekas, et koos teabenõudega luuakse telefonikontakt tagamaks, et nõude saanud riik menetleb seda kiiresti ja et tagasisidet antakse kaheksa tunni jooksul, kinnitades nõuete kättesaamist ja osutades, kas ja millal sellele tõenäoliselt vastatakse.

(12) Selleks et saada ELi tasandil probleemist senisest parem ülevaade ja aidata kaasa senisest tõhusamate lahenduste väljatöötamisele, on käesoleva direktiivi kohaselt vaja koguda andmeid süütegude kohta. Andmeid saavad kasutada ka spetsialiseeritud asutused, näiteks Europol ning Euroopa Võrgu- ja Infoturbeamet, et hinnata senisest täpsemini küberkuritegevuse ulatust ning võrgu- ja infoturbe olukorda Euroopas.

[3] ELT L 300, 11.11.2008, lk 42.

(13) Märkimisväärsed lüngad ja erinevused liikmesriikide infosüsteemide vastu suunatud rünnete valdkonna õigusaktides võivad takistada organiseeritud kuritegevuse ja terrorismi vastast võitlust ning raskendada tõhusat politsei- ja õigusalast koostööd kõnealuses valdkonnas. Tänapäevaste infosüsteemide riikidevahelise ja piirideta olemuse tõttu on selliste süsteemide vastu suunatud rünnetel sageli piiriülene mõõde, mis rõhutab kiireloomulist vajadust asjaomase valdkonna kriminaalõiguse edasise ühtlustamise järele. Lisaks sellele peaks nõukogu raamotsus 2009/948/JSK (kohtualluvuskonflikti vältimise ja lahendamise kohta kriminaalmenetluses) hõlbustama infosüsteemide vastu suunatud rünnete eest süüdistuse esitamise kooskõlastamist.

(14) Kuna käesoleva direktiivi eesmärke, nimelt tagada kõikides liikmesriikides tõhusad, proportsionaalsed ja hoiatavad kriminaalkaristused infosüsteemide vastu suunatud rünnete eest ning arendada ja soodustada õigusalast koostööd võimalike probleemide kõrvaldamise teel, ei suuda liikmesriigid piisaval määral saavutada, kuna eeskirjad peavad olema ühised ja üksteisega kooskõlas, ning need on paremini saavutatavad ELi tasandil, võib EL võtta meetmeid kooskõlas Euroopa Liidu lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega. Käesolev direktiiv ei lähe nimetatud eesmärkide saavutamiseks vajalikust kaugemale.

(15) Käesoleva direktiivi rakendamise eesmärgil töödeldud isikuandmeid tuleks kaitsta vastavalt nõukogu 27. novembri 2008. aasta raamotsusele 2008/977/JSK (kriminaalasjades tehtava politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta)[4], kui töötlustoimingud kuuluvad käesoleva direktiivi reguleerimisalasse, ning Euroopa Parlamendi ja nõukogu 18. detsembri 2000. aasta määrusele (EÜ) nr 45/2001 (üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta)[5].

[4] ELT L 350, 30.12.2008, lk 60.
[5] EÜT L 8, 12.1.2001, lk 1.

(16) Käesolevas direktiivis austatakse põhiõigusi ja järgitakse eelkõige Euroopa Liidu põhiõiguste hartas tunnustatud põhimõtteid, sealhulgas isikuandmete kaitset, sõna- ja teabevabadust, õigust õiglasele kohtulikule arutamisele, süütuse presumptsiooni ja kaitseõigust ning kuritegude ja karistuste seaduslikkuse ja proportsionaalsuse põhimõtet. Eelkõige on käesoleva direktiivi eesmärk tagada nimetatud õiguste täielik austamine ja sellest tuleb direktiivi järgimisel ka lähtuda.

(17) Euroopa Liidu toimimise lepingule lisatud protokolli (Ühendkuningriigi ja Iirimaa seisukoha kohta vabadusel, turvalisusel ja õigusel rajaneva ala suhtes) artikli (…) 3 (…) kohaselt on Ühendkuningriik ja Iirimaa teatanud oma soovist osaleda käesoleva direktiivi vastuvõtmisel ja kohaldamisel.

(18) Euroopa Liidu toimimise lepingule lisatud Taani seisukohta käsitleva protokolli artiklite 1 ja 2 kohaselt ei osale Taani käesoleva direktiivi vastuvõtmisel, mistõttu see ei ole tema suhtes siduv ega kohaldatav.

(19) Käesoleva direktiivi eesmärk on muuta ja laiendada raamotsuse 2005/222/JSK sätteid. Kuna tehtavad muudatused on arvukad ja sisulised, siis tuleks raamotsus selguse huvides täielikult asendada käesoleva direktiivi vastuvõtmises osalevate liikmesriikide suhtes.

(20) Kooskõlas paremat õigusloomet käsitleva institutsioonidevahelise kokkuleppe[6] punktiga 34 julgustatakse liikmesriike koostama enda jaoks ja liidu huvides oma tabelid, mis võimalikult suures ulatuses näitlikustavad vastavust direktiivi ja selle ülevõtmise meetmete vahel, ning need avaldama,

[6] ELT C 321, 31.12.2003, lk 1.

ON VASTU VÕTNUD KÄESOLEVA DIREKTIIVI:

Artikkel 1

Sisu

Käesoleva direktiiviga kehtestatakse miinimumeeskirjad infosüsteemide vastu suunatud rünnete valdkonna kuritegude ja sanktsioonide määratlemise kohta. Samuti on direktiivi eesmärk hõlbustada selliste süütegude vältimist ja arendada koostööd kohtuasutuste ja muude pädevate asutuste vahel.

Artikkel 2

Mõisted

Käesolevas direktiivis kasutatakse järgmisi mõisteid:

a) „infosüsteem" – seade või omavahel ühendatud või seotud seadmete rühm, mille hulgast üks või mitu seadet teostavad vastavalt programmile arvutiandmete automaattöötlust; samuti nimetatud seadme või seadmete rühma salvestatud, töödeldud, välja võetud ja edastatud arvutiandmed, mis on vajalikud kõnealuse seadme või seadmete rühma toimimiseks, kasutamiseks, kaitseks ja hoolduseks;

b) „arvutiandmed" – faktide, teabe või mõistete esitamine infosüsteemis töötlemiseks sobivas vormis, sealhulgas programm, mille abil saab infosüsteemi panna ülesannet täitma;

c) „juriidiline isik" – üksus, millel on vastavalt kohaldatavale õigusele juriidilise isiku staatus, välja arvatud riigid ja riigivõimu teostavad avalik-õiguslikud asutused ning avalik-õiguslikud rahvusvahelised organisatsioonid;

d) „õigusliku aluseta" – süsteemi sisenemine, selle häirimine, pealtkuulamine või mistahes muu käesolevas direktiivis osutatud toiming ilma süsteemi või selle osa omaniku või selle suhtes muu õiguse valdaja loata või rikkudes riiklikke õigusakte.

Artikkel 3

Ebaseaduslik sisenemine infosüsteemi

Liikmesriik võtab vajalikud meetmed tagamaks, et tahtlikult toime pandud õigusliku aluseta sisenemine infosüsteemi või selle osasse on vähemalt siis, kui süüteo toimepanemisel rikutakse mõnda turvameedet ja oluliste juhtumite puhul kriminaalkorras karistatav.

Artikkel 4

Ebaseaduslik süsteemi häirimine

Liikmesriik võtab vajalikud meetmed tagamaks, et infosüsteemi töö takistamine ja katkestamine arvutiandmete sisestamise, edastamise, kahjustamise, kustutamise, rikkumise, muutmise, sulustamise ja ligipääsmatuks muutmise teel juhul, kui tegu pannakse toime tahtlikult ja ilma õigusliku aluseta, on vähemalt raskemate juhtumite puhul kriminaalkorras karistatav.

Artikkel 5

Ebaseaduslik andmetesse sekkumine

Liikmesriik võtab vajalikud meetmed tagamaks, et infosüsteemis olevate arvutiandmete kustutamine, kahjustamine, rikkumine, muutmine, sulustamine ja ligipääsmatuks muutmine juhul, kui tegu pannakse toime tahtlikult ja ilma õigusliku aluseta, on vähemalt raskete juhtumite puhul kriminaalkorras karistatav.

Artikkel 6

Teabe ebaseaduslik pealtkuulamine

Liikmesriik võtab vajalikud meetmed tagamaks, et infosüsteemi, sellest süsteemist või selle süsteemi piires, sealhulgas infosüsteemi elektromagnetkiirguse abil mitteavalikult edastatavate arvutiandmete tahtlik pealtkuulamine tehniliste vahendite abil on kriminaalkorras karistatav, kui tegu pannakse toime tahtlikult ja ilma õigusliku aluseta, seda vähemalt raskemate juhtumite puhul.

Artikkel 7

Süüteo toimepanemisel kasutatud vahendid

(1) Liikmesriik võtab vajalikud meetmed tagamaks, et järgmiste seadmete ja andmete tootmine, müük, kasutamiseks hankimine, importimine, levitamine ja muul viisil kättesaadavaks tegemine on kriminaalkorras karistatav, kui tegu on toime pandud tahtlikult ja ilma õigusliku aluseta, kavatsusega kasutada seda eesmärgiga panna toime mõni artiklites 3–6 nimetatud süütegu, seda vähemalt raskemate juhtumite puhul:

a) arvutiprogramm, mis on loodud või kohandatud eelkõige artiklites 3–6 nimetatud süütegude toimepanemiseks;

b) arvuti salasõna, juurdepääsukood ja samalaadsed andmed, mille abil on võimalik siseneda infosüsteemi või selle osasse.

Artikkel 8

Süüteole kihutamine, kaasaaitamine ja süüteokatse

1. Liikmesriik tagab, et artiklites 3–7 nimetatud süütegude toimepanemisele kihutamine ja kaasaaitamine on kriminaalkorras karistatav.

2. Liikmesriik tagab, et artiklites 4–5 nimetatud süüteo katsed on kriminaalkorras karistatavad.

Artikkel 9

Karistused

1. Liikmesriik võtab vajalikud meetmed tagamaks, et artiklites 3–8 nimetatud süütegude eest karistatakse tõhusate, proportsionaalsete ja hoiatavate kriminaalkaristustega.

2. Liikmesriik võtab vajalikud meetmed tagamaks, et artiklites 3–6 nimetatud süütegude eest määratakse karistus, mille maksimummäär on vähemalt kaheaastane vangistus.

3. Liikmesriik võtab vajalikud meetmed tagamaks, et artiklites 4–5 nimetatud süütegude tahtliku toimepanemise eest määratakse karistus, mille maksimummäär on vähemalt kolmeaastane vangistus, kui (…) arvestatavat hulka infosüsteeme on mõjutatud artikli 7 lõikes 1 osutatud vahendi kasutamise tulemusel, mis on loodud või kohandatud eelkõige süüteo toimepanemiseks[7].

4. Liikmesriik võtab vajalikud meetmed tagamaks, et artiklites 4–5 nimetatud süütegude eest määratakse karistus, mille maksimummäär on vähemalt viieaastane vangistus, kui need

a) on toime pandud raamotsuses 2008/841/JSK määratletud kuritegeliku ühenduse raames, sõltumata selles viidatud karistusmäärast, või
b) põhjustavad suurt kahju[8] või
c) on toime pandud elutähtsa infrastruktuuri infosüsteemi vastu.

(…)

[…]

Artikkel 11

Juriidilise isiku vastutus

1. Liikmesriik võtab vajalikud meetmed tagamaks, et juriidilist isikut saab vastutusele võtta artiklites 3–8 nimetatud süütegude eest, mille on tema kasuks toime pannud eraisikuna või juriidilise isiku organi liikmena tegutsenud isik, kes on juriidilise isiku juures juhtival kohal ühel järgmistest alustest:

a) õigus esindada juriidilist isikut;

[7] FR, ES ja EE esitasid analüüsi reservatsiooni. LV ei saa seda ettepanekut toetada.
[8] RO esitas analüüsi reservatsiooni artikli 9 lõike 4 punkti b suhtes.

b) õigus teha juriidilise isiku nimel otsuseid;

c) õigus kontrollida juriidilist isikut.

2. Liikmesriik võtab vajalikud meetmed tagamaks, et juriidilist isikut saab vastutusele võtta juhul, kui lõikes 1 osutatud isiku järelevalve või kontrolli puudumise tõttu on osutunud võimalikuks, et kõnealuse juriidilise isiku alluvuses olev isik on tema kasuks pannud toime mõne artiklites 3–8 nimetatud süüteo.

3. Juriidilise isiku lõigete 1 ja 2 kohane vastutus ei vabasta kriminaalmenetlusest füüsilist isikut, kes on mõne artiklites 3–8 nimetatud süüteo täideviija, sellele kihutaja või sellele kaasaaitaja.

Artikkel 12

Juriidilise isiku suhtes kohaldatavad karistused

1. Liikmesriik võtab vajalikud meetmed tagamaks, et artikli 11 lõike 1 kohaselt vastutusele võetud juriidilise isiku suhtes kohaldatakse tõhusaid, proportsionaalseid ja hoiatavaid karistusi, mille hulka kuuluvad kriminaalõiguslikud ja muud trahvid ning võivad kuuluda muud sanktsioonid, näiteks:
   a) riiklike hüvitiste või abi saamise õigusest ilmajätmine;
   b) ajutine või alaline ettevõtluskeeld;
   c) kohtuliku järelevalve alla võtmine;
   d) sundlõpetamine;
   e) süüteo toimepanekuks kasutatud üksuste ajutine või lõplik sulgemine.
2. Liikmesriik võtab vajalikud meetmed tagamaks, et artikli 11 lõike 2 kohaselt vastutusele võetud juriidilise isiku suhtes kohaldatakse tõhusaid, proportsionaalseid ja hoiatavaid karistusi ning meetmeid.

Artikkel 13
Jurisdiktsioon[9]

1. Liikmesriik kehtestab oma jurisdiktsiooni artiklites 3–8 nimetatud süütegude suhtes, kui süütegu on pandud toime:

   a) osaliselt või tervikuna asjaomase liikmesriigi territooriumil või

   b) asjaomase liikmesriigi kodaniku poolt, vähemalt juhtudel, kui seda käsitatakse toimepanemise asukohas kuriteona.

2. Jurisdiktsiooni kehtestamisel kooskõlas lõike 1 punktiga a tagab liikmesriik, et jurisdiktsioon hõlmab juhtumeid, mille puhul:

   a) teo toimepanija viibib süüteo toimepanemise ajal füüsiliselt asjaomase liikmesriigi territooriumil, olenemata sellest, kas süütegu on suunatud selle liikmesriigi territooriumil asuva infosüsteemi vastu või mitte, või

   b) süütegu on suunatud asjaomase liikmesriigi territooriumil asuva infosüsteemi vastu, olenemata sellest, kas teo toimepanija viibib süüteo toimepanemise ajal selle liikmesriigi territooriumil.

3. Liikmesriik teatab komisjonile, kui ta otsustab kehtestada täiendava jurisdiktsiooni artiklites 3–8 osutatud süüteo suhtes, mis pannakse toime väljaspool tema territooriumi, näiteks kui:

   a) süüteo toimepanija peamine elukoht asub selle liikmesriigi territooriumil või

   b) süütegu on toime pandud selle liikmesriigi territooriumil asutatud juriidilise isiku kasuks.

[9] UK säilitab analüüsi reservatsiooni selle artikli suhtes.

Artikkel 14

Teabevahetus[10]

1. Liikmesriik kasutab artiklites 3–8 nimetatud süütegudega seotud teabe vahetamiseks operatiivsete kontaktpunktide võrgustikku, mis on tema käsutuses seitse päeva nädalas ööpäev läbi. Samuti tagab liikmesriik menetlused, mis võimaldavad tal kiireloomuliste taotluste puhul teatada hiljemalt kaheksa tunni jooksul vähemalt seda, kas abitaotlusele vastatakse, samuti teatada selle vastuse vormi ja eeldatava vastamise aja.

2. Liikmesriik teatab komisjonile oma määratud kontaktpunktist, mille kaudu vahetatakse artiklites 3–8 nimetatud süütegude alast teavet. Komisjon edastab selle teabe teistele liikmesriikidele.

Artikkel 15

Järelevalve ja statistika[11]

1. Liikmesriik tagab süsteemi artiklites 3–7 nimetatud süütegusid käsitlevate statistiliste andmete salvestamiseks, koostamiseks ja esitamiseks.

2. Lõikes 1 nimetatud statistika hõlmab vähemalt olemasolevaid andmeid liikmesriikide poolt registreeritud, artiklites 3–7 nimetatud süütegude arvu kohta ja selliste isikute arvu kohta, kellele on esitatud süüdistus ja kes on artiklites 3–7 nimetatud süütegude eest süüdi mõistetud.

3. Liikmesriik edastab käesoleva artikli kohaselt kogutud andmed komisjonile. Komisjon tagab statistiliste aruannete koondülevaate avaldamise.

---

10 ES esitas analüüsi reservatsiooni.

11 ES esitas analüüsi reservatsiooni.

Artikkel 16

Raamotsuse 2005/222/JSK asendamine[12]

Raamotsus 2005/222/JSK asendatakse käesoleva direktiivi vastuvõtmises osalevate liikmesriikide suhtes, ilma et see piiraks liikmesriigi kohustusi, mis on seotud raamotsuse liikmesriigi õigusesse ülevõtmise tähtajaga.

Käesoleva direktiivi vastuvõtmises osalevate liikmesriikide suhtes tõlgendatakse viiteid raamotsusele 2005/222/JSK viidetena käesolevale direktiivile.

Artikkel 17

Liikmesriigi õigusesse ülevõtmine

1. Liikmesriik jõustab käesoleva direktiivi järgimiseks vajalikud õigus- ja haldusnormid [kahe aasta jooksul alates direktiivi vastuvõtmisest].

2. Liikmesriigid edastavad komisjonile sätete teksti, millega võetakse riiklikku õigusse üle käesolevast direktiivist tulenevad kohustused.

3. Kui liikmesriigid need meetmed vastu võtavad, lisavad nad nendesse meetmetesse või nende meetmete ametliku avaldamise korral nende juurde viite käesolevale direktiivile. Sellise viitamise viisi näevad ette liikmesriigid.

Artikkel 18

Aruandlus

1. Komisjon esitab [NELJA AASTA JOOKSUL ALATES DIREKTIIVI VASTUVÕTMISEST] Euroopa Parlamendile ja nõukogule aruande, milles hinnatakse, millises ulatuses on liikmesriigid võtnud käesoleva direktiivi järgimiseks vajalikke meetmeid, ning millele vajaduse korral lisatakse seadusandlikke ettepanekuid.

(…)

[12] UK säilitab oma analüüsi reservatsiooni.

Artikkel 19

Jõustumine

Käesolev direktiiv jõustub selle *Euroopa Liidu Teatajas* avaldamise päeval.

Artikkel 20

Adressaadid

Käesolev direktiiv on vastavalt aluslepingutele adresseeritud liikmesriikidele.

Brüssel,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*