EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV 2013/40/EL,

12. august 2013,

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,

olles edastanud seadusandliku akti eelnõu liikmesriikide parlamentidele,

võttes arvesse Euroopa Majandus- ja Sotsiaalkomitee arvamust [1],

toimides seadusandliku tavamenetluse kohaselt [2]

ning arvestades järgmist:

(1) Käesoleva direktiivi eesmärkideks on ühtlustada liikmesriikide kriminaalõigust infosüsteemide vastu suunatud rünnete valdkonnas, kehtestada miinimumeeskirjad kuritegude määratlemise ja asjakohaste sanktsioonide kohta ning tõhustada koostööd pädevate asutuste, sealhulgas liikmesriikide politsei- ja muude spetsialiseeritud õiguskaitseasutuste ning liidu pädevate spetsialiseeritud asutuste ja organite (näiteks Eurojust, Europol, Europolis asuv ELi küberkuritegevuse keskus ning Euroopa Võrgu- ja Infoturbeamet (ENISA)) vahel.

(2) Infosüsteemid on liidu poliitilise, sotsiaalse ja majandusliku koostoimimise oluline osa. Ühiskond sõltub sellistest süsteemidest suurel määral ja üha enam. Kõnealuste süsteemide tõrgeteta toimimine ja turvalisus liidus on siseturu ning konkurentsivõimelise ja innovaatilise majanduse arengu seisukohalt äärmiselt oluline. Infosüsteemide kaitse asjakohase taseme tagamine peaks olema osa tulemuslikust ja terviklikust ennetusmeetmete raamistikust, mis toetab kriminaalõiguslikku reageerimist küberkuritegevusele.

(3) Infosüsteemide vastu suunatud, eelkõige organiseeritud kuritegevusega seonduvate rünnete oht nii liidus kui ka kogu maailmas aina suureneb ning seega mure infosüsteemide kui liikmesriikide ja liidu elutähtsa infrastruktuuri osa vastu suunatud võimalike terrori- või poliitiliselt ajendatud rünnakute pärast kasvab. See ohustab nii infoühiskonna turvalisemaks muutmist kui ka vabadusel, turvalisusel ja õigusel rajaneva ala saavutamist ning nõuab seega liidu tasandi meedet ning tõhusamat koostööd ja koordineerimist rahvusvahelisel tasandil.

(4) Liidus on hulk elutähtsaid infrastruktuure, mille kahjustada saamisel või hävimisel oleks olulised piiriülesed mõjud. Vajadusest suurendada liidus elutähtsate infrastruktuuride kaitsevõimet on muutunud ilmseks, et küberrünnakute vastaseid meetmeid tuleks täiendada rangete kriminaalkaristustega, mis kajastavad selliste rünnakute raskusastet. Elutähtsa infrastruktuurina võib käsitada liikmesriikides asuvat vara, süsteemi või selle osa (näiteks elektrijaamad, transpordivõrgud ja valitsusvõrgud), mis on hädavajalik eluliselt tähtsate ühiskondlike toimingute, rahvatervise, turvalisuse, julgeoleku, majandusliku ja sotsiaalse heaolu toimimiseks ning mille kahjustada saamine või hävimine mõjutaks nimetatud funktsioonide häirumise tulemusena oluliselt liikmesriiki.

(5) On tõendeid, et üha ohtlikumaid ja korduvaid suuremahulisi küberründeid suunatakse järjest enam infosüsteemide vastu, mis on sageli liikmesriikidele või avaliku või erasektori toimimise seisukohalt äärmiselt olulised. Selle tendentsiga kaasneb üha keerukamate meetodite arendamine, nagu näiteks nn robotivõrkude loomine ja kasutamine, mis hõlmab kuriteo mitmeid etappe, mis ka eraldiseisvalt kujutavad endast tõsist riski üldistele huvidele. Käesoleva direktiivi üheks eesmärgiks on kehtestada kriminaalkaristused seoses „robotivõrgu" loomisega, kus luuakse kaugkontroll märkimisväärse arvu arvutite üle sel teel, et nakatatakse eesmärgipäraste küberrünnakute abil kõnealused arvutid kurivaraga. Pärast „robotivõrgu" loomist saab moodustuva nakatatud arvutite võrgu aktiveerida arvutikasutaja teadmata, et panna toime suuremahulise küberrünnaku, mis üldjuhul võib põhjustada suurt kahju, nagu sellele on osutatud käesolevas direktiivis. Liikmesriikidel peaks vastavalt oma riiklikule õigusele ja praktikale olema võimalik määratleda suure kahju mõiste, nagu märkimisväärse tähtsusega avalike teenuste osutamise häirimine või suure rahalise kahju või isikuandmete või tundliku teabe kaotsimineku põhjustamine.

(6) Suuremahulised küberründed võivad tekitada märkimisväärset majanduslikku kahju nii infosüsteemide ja sidevõrkude töö katkemise kui ka oluliste ärialaste salajaste andmete või muude andmete kadumise või muutumise näol. Erilist tähelepanu tuleks pöörata suuremahuliste küberrünnetega seonduvate ohtude alase teadlikkuse suurendamisele uuenduslike väike- ja keskmise suurusega ettevõtjate seas, kelle sõltuvus infosüsteemide nõuetekohasest toimimisest ja kättesaadavusest on suurem ning kellel on sageli vähem võimalusi panustada infoturbesse, ja nende nõrkade kohtade kohta selliste küberrünnetega seoses.

[1] ELT C 218, 23.7.2011, lk 130.

[2] Euroopa Parlamendi 4. juuli 2013. aasta seisukoht (*Euroopa Liidu Teatajas* seni avaldamata) ja nõukogu 22. juuli 2013. aasta otsus.

(7) Ühised eeskirjad selles valdkonnas on olulised tagamaks liikmesriikides järjekindlat lähenemisviisi käesoleva direktiivi kohaldamisel.

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

(9) Pealtkuulamine hõlmab teabe sisu kuulamist, jälgimist või seiret ning andmete sisu hankimist kas vahetult – infosüsteemidesse sisenemise ja nende kasutamise teel – või kaudselt – tehniliste vahendite abil elektrooniliste pealtkuulamisseadmete kasutamise teel –, kuid ei pea tingimata eeltooduga piirduma.

(10) Liikmesriigid peaksid kehtestama karistused infosüsteemide vastu suunatud rünnete eest. Need karistused peaksid olema tõhusad, proportsionaalsed ja hoiatavad ning peaksid hõlmama vabadusekaotust ja/või rahalisi karistusi.

(11) Käesoleva direktiiviga sätestatakse kriminaalkaristused vähemalt oluliste juhtumite puhul. Liikmesriikidel peaks olema vastavalt oma riiklikule õigusele ja praktikale võimalik määratleda vähem olulise juhtumi mõiste. Juhtumit võidakse käsitada vähem olulisena näiteks siis, kui kuriteoga põhjustatud kahju ja/või oht avalikele või erahuvidele, näiteks arvutisüsteemi või arvutiandmete puutumatusele, või isiku puutumatusele, õigustele või muudele huvidele, ei ole märkimisväärne või ei ole sellise iseloomuga, et kriminaalkaristuse kohaldamine õigusaktidega sätestatud piirmäärade raames või kriminaalvastutuse kohaldamine oleks vajalik.

(12) Küberrünnakutest tulenevate ohtude ja riskide ning nendega seonduvate infosüsteemide nõrkade kohtade identifitseerimine ja nendest teatamine on oluline osa tulemuslikust küberrünnakute ärahoidmisest ja neile reageerimisest ning infosüsteemide küberturbe parandamisest. Kõnealuse eesmärgi saavutamiseks võiks anda stiimuleid turvaaukudest teatamiseks. Liikmesriigid peaksid püüdma luua võimalusi turvaaukude seaduslikuks tuvastamiseks ja nendest teatamiseks.

(13) 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), [1] kui küberrünne on suuremahuline ja mõjutab märkimisväärset arvu infosüsteeme, sealhulgas kui selle eesmärgiks on luua „robotivõrk", või kui küberrünne põhjustab suurt kahju, sealhulgas kui see pannakse toime „robotivõrgu" abil. Samuti on asjakohane näha ette keskmisest rangemad karistused juhuks, kui selline rünne on suunatud liikmesriikide või liidu elutähtsa infrastruktuuri vastu.

(14) Küberkuritegevuse vastase võitluse integreeritud lähenemisviisi täiendavaks oluliseks elemendiks on tõhusate meetmete kehtestamine identiteedivarguse ja teiste identiteediga seonduvate kuritegude vastu. Kõnealuse kriminaalse käitumise suhtes liidu tasandil meetmete võtmise vajadust tuleks samuti analüüsida ulatusliku horisontaalse liidu vahendi loomise vajaduse hindamise kontekstis.

(15) Nõukogu 27.–28. novembri 2008. aasta järeldustes märgiti, et liikmesriigid ja komisjon peaksid välja töötama uue strateegia, võttes arvesse Euroopa Nõukogu 2001. aasta küberkuritegevuse konventsiooni. Nimetatud konventsiooniga on kehtestatud küberkuritegevuse, sealhulgas infosüsteemide vastu suunatud rünnete vastase võitluse õiguslik raamistik. Käesolev direktiiv tugineb nimetatud konventsioonile. Tuleks pidada esmatähtsaks, et kõik liikmesriigid viiksid võimalikult kiiresti lõpule konventsiooni ratifitseerimise protsessi.

(16) 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. Nende vahendite all mõistetakse näiteks kurivara, sealhulgas sellist kurivara, mille abil on võimalik luua robotivõrke, mida kasutatakse küberrünnete toimepanemiseks. Juhul kui selline vahend on käesolevas direktiivis sätestatud kuritegude toimepanemiseks sobiv või eriti sobiv, võib ta siiski olla toodetud õiguspärasel eesmärgil. Et vältida kriminaliseerimist juhul, kui sellised vahendid on toodetud ja turule viidud õiguspärastel eesmärkidel, näiteks infotehnoloogiatoodete usaldusväärsuse või infosüsteemide turvalisuse testimiseks, ei ole piisav, kui isikul on üldine kavatsus, tal peab olema otsene tahtlus kasutada neid vahendeid ühe või mitme käesolevas direktiivis sätestatud kuriteo toimepanemiseks.

(17) Käesoleva direktiiviga ei nähta ette kriminaalvastutust juhul, kui on täidetud käesolevas direktiivis loetletud kuritegude objektiivsed kriteeriumid, kuid tegu on sooritatud kuritegeliku kavatsuseta, näiteks kui isik ei ole teadlik, et infosüsteemi sisenemine ei ole lubatud, või infosüsteemide volitatud testimise või kaitsmise korral, näiteks kui ettevõte või müüja on teinud isikule ülesandeks testida oma turbesüsteemi tugevust. Käesoleva direktiiviga ei nähta ette kriminaalvastutust, mis tuleneks lepingulistest kohustustest või kokkulepetest infosüsteemidesse sisenemise piiramiseks kasutajapoliitika või teenuste tingimuste abil või töövaidlustest, mis tulenevad tööandja infosüsteemidesse sisenemisest ja nende kasutamisest eraotstarbel, ning tekiks juhul kui sellistele tingimustele vastavat sisenemist käsitatakse mittelubatuna, mis oleks ka kriminaalmenetluse alustamise ainus alus. Käesoleva direktiiviga ei piirata siseriiklike ja liidu õigusaktidega sätestatud juurdepääsuõigust teabele, samas ei saa direktiivi käsitada õigustusena ebaseaduslikule või omavolilisele juurdepääsule teabele.

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

(18) Küberrünnakuid võivad hõlbustada erinevad asjaolud, näiteks kui kuriteo toimepanijal on tööülesannete täitmisel juurdepääs mõjutatud infosüsteemidele omastele turbesüsteemidele. Selliseid asjaolusid tuleks asjakohaselt arvesse võtta siseriikliku õiguse kontekstis ja kriminaalmenetluse käigus.

(19) Liikmesriigid peaksid oma siseriiklikus õiguses nägema ette raskendavad asjaolud kooskõlas nende õigussüsteemis raskendavaid asjaolusid reguleerivate eeskirjadega. Liikmesriigid peaksid tagama, et kõnealused raskendavad asjaolud on kohtunikele kaalumiseks teada õigusrikkujatele karistuse määramisel. Kohtuniku kaalutlusõigusse jääb kõnealuste asjaolude hindamine koos konkreetse juhtumi teiste faktidega.

(20) Käesoleva direktiiviga ei sätestata tingimusi jurisdiktsiooni teostamiseks selles viidatud kuritegude üle, näiteks ohvri avaldus õigusrikkumise toimepanemise asukohas, õigusrikkumise toimepanemise asukohariigi avaldus, või asjaolu, et õigusrikkumise toimepanijale ei ole esitatud süüdistust õigusrikkumise toimepanemise asukohas.

(21) Käesoleva direktiivi raames on liikmesriigid ja kolmandad riigid ning nende avalik-õiguslikud organid jätkuvalt kohustatud täielikult tagama inimõiguste ja põhivabaduste austamise vastavalt kehtivatele liidu ja rahvusvahelistele kohustustele.

(22) Käesoleva direktiiviga tugevdatakse võrgustike, näiteks G8 või teabevahetuseks loodud Euroopa Nõukogu seitse päeva nädalas ööpäev läbi töötavate kontaktpunktide võrgustiku tähtsust. Sellised kontaktpunktid peaksid suutma anda tõhusat abi, millega lihtsustatakse näiteks olemasoleva asjakohase teabe vahetamist ja tehnilist nõustamist või õigusteabe andmist seoses infosüsteemide ja seonduvate andmetega seotud kuritegude uurimise või menetlusega, kaasates taotlevaid liikmesriike. Võrgustike sujuvaks toimimiseks peaks iga kontaktpunkt olema suuteline pidama sidet teise liikmesriigi kontaktpunktiga, tehes seda muu hulgas koolituse läbinud ja asjakohase varustusega töötajate abil. Arvestades suuremahuliste küberrünnakute 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 liikmesriik menetleb seda kiiresti ja et tagasisidet antakse kaheksa tunni jooksul.

(23) Ühelt poolt riigiasutuste ning teiselt poolt erasektori ja kodanikuühiskonna vaheline koostöö on infosüsteemide vastu suunatud rünnete vältimiseks ja nende vastu võitlemiseks väga oluline. Tõhustada ja parandada tuleb koostööd teenuseosutajate, tootjate, õiguskaitseasutuste ja kohtuorganite vahel, järgides samas täielikult õigusriigi põhimõtteid. Selline koostöö võib hõlmata teenuseosutajate poolset toetust, mida antakse, et aidata säilitada võimalikke tõendeid, anda õigusrikkumise toimepanijate tuvastamisele kaasa aitavat teavet ning viimase võimalusena, et täielikult või osaliselt sulgeda või lõpetada infosüsteemid või funktsioonid, mis on kas nakatatud või mida on kasutatud ebaseaduslikel eesmärkidel, tehes seda kooskõlas siseriikliku õiguse ja tavadega. Liikmesriigid peaksid samuti kaaluma koostöö- ja partnerlusvõrgustike loomist teenuseosutajate ja tootjatega, et vahetada teavet, mis seondub käesoleva direktiivi reguleerimisalasse kuuluvate kuritegudega.

(24) Olemas on vajadus koguda võrreldavaid andmeid käesolevas direktiivis osutatud kuritegude kohta. Selleks et saada parem ülevaade küberkuritegevuse probleemist ning võrgu- ja infoturbe olukorrast liidus ning aidata seeläbi kaasa senisest tõhusamate lahenduste väljatöötamisele, tuleks pädevatele spetsialiseeritud liidu asutustele, näiteks Europolile ja ENISA-le, edastada asjakohane teave, võttes arvesse nende ülesandeid ja teabevajadusi. Liikmesriigid peaksid Europolile ja Europolis asuvale ELi küberkuritegevuse keskusele edastama teavet õigusrikkumiste toimepanijate töömeetodite kohta, et viia läbi küberkuritegevuse ohtude hindamised ja strateegilised analüüsid vastavalt nõukogu 6. aprilli 2009. aasta otsusele 2009/371/JSK (millega asutatakse Euroopa Politseiamet (Europol)) [1]. Teabe edastamine võib hõlbustada teadmiste suurendamist praegustest ja tulevastest ohtudest ning seeläbi toetada otsustusprotsessi asjakohasemaks ja sihipärasemaks muutmist infosüsteemide vastu suunatud rünnete vastu võitlemise ja nende vältimise valdkonnas.

(25) Komisjon peaks esitama aruande direktiivi kohaldamise kohta ning vajalikud seadusandlikud ettepanekud, mille tõenäoliseks tulemuseks on käesoleva direktiivi reguleerimisala laienemine, võttes arvesse arenguid küberkuritegevuse valdkonnas. Sellised arengud võivad hõlmata tehnoloogilist arengut, näiteks mis võimaldab tõhusamat tegevust infosüsteemide vastu suunatud rünnete tõrjumise valdkonnas või võimaldab selliseid ründeid ära hoida või viia nende mõju miinimumini. Sel eesmärgil peaks komisjon võtma arvesse olemasolevaid analüüse ja aruandeid, mille on koostanud asjaomased osapooled, eelkõige Europol ja ENISA.

(26) Tulemuslikuks võitluseks küberkuritegevuse vastu on vaja suurendada infosüsteemide vastupidavust, et neid paremini küberrünnakute vastu kaitsta, ning võtta selleks sobivad meetmed. Liikmesriigid peaksid võtma vajalikke meetmeid, et kaitsta infosüsteeme, mis on osa nende elutähtsatest infrastruktuuridest, küberrünnakute eest; kõnealuste meetmete osaks peaks olema liikmesriikide infosüsteemide ja nendega seotud andmete kaitsmine. Küberkuritegevuse vastase tulemusliku võitluse tervikliku

[1] ELT L 121, 15.5.2009, lk 37.

lähenemisviisi oluline osa on see, et juriidilised isikud tagavad infosüsteemide kaitse ja turvalisuse piisava taseme, näiteks seoses avalikult kättesaadavate elektrooniliste sideteenuste osutamisega, tehes seda kooskõlas liidu kehtivate õigusaktidega, mis käsitlevad eraelu puutumatust ja elektroonilist sidet ning andmekaitset. Tuleks tagada asjakohane kaitsetase mõistlikult tuvastatavate ohtude ja puuduste puhul, tehes seda vastavalt viimastele suundumustele konkreetsetes sektorites ning konkreetsetele andmetöötluse olukordadele. Sellise kaitse kulud ja koormus peaksid olema proportsionaalsed mõjutatud süsteemidele küberrünnaku poolt põhjustatavate tõenäoliste kahjustustega. Liikmesriike innustatakse võtma asjakohaseid meetmeid, millega kehtestatakse nende siseriiklikus õiguses vastutus, mida kohaldatakse nende juriidiliste isikute suhtes, kes ilmselgelt ei ole taganud kaitse asjakohast taset küberrünnakute eest.

(27) Märkimisväärsed lüngad ja erinevused liikmesriikide infosüsteemide vastu suunatud rünnete valdkonna õigusaktides ja kriminaalmenetlustes 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 piiriülene mõõde, mis rõhutab kiireloomulist vajadust asjaomase valdkonna kriminaalõiguse edasise ühtlustamise järele. Lisaks sellele peaks nõukogu 30. novembri 2009. aasta raamotsuse 2009/948/JSK (kohtualluvuskonflikti vältimise ja lahendamise kohta kriminaalmenetluses) [1] nõuetekohane rakendamine ja kohaldamine hõlbustama infosüsteemide vastu suunatud rünnete eest süüdistuse esitamise kooskõlastamist. Samuti peaksid liikmesriigid koostöös liiduga püüdma parandada rahvusvahelist koostööd infosüsteemide, arvutivõrkude ja arvutiandmete turvalisuse valdkonnas. Kõikide andmevahetust käsitlevate rahvusvaheliste lepingute puhul tuleks nõuetekohaselt arvesse võtta andmete edastamise ja säilitamise turvalisust.

(28) Pädevate õiguskaitseasutuste ja kohtuorganite vahelise koostöö parandamine üle kogu liidu on ülioluline, et tulemuslikult võidelda küberkuritegevuse vastu. Selles kontekstis tuleks innustada suuremaid jõupingutusi asjakohaste asutuste piisava koolitamise alal, et suurendada küberkuritegevusest ja selle mõjust arusaamist ning tõhustada koostööd ja parimate tavade vahetamist, näiteks pädevate spetsialiseeritud liidu asutuste ja organite kaudu. Sellise koolituse eesmärgiks peaks muu hulgas olema teadlikkuse suurendamine erinevate riikide õigussüsteemidest, võimalikest eeluurimise käigus tekkida võivatest õiguslikest ja tehnilistest probleemidest ning pädevuste jaotusest asjakohaste siseriiklike asutuste vahel.

(29) Käesoleva direktiiviga austatakse inimõigusi ja põhivabadusi ning järgitakse eelkõige Euroopa Liidu põhiõiguste hartas ning Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis tunnustatud põhimõtteid, sealhulgas isikuandmete kaitset, eraelu puutumatust, 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 ja põhimõtete täielik austamine ja sellest tuleb direktiivi järgimisel ka lähtuda.

(30) Isikuandmete kaitse on ELi toimimise lepingu artikli 16 lõike 1 ja Euroopa Liidu põhiõiguste harta artikli 8 kohaselt põhiõigus. Seetõttu peab käesoleva direktiivi rakendamise raames aset leidev isikuandmete töötlemine olema täielikus vastavuses asjakohaste andmekaitsealaste liidu õigusaktidega.

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

(32) Euroopa Liidu lepingule ja Euroopa Liidu toimimise lepingule lisatud protokolli (Taani seisukoha kohta) artiklite 1 ja 2 kohaselt ei osale Taani käesoleva direktiivi vastuvõtmisel ning see ei ole tema suhtes siduv ega kohaldatav.

(33) Kuna käesoleva direktiivi eesmärke, nimelt infosüsteemide vastu suunatud rünnete eest tõhusate, proportsionaalsete ja hoiatavate kriminaalkaristuste kehtestamist kõikides liikmesriikides ning kohtuasutuste ja muude pädevate asutuste koostöö parandamist ja soodustamist, ei suuda liikmesriigid piisavalt saavutada ning neid on nende ulatuse või mõju tõttu parem saavutada liidu tasandil, võib liit võtta meetmeid kooskõlas Euroopa Liidu lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega. Kõnealuses artiklis sätestatud proportsionaalsuse põhimõtte kohaselt ei lähe käesolev direktiiv nimetatud eesmärkide saavutamiseks vajalikust kaugemale.

(34) Käesoleva direktiivi eesmärk on muuta ja laiendada nõukogu 24. veebruari 2005. aasta raamotsuse 2005/222/JSK (infosüsteemide vastu suunatud rünnete kohta) [2] sätteid. Kuna tehtavad muudatused on arvukad ja sisulised, siis tuleks raamotsus 2005/222/JSK selguse huvides täielikult asendada käesoleva direktiivi vastuvõtmises osalevate liikmesriikide suhtes,

[1] ELT L 328, 15.12.2009, lk 42.

[2] ELT L 69, 16.3.2005, lk 67.

ON VASTU VÕTNUD KÄESOLEVA DIREKTIIVI:

Artikkel 1

Sisu

Käesoleva direktiiviga kehtestatakse miinimumeeskirjad infosüsteemide vastu suunatud rünnete valdkonna kriminaalkuritegude ja karistuste määratlemise kohta. Samuti on direktiivi eesmärk hõlbustada selliste kuritegude ärahoidmist ja arendada koostööd kohtuorganite 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 töötlevad vastavalt programmile automaatselt arvutiandmeid; samuti nimetatud seadme või seadmete rühma salvestatud, töödeldud, välja võetud või 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 liikmesriigid, kolmandad riigid või riigivõimu teostavad avalik-õiguslikud asutused või avalik-õiguslikud rahvusvahelised organisatsioonid;

d) „õigusliku aluseta" – toiming, mis ei ole lubatud süsteemi või selle osa omaniku või selle suhtes muu õiguse valdaja poolt, või millega rikutakse riiklikke õigusakte.

Artikkel 3

Ebaseaduslik sisenemine infosüsteemi

Liikmesriik võtab vajalikud meetmed tagamaks, et tahtlikult ja õigusliku aluseta sisenemine infosüsteemi või selle osasse, kui selline sisenemine rikub mõnda turvameedet, on vähemalt raskemate juhtumite puhul kriminaalkorras karistatav.

Artikkel 4

Ebaseaduslik süsteemi häirimine

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

Artikkel 5

Ebaseaduslik andmetesse sekkumine

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

Artikkel 6

Teabe ebaseaduslik pealtkuulamine

Liikmesriik võtab vajalikud meetmed tagamaks, et infosüsteemi, sellest infosüsteemist või selle infosüsteemi piires, sealhulgas infosüsteemi elektromagnetkiirguse abil mitteavalikult edastatavate arvutiandmete tahtlik ja õigusliku aluseta pealtkuulamine tehniliste vahendite abil on vähemalt raskemate juhtumite puhul kriminaalkorras karistatav.

Artikkel 7

Kuriteo toimepanemisel kasutatud vahendid

Liikmesriik võtab vajalikud meetmed tagamaks, et järgmiste seadmete tahtlik tootmine, müük, kasutamiseks hankimine, importimine, levitamine või muul viisil kättesaadavaks tegemine õigusliku aluseta ja kavatsusega kasutada seda eesmärgiga panna toime mõni artiklites 3–6 osutatud kuritegu, on vähemalt raskemate juhtumite puhul kriminaalkorras karistatav:

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

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

Artikkel 8

Kuriteole kihutamine, kaasaaitamine ja kuriteokatse

1. Liikmesriik tagab, et artiklites 3–7 osutatud kuritegude toimepanemisele kihutamine või kaasaaitamine on kriminaalkorras karistatav.

2. Liikmesriik tagab, et artiklites 4 ja 5 osutatud kuriteokatse on kriminaalkorras karistatav.

Artikkel 9

Karistused

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

2. Liikmesriik võtab vajalikud meetmed tagamaks, et artiklites 3–7 osutatud kuritegude eest määratakse karistus, mille maksimummäär on vähemalt kaheaastane vangistus, seda vähemalt raskemate juhtumite puhul.

3. Liikmesriik võtab vajalikud meetmed tagamaks, et artiklites 4 ja 5 osutatud kuritegude tahtliku toimepanemise eest määratakse karistus, mille maksimummäär on vähemalt kolmeaastane vangistus, kui arvestatavat hulka infosüsteeme on

mõjutatud sellise artiklis 7 osutatud vahendi kasutamise teel, mis on loodud või kohandatud eelkõige kuriteo toimepanemiseks.

4. Liikmesriik võtab vajalikud meetmed tagamaks, et artiklites 4 ja 5 osutatud kuritegude eest määratakse karistus, mille maksimummäär on vähemalt viieaastane vangistus, kui

a) need on toime pandud raamotsuses 2008/841/JSK määratletud kuritegeliku ühenduse raames, sõltumata selles sätestatud karistusmäärast;

b) need põhjustavad rasket kahju või

c) need on toime pandud elutähtsa infrastruktuuri infosüsteemi vastu.

5. Liikmesriik võtab vajalikud meetmed tagamaks, et kui artiklites 4 ja 5 osutatud kuriteod pannakse toime teise isiku isikuandmete väärkasutamise teel, eesmärgiga võita kolmanda isiku usaldus, ning tekitatakse seeläbi kahju tegeliku identiteedi omanikule, võib seda siseriikliku õiguse kohaselt käsitada raskendava asjaoluna, välja arvatud juhul, kui need asjaolud kuuluvad teise siseriikliku õiguse alusel karistatava kuriteo koosseisu.

Artikkel 10

Juriidilise isiku vastutus

1. Liikmesriik võtab vajalikud meetmed tagamaks, et juriidilist isikut saab vastutusele võtta artiklites 3–8 osutatud kuritegude 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;

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 puudumine võimaldas kõnealuse juriidilise isiku alluvuses oleval isikul panna tema kasuks toime mõne artiklites 3–8 osutatud kuriteo.

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

Artikkel 11

Juriidilise isiku suhtes kohaldatavad karistused

1. Liikmesriik võtab vajalikud meetmed tagamaks, et artikli 10 lõike 1 kohaselt vastutusele võetud juriidilise isiku suhtes kohaldatakse tõhusaid, proportsionaalseid ja hoiatavaid karistusi, mille hulka kuuluvad kriminaalõiguslikud või muud trahvid ning võivad kuuluda näiteks:

a) riiklike hüvitiste või abi saamise õigusest ilmajätmine;

b) ajutine või alaline ettevõtluskeeld;

c) kohtuliku järelevalve alla võtmine;

d) sundlõpetamine;

e) kuriteo toimepanekuks kasutatud üksuste ajutine või lõplik sulgemine.

2. Liikmesriik võtab vajalikud meetmed tagamaks, et artikli 10 lõike 2 kohaselt vastutusele võetud juriidilise isiku suhtes kohaldatakse tõhusaid, proportsionaalseid ja hoiatavaid karistusi või muid meetmeid.

Artikkel 12

Jurisdiktsioon

1. Liikmesriik kehtestab oma jurisdiktsiooni artiklites 3–8 osutatud kuritegude suhtes, kui kuritegu on pandud toime:

a) osaliselt või tervikuna tema 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 tal on jurisdiktsioon, kui

a) teo toimepanija viibib kuriteo toimepanemise ajal füüsiliselt tema territooriumil, olenemata sellest, kas kuritegu on suunatud selle liikmesriigi territooriumil asuva infosüsteemi vastu või mitte, või

b) kuritegu on suunatud tema territooriumil asuva infosüsteemi vastu, olenemata sellest, kas teo toimepanija viibib kuriteo toimepanemise ajal selle liikmesriigi territooriumil või mitte.

3. Liikmesriik teatab komisjonile, kui ta otsustab kehtestada jurisdiktsiooni artiklites 3–8 osutatud kuriteo suhtes, mis pannakse toime väljaspool tema territooriumi, sealhulgas kui

a) kuriteo toimepanija peamine elukoht asub tema territooriumil või

b) kuritegu on toime pandud tema territooriumil asutatud juriidilise isiku kasuks.

Artikkel 13

Teabevahetus

1. Liikmesriik tagab, et artiklites 3–8 osutatud kuritegudega seotud teabe vahetamiseks on liikmesriigis olemas toimiv riiklik kontaktpunkt ning et liikmesriik kasutab olemasolevat operatiivsete kontaktpunktide võrgustikku, mis töötab seitse päeva nädalas ööpäev läbi. Samuti tagab liikmesriik menetlused, mis võimaldavad pädeval asutusel kiireloomuliste abitaotluste puhul teatada hiljemalt kaheksa tunni jooksul taotluse kättesaamisest vähemalt seda, kas abitaotlusele vastatakse, ning selle vastuse vormi ja eeldatava vastamise aja.

2. Liikmesriik teatab komisjonile oma määratud lõikes 1 osutatud kontaktpunktist. Komisjon edastab selle teabe teistele liikmesriikidele ning liidu pädevatele spetsialiseeritud asutustele ja organitele.

3. Liikmesriik võtab vajalikud meetmed, millega tagatakse asjakohaste aruandlusmooduste olemasolu, millega lihtsustatakse artiklites 3–6 osutatud kuritegude kohta aruannete esitamist pädevatele siseriiklikele asutustele põhjendamatu viivituseta.

Artikkel 14

Järelevalve ja statistika

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

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

3. Liikmesriik edastab käesoleva artikli kohaselt kogutud andmed komisjonile. Komisjon tagab statistiliste aruannete koondülevaate avaldamise ja esitamise liidu pädevatele spetsialiseeritud asutustele ja organitele.

Artikkel 15

Raamotsuse 2005/222/JSK asendamine

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

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

Artikkel 16

Liikmesriigi õigusesse ülevõtmine

1. Liikmesriik jõustab käesoleva direktiivi järgimiseks vajalikud õigus- ja haldusnormid hiljemalt 4. septembriks 2015.

2. Liikmesriigid edastavad komisjonile meetmete 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 17

Aruandlus

Komisjon esitab hiljemalt 4. septembriks 2017 Euroopa Parlamendile ja nõukogule aruande, milles hinnatakse, millises ulatuses on liikmesriigid võtnud käesoleva direktiivi järgimiseks vajalikke meetmeid, ning millele vajaduse korral lisatakse seadusandlikud ettepanekud. Komisjon võtab ka arvesse tehnilisi ja õiguslikke arenguid küberkuritegevuse valdkonnas, eelkõige käesoleva direktiivi reguleerimisala osas.

Artikkel 18

Jõustumine

Käesolev direktiiv jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas.*

Artikkel 19

Adressaadid

Käesolev direktiiv on adresseeritud liikmesriikidele kooskõlas aluslepingutega.

Brüssel, 12. august 2013

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*
M. SCHULZ	L. LINKEVIČIUS