

## EIROPAS PARLAMENTA UN PADOMES DIREKTĪVA 2013/40/ES

(2013. gada 12. augusts)

## par uzbrukumiem informācijas sistēmām, un ar kuru aizstāj Padomes Pamatlēmumu 2005/222/TI

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 83. panta 1. punktu,

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu <sup>(1)</sup>,

saskaņā ar parasto likumdošanas procedūru <sup>(2)</sup>,

tā kā:

- (1) Šīs direktīvas mērķi ir tuvināt dalībvalstu krimināltiesības attiecībā uz uzbrukumiem informācijas sistēmām, ieviešot minimālos noteikumus attiecībā uz noziedzīgu nodarījumu definēšanu un attiecīgām sankcijām, un uzlabot sadarbību starp kompetentajām iestādēm, tostarp dalībvalstu policijas un citiem specializētiem tiesībsardzības dienestiem, kā arī kompetentajām specializētajām Savienības aģentūrām un struktūrām, piemēram, Eurojust, Eiropu un tā Eiropas kibernetizācijas centru un Eiropas Tīklu un informācijas drošības aģentūru (ENISA).
- (2) Informācijas sistēmas ir būtisks elements Savienības politiskajā, sociālajā un ekonomiskajā mijiedarbībā. Sabiedrība ir lielā mērā atkarīga no šādām sistēmām, un šī atkarība arvien palielinās. Minēto sistēmu netraucēta darbība un drošība Savienībā ir ārkārtīgi svarīga iekšējā tirgus un konkurētspējīgas un inovatīvas ekonomikas attīstībai. Informācijas sistēmu pienācīga līmeņa aizsardzības nodrošināšanai vajadzētu būt tādu preventīvu pasākumu iedarbīgas kompleksas sistēmas sastāvdaļai, ar kuriem papildina krimināltiesisku vēršanos pret kibernetizāciju.
- (3) Uzbrukumu informācijas sistēmām un, jo īpaši uzbrukumam, kas saistīti ar organizētu noziedzību, draudi gan Savienības, gan pasaules mērogā, kā arī bažas par iespējamajiem teroristiskiem vai politiski motivētiem uzbrukumiem informācijas sistēmām, kas ir dalībvalstu un Savienības kritiskās infrastruktūras sastāvdaļa, arvien pieaug. Tas apdraud drošākas informācijas sabiedrības un brīvī-

bas, drošības un tiesiskuma telpas izveidi, un tāpēc ir jārikojas Savienības līmenī un jāuzlabo sadarbība un koordinācija starptautiskā līmenī.

- (4) Savienībā atrodas virkne kritisku infrastruktūru, kuru darbības pārtraukšanai vai iznīcināšanai būtu nopietna pārrobežu ietekme. Ņemot vērā nepieciešamību palielināt kritiskās infrastruktūras aizsardzības spējas Savienībā, kļuvis acīmredzams, ka pasākumi pret kibernetizācijas uzbrukumiem būtu jāpapildina ar stingriem kriminālsodiem, kas būtu atbilstīgi šādu uzbrukumu smagumam. Par kritiskām infrastruktūrām varētu uzskatīt objektus, sistēmas vai to daļas, kas ir izvietotas dalībvalstīs un kas ir būtiskas svarīgu sabiedrības funkciju uzturēšanai, veselības, drošuma, drošības, saimnieciskās vai sociālās labklājības nodrošināšanai, piemēram, spēkstacijas, transporta tīkli vai valdības tīkli, un kuru darbības pārtraukšana vai kuru iznīcināšana nopietni ietekmētu dalībvalsti, jo būtu traucēta turpmāka minēto funkciju izpilde.

- (5) Ir vērojama tendence, ka plaša mēroga uzbrukumi informācijas sistēmām, kas bieži var būt kritiski svarīgas dalībvalstīm vai atsevišķām publiskā vai privātā sektora funkcijām, kļūst aizvien bīstamāki un atkarīgas aizvien biežāk. Līdztekus šai tendencei ir konstatējama arvien sarežģītāku metožu attīstība, piemēram, tā saukto "robot-tīklu" ("botnets") izveide un izmantošana, kurā noziedzīgai darbībai ir vairāki posmi un kurā katrs posms atsevišķi varētu radīt nopietnu risku sabiedrības interesēm. Šajā direktīvā *inter alia* ir paredzēts noteikt kriminālsodus par "robot-tīkla" izveidošanu, proti, ievērojama skaita datoru tālvadības iespējas iegūšanu, ar mērķtiecīgiem kibernetizācijas uzbrukumiem inficējot tos ar ļaunprātīgu programmatūru. Kad tas ir izveidots, inficēto datoru tīklu, kas veido "robot-tīklu", var aktivizēt bez datoru lietotāju ziņas, lai izraisītu plaša mēroga kibernetizācijas uzbrukumu, kurš parasti ir pietiekami spēcīgs, lai radītu nopietnu kaitējumu, kā minēts šajā direktīvā. Dalībvalstis saskaņā ar saviem tiesību aktiem un praksi var noteikt, kas ir nopietns kaitējums, piemēram, traucējumu radīšana sabiedrībai ļoti svarīgos sistēmas pakalpojumos vai lielu finansiālu izmaksu radīšana vai personas datu vai sensitīvas informācijas zaudēšana.

- (6) Plaša mēroga kibernetizācijas uzbrukumi var izraisīt ievērojamu ekonomisku kaitējumu gan informācijas sistēmu darbības un sakaru pārtraukumu, gan komerciāli svarīgas konfidencialas informācijas vai citu datu zaudēšanas vai izmaiņšanas rezultātā. Īpaša uzmanība būtu jāpievērš novatorisku mazo un vidējo uzņēmumu izpratnes uzlabošanai par draudiem, kas saistīti ar šādiem uzbrukumiem, un to neaizsargātību pret šādiem uzbrukumiem, jo tie arvien vairāk ir atkarīgi no informācijas sistēmu pareizas darbības un pieejamības un tiem bieži vien ir ierobežoti resursi informācijas drošībai.

<sup>(1)</sup> OV C 218, 23.7.2011., 130. lpp.

<sup>(2)</sup> Eiropas Parlamenta 2013. gada 4. jūlija nostāja (Oficiālajā Vēstnesī vēl nav publicēta) un Padomes 2013. gada 22. jūlija lēmums.

- (7) Lai nodrošinātu saskaņotu pieeju šīs direktīvas piemērošanai dalībvalstīs, šajā jomā ir svarīgas vienotas definīcijas.
- (8) Ir jāpanāk kopīga pieeja noziedzīgu nodarījumu sastāvdalīšanai, ieviešot vienotus noziedzīgu nodarījumu sastāvu attiecībā uz nelikumīgu piekļuvi informācijas sistēmām, nelikumīgu iejaukšanos sistēmā, nelikumīgu iejaukšanos datus un nelikumīgu pārtveršanu.
- (9) Pārtveršana ietver, bet neaprobežojas ar saziņas satura noklausīšanos, uzraudzīšanu vai novērošanu, satura datu saņemšanu tiešā veidā, piekļūstot un izmantojot informācijas sistēmu, vai netieši, ar tehniskiem līdzekļiem izmantojot elektroniskas noklausīšanās vai uztveršanas ierīces.
- (10) Dalībvalstīm būtu jāparedz sodi par uzbrukumiem informācijas sistēmām. Minētajiem sodiem vajadzētu būt iedarbīgiem, samērīgiem un preventīviem, un tiem vajadzētu ietvert cietumsodu un/vai naudas sodu.
- (11) Ar šo direktīvu paredz noteikt kriminālsodus vismaz tādos gadījumos, kas nav mazsvarīgi. Katra dalībvalsts saskaņā ar saviem tiesību aktiem un praksi var noteikt, kuru pārkāpumu var uzskatīt par mazsvarīgu. Nodarījumu var uzskatīt par mazsvarīgu, piemēram, ja nodarījuma izraisītais kaitējums un/vai risks, ko tas rada publiskām vai privātām interesēm, tādām kā datortīkla vai datorizētu datu integritātei, vai personas neaizskaramībai, tiesībām vai citām personas interesēm, ir nenozīmīgs vai tāds, ka kriminālsoda piemērošana likumā paredzētajās robežās vai kriminālatbildības piemērošana nav nepieciešama.
- (12) Kiberuzbrukumu izraisītā apdraudējuma un riska, kā arī informācijas sistēmu saistītās neaizsargātības identifikācija un ziņošana par to ir būtisks elements kiberuzbrukumu efektīvā profilaksē un reaģēšanā uz tiem, kā arī informācijas sistēmu drošības uzlabošanā. Tādēļ varētu būt lietderīgi noteikt stimulus, lai ziņotu par drošības robiem. Dalībvalstīm būtu jātiecas piedāvāt šādas iespējas, lai varētu tiesiski noteikt drošības robus un ziņot par tiem.
- (13) Ir atbilstīgi noteikt bargākus sodus, ja uzbrukumu informācijas sistēmai ir veikusi noziedzīga organizācija, kā definēts Padomes Pamatlēmumā 2008/841/TI (2008. gada 24. oktobris) par cīņu pret organizēto noziedzību<sup>(1)</sup>, ja kiberuzbrukums tiek veikts plašā mērogā, tādējādi skarot būtisku skaitu informācijas sistēmu, tostarp – ja uzbrukuma mērķis ir bijis izveidot “robototiklu”, vai ja kiberuzbrukums rada nopietnu kaitējumu, tostarp – ja tas izdarīts, izmantojot “robototiklu”. Ir atbilstīgi arī noteikt bargākus sodus, ja uzbrukums ir vērst pret dalībvalsti vai Savienības kritisku infrastruktūru.
- (14) Vēl viens nozīmīgs elements integrētā pieejā kibernetizācijas apkarošanai ir efektīvu pasākumu noteikšana pret identitātes zādzību un citiem nodarījumiem saistībā ar identitāti. Novērtējot vajadzību pēc visaptveroša horizontāla Savienības instrumenta, varētu arī apsvērt, vai ir vajadzīga Savienības rīcība attiecībā uz šādu kriminālsodāmu uzvedību.
- (15) Padomes 2008. gada 27. līdz 28. novembra secinājumos ir norādīts, ka dalībvalstīm un Komisijai būtu jāizstrādā jauna stratēģija, ņemot vērā Eiropas Padomes 2001. gada Konvenciju par kibernetizāciju. Minētā konvencija ir atsaucis tiesiskais regulējums cīņai pret kibernetizāciju, tostarp uzbrukumiem informācijas sistēmām. Šī direktīva ir izstrādāta, pamatojoties uz minēto konvenciju. Par prioritāti būtu jāuzskata tas, lai visas dalībvalstis pēc iespējas ātrāk pabeigtu minētās konvencijas ratificēšanas procesu.
- (16) Ņemot vērā, ka uzbrukumus ir iespējams veikt dažādos veidos, un to, cik ātri attīstās aparatūra un programmatūra, šajā direktīvā ir atsaucis uz rīkiem, ko var izmantot šajā direktīvā izklāstīto nodarījumu izdarīšanai. Šādi rīki varētu būt ļaunprātīga programmatūra, tostarp arī tāda programmatūra, ar ko ir iespējams izveidot “robototiklus”, ko izmanto kiberuzbrukumu izdarīšanai. Pat ja šāds rīks ir piemērots vai īpaši piemērots kāda no šajā direktīvā izklāstīto nodarījumu veikšanai, ir iespējams, ka tas ir izstrādāts likumīgam mērķim. Lai izvairītos no kriminālatbildības piemērošanas gadījumos, kad šādi rīki ir izstrādāti un laisti tirgū likumīgiem mērķiem, piemēram, informācijas tehnoloģiju produktu izturības vai informācijas sistēmu drošības pārbaudēm, papildus prasībai par vispārīgu nodomu jābūt izpildītai arī prasībai par tiešu nodomu minētos rīkus izmantot, lai veiktu vienu vai vairākus no šajā direktīvā izklāstītajiem nodarījumiem.
- (17) Ar šo direktīvu nenosaka kriminālatbildību, ja objektīvie kritēriji šajā direktīvā izklāstītajiem nodarījumiem ir izpildīti, tomēr darbības ir veiktas bez noziedzīga nodoma, piemēram, ja persona nezina, ka piekļuve bija neatļauta, vai ja ir notikusi informācijas sistēmas aizsardzības pilnvarota pārbaude, piemēram, ja uzņēmums vai tirgotājs personai ir uzdevis pārbaudīt savas drošības sistēmas izturību. Saistībā ar šo direktīvu līgumiskas saistības vai vienošanās ierobežot piekļuvi informācijas sistēmām, izmantojot lietotāju politiku vai lietošanas noteikumus, kā arī darba strīdi attiecībā uz tiesībām piekļūt un izmantot darba devēja informācijas sistēmas privātiem mērķiem nedrīkstētu izraisīt kriminālatbildību, ja šādos apstākļos piekļuvi uzskatītu par neatļautu un tā tādējādi būtu vienīgais kriminālprocesa pamats. Šī direktīva neskar tiesības uz piekļuvi informācijai, kā noteikts valsts un Savienības tiesību aktos, lai gan tā nevar būt par attaisnojumu nelikumīgai vai patvaļīgai piekļuvei informācijai.

(1) OV L 300, 11.11.2008., 42. lpp.

- (18) Kiberuzbrukumu izdarīšanu varētu atvieglot dažādi apstākļi, piemēram, ja nodarījuma izdarītājam saistībā ar viņa darbu ir piekļuve drošības sistēmām, kas ir daļa no skartajām informācijas sistēmām. Ievērojot valstu tiesību aktus, šādi apstākļi būtu attiecīgi jāņem vērā kriminālprocesa gaitā.
- (19) Dalībvalstīm savos valsts tiesību aktos būtu jāparedz atbildību pastiprinoši apstākļi saskaņā ar to tiesību sistēmā noteiktajiem piemērojamiem noteikumiem par atbildību pastiprinošiem apstākļiem. Tām būtu jānodrošina, ka minētie atbildību pastiprinošie apstākļi ir pieejami tiesnešiem apsvēršanai, nosakot sodu nodarījuma izdarītājiem. Attiecībā uz minēto apstākļu izvērtēšanu kopā ar citiem konkrētās lietas faktiem tiesnesim ir rīcības brīvība.
- (20) Šajā direktīvā nereglamentē nosacījumus jurisdikcijas īstenošanai attiecībā uz jebkuru no šeit minētajiem nodarījumiem, piemēram, cietušā iesniegumu nodarījuma izdarīšanas vietā, apsūdzību no valsts, kurā nodarījums izdarīts, vai kriminālvajāšanas neveikšanu pret nodarījuma izdarītāju nodarījuma izdarīšanas vietā.
- (21) Saistībā ar šo direktīvu valstīm un to publiskām iestādēm arvien pilnā mērā ir pienākums nodrošināt cilvēktiesību un pamatbrīvību ievērošanu saskaņā ar spēkā esošajām starptautiskajām saistībām.
- (22) Šajā direktīvā ir uzsvērtā tādu tīklu nozīme kā G8 vai Eiropas Padomes kontaktpunktu tīkls, kas ir pieejami divdesmit četras stundas diennaktī, septiņas dienas nedēļā. Minētajiem kontaktpunktiem vajadzētu būt spējīgiem nodrošināt efektīvu palīdzību un tādējādi, piemēram, veicināt pieejamās attiecīgās informācijas apmaiņu vai tehnisku konsultāciju vai juridiskas informācijas sniegšanu ar nolūku veikt izmeklēšanu vai tiesvedību par noziedzīgiem nodarījumiem, kas saistīti ar informācijas sistēmām un saistītiem datiem, kas attiecas uz pieprasītāju dalībvalsti. Lai nodrošinātu tīklu netraucētu darbību, katram kontaktpunktam būtu jāspēj ātri sazināties ar citas dalībvalsts kontaktpunktu *inter alia* ar apmācīta un ekipēta personāla starpniecību. Ņemot vērā, cik ātri ir iespējams veikt plaša mēroga kiberuzbrukumus, dalībvalstīm vajadzētu būt spējīgām nekavējoties sniegt atbildi uz šī kontaktpunktu tīkla steidzamiem pieprasījumiem. Šādos gadījumos varētu būt lietderīgi, ka informācijas pieprasījumu papildina telefoniska sazināšanās, lai nodrošinātu, ka pieprasījuma saņēmēja dalībvalsts pieprasījumu apstrādā ātri un atbildi sniedz astoņās stundās.
- (23) Publisko iestāžu sadarbība savā starpā, no vienas puses, un privātais sektors un pilsoniskā sabiedrība, no otras puses, ir ļoti nozīmīga informācijas sistēmu uzbrukumu novēršanā un apkarošanā. Ir jāpastiprina un jāuzlabo sadarbība starp pakalpojumu sniedzējiem, ražotājiem, tiesībsargdzības struktūrām un tiesu iestādēm, pilnībā ievērojot tiesiskumu. Šāda sadarbība varētu ietvert pakalpojumu sniedzēju atbalstu, palīdzot saglabāt iespējamus pierādījumus, sniedzot informāciju, kas palīdzētu identificēt nodarījumu izdarītājus, un kā pēdējo līdzekli saskaņā ar valstu tiesību aktiem un praksi pilnībā vai daļēji izslēdzot informācijas sistēmas vai funkcijas, kuras tiek apdraudētas vai izmantotas nelikumīgiem mērķiem. Dalībvalstīm būtu arī jāapsver iespēja izveidot sadarbības un partnerības tīklus ar pakalpojumu sniedzējiem un ražotājiem, lai apmainītos ar informāciju saistībā ar nodarījumiem, uz kuriem attiecas šīs direktīvas darbības joma.
- (24) Ir jāvāc salīdzināmi dati par šajā direktīvā izklāstītajiem nodarījumiem. Atbilstīgi dati būtu jādara pieejami kompetentajām specializētajām Savienības aģentūrām un struktūrām, piemēram, Eiropolam un ENISA atbilstīgi to uzdevumiem un vajadzībai pēc informācijas, lai panāktu pilnīgāku izpratni par problemātiku saistībā ar kibernetizāciju un tīklu un informācijas drošību Savienības līmenī un tādējādi sekmētu efektīvākas atbildes rīcības sagatavošanu. Dalībvalstīm būtu jāiesniedz Eiropolam un tā Eiropas Kibernetizācijas centram informācija par nodarījumu izdarītāju darbības veidu, lai tie veiktu kibernetizācijas izraisīto draudu novērtējumu un stratēģisko analīzi atbilstīgi Padomes Lēmumam 2009/371/TI (2009. gada 6. aprīlis), ar ko izveido Eiropas Policijas biroju (Eiropolu) <sup>(1)</sup>. Informācijas sniegšana var sekmēt labāku izpratni par esošajiem un nākotnē gaidāmajiem draudiem un tādējādi var veicināt piemērotāku un mērķtiecīgāku lēmumu pieņemšanu par uzbrukumu informācijas sistēmām apkarošanu un novēršanu.
- (25) Komisijai būtu jāiesniedz ziņojums par šīs direktīvas piemērošanu un jānāk klajā ar visiem vajadzīgajiem likumdošanas akta priekšlikumiem, ar kuriem varētu paplašināt tās darbības jomu, ņemot vērā norises kibernetizācijas jomā. Šādas norises varētu ietvert tehnoloģiju attīstību, piemēram tādu, kuras nodrošina efektīvāku izpildi attiecībā uz uzbrukumiem informācijas sistēmām vai kuras veicina šādu uzbrukumu nepieļaušanu vai to seku mazināšanu. Tālab Komisijai būtu jāņem vērā pieejamās analīzes un ziņojumi, ko izstrādājuši atbilstīgi dalībnieki un jo īpaši Eiropols un ENISA.
- (26) Kibernetizācijas efektīvai apkarošanai jāpaliekina informācijas sistēmu izturība, veicot piemērotus pasākumus, lai tās efektīvāk aizsargātu pret kiberuzbrukumiem. Dalībvalstīm būtu jāveic vajadzīgie pasākumi to kritiskās infrastruktūras aizsardzībai pret kiberuzbrukumiem, tostarp apsverot iespēju aizsargāt savas informācijas sistēmas un saistītos datus. Svarīga kompleksas pieejas sastāvdaļa kibernetizācijas efektīvai apkarošanai ir juridisku personu rīcība, nodrošinot informācijas sistēmu aizsardzības un drošības piemērotu līmeni, piemēram,

<sup>(1)</sup> OV L 121, 15.5.2009., 37. lpp.

saistībā ar publiski pieejamu elektroniskās saziņas pakalpojumu sniegšanu atbilstīgi spēkā esošajiem Savienības tiesību aktiem par privāto dzīvi un elektroniskajiem sakariem un datu aizsardzību. Būtu jānodrošina pienācīgs aizsardzības līmenis pret iespējami identificējamiem draudiem un neaizsargātību atbilstoši augstākajam iespējamajam līmenim attiecīgajā nozarē un konkrētām datu apstrādes situācijām. Izmaksām un slogam saistībā ar šādu aizsardzību vajadzētu būt samērīgam ar iespējamo kaitējumu, ko kibernetiskie uzbrukumi izraisītu ietekmētajām personām. Dalībvalstis tiek mudinātas savos valsts tiesību aktos noteikt atbilstīgus pasākumus, paredzot atbildību gadījumos, kad juridiskā persona nepārprotami nav nodrošinājusi atbilstīga līmeņa aizsardzību pret kibernetiskajiem uzbrukumiem.

(27) Ievērojami trūkumi un atšķirības dalībvalstu tiesību aktos un kriminālprocesā, kas attiecas uz uzbrukumiem informācijas sistēmām, var kavēt organizētās noziedzības un terorisma apkarošanu un sarežģīt efektīvu policijas un tiesu iestāžu sadarbību šajā jomā. Modernās informācijas sistēmas ir starptautiskas, un uz tām neattiecas robežas, tādēļ uzbrukumiem šādām sistēmām ir pārrobežu raksturs, tādējādi izceļot to, ka ir steidzami vajadzīga turpmāka rīcība krimināltiesību tuvināšanai šajā jomā. Turklāt būtu jāuzlabo saistībā ar uzbrukumiem informācijas sistēmām īstenotā kriminālprocesa koordinācija, atbilstīgi īstenojot un piemērojot Padomes Pamatlēmumu 2009/948/TI (2009. gada 30. novembris) par jurisdikcijas īstenošanas konfliktu novēršanu un atrisināšanu kriminālprocesā <sup>(1)</sup>. Dalībvalstīm sadarbībā ar Savienību būtu arī jātiecas uzlabot starptautisku sadarbību saistībā ar informācijas sistēmu, datortīklu un datoru datu drošību. Visos starptautiskos nolīgumos, kas aptver datu apmaiņu, būtu pienācīgi jāapsver datu pārsūtīšanas un glabāšanas drošības jautājumi.

(28) Lai efektīvi apkarotu kibernetiskos uzbrukumus, ir būtiski uzlabot sadarbību starp kompetentajām tiesībsargājošajām struktūrām un tiesu iestādēm visā Savienībā. Šajā sakarā būtu jāveicina tas, ka tiek pastiprināti centieni nodrošināt atbilstīgajām iestādēm piemērotu apmācību, lai uzlabotu izpratni par kibernetiskajiem uzbrukumiem un tās ietekmi, un pastiprināta sadarbība un paraugprakses apmaiņa, piemēram, ar kompetentu specializētu Savienības aģentūru un struktūru starpniecību. Ar šādu apmācību būtu *inter alia* jātiecas uzlabot informētību par atšķirīgajām valstu tiesību sistēmām, iespējamām juridiskām un tehniskām problēmām, ar kurām saskaras kriminālizmeklēšanā, un kompetenču sadalījumu starp atbilstīgajām valstu iestādēm.

(29) Šajā direktīvā ir respektētas cilvēktiesības un pamatbrīvības un ievēroti principi, kas jo īpaši atzīti Eiropas Savienības Pamattiesību hartā un Eiropas Cilvēktiesību un

pamatbrīvību aizsardzības konvencijā, tostarp personas datu aizsardzība, tiesības uz privāto dzīvi, vārda un informācijas brīvība, tiesības uz taisnīgu tiesu, nevainīguma prezumpcija un tiesības uz aizstāvību, kā arī noziedzīgu nodarījumu un sodu likumības un samērīguma princips. Šo tiesību un principu pilnīga ievērošana ir īpaši šīs direktīvas mērķis, un tā ir attiecīgi jāīsteno.

(30) Personas datu aizsardzība saskaņā ar LESD 16. panta 1. punktu un Pamattiesību hartas 8. pantu ir pamattiesība. Tāpēc, veicot jebkādu personas datu apstrādi saistībā ar šīs direktīvas īstenošanu, būtu pilnībā jāievēro atbilstīgie Savienības tiesību akti par datu aizsardzību.

(31) Saskaņā ar 3. pantu Protokolā par Apvienotās Karalistes un Īrijas nostāju saistībā ar brīvības, drošības un tiesiskuma telpu, kas pievienots Līgumam par Eiropas Savienību un Līgumam par Eiropas Savienības darbību, minētās dalībvalstis ir informējušas par savu vēlmi piedalīties šīs direktīvas pieņemšanā un piemērošanā.

(32) Saskaņā ar 1. un 2. pantu Protokolā par Dānijas nostāju, kas pievienots Līgumam par Eiropas Savienību un Līgumam par Eiropas Savienības darbību, Dānija nepiedalās šīs direktīvas pieņemšanā, un šī direktīva tai nav saistoša un nav jāpiemēro.

(33) Ņemot vērā to, ka šīs direktīvas mērķus, proti, visās dalībvalstīs par uzbrukumiem informācijas sistēmām piemērot iedarbīgus, samērīgus un atturošus kriminālsodus un uzlabot un veicināt tiesu iestāžu un citu kompetentu iestāžu sadarbību, nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, un to, ka paredzētās rīcības mēroga un iedarbības dēļ šos mērķus var labāk sasniegt Savienības līmenī, Savienība var pieņemt pasākumus saskaņā ar Līguma par Eiropas Savienību 5. pantā noteikto subsidiaritātes principu. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šajā direktīvā paredz vienīgi tos pasākumus, kas ir vajadzīgi minēto mērķu sasniegšanai.

(34) Šīs direktīvas mērķis ir grozīt un paplašināt Padomes Pamatlēmuma 2005/222/TI (2005. gada 24. februāris) par uzbrukumiem informācijas sistēmām <sup>(2)</sup> noteikumus. Tā kā veicamie grozījumi ir būtiski un to skaits ir ievērojams, skaidrības labad attiecībā uz tām dalībvalstīm, kuras piedalās šīs direktīvas pieņemšanā, Pamatlēmums 2005/222/TI būtu jāaizstāj pilnībā,

<sup>(1)</sup> OV L 328, 15.12.2009., 42. lpp.

<sup>(2)</sup> OV L 69, 16.3.2005., 67. lpp.



IR PIEŅĒMUŠI ŠO DIREKTĪVU.

### 1. pants

#### Priekšmets

Ar šo direktīvu izveido minimālos noteikumus, lai noteiktu noziedzīgus nodarījumus un sankcijas uzbrukumu informācijas sistēmām jomā. Tās mērķis ir arī veicināt šādu nodarījumu novēršanu un uzlabot tiesu iestāžu un citu kompetento iestāžu sadarbību.

### 2. pants

#### Definīcijas

Šajā direktīvā piemēro šādas definīcijas:

- a) "informācijas sistēma" ir ierīce vai savstarpēji savienotu vai saistītu ierīču kopums, no kurām viena vai vairākas ierīces saskaņā ar programmu automātiski apstrādā datorizētus datus, kā arī datorizēti dati, ko minētās ierīces vai ierīču kopums glabā, apstrādā, iegūst vai sūta, lai nodrošinātu savu darbību, izmantošanu, aizsargāšanu un uzturēšanu;
- b) "datorizēti dati" ir fakti, informācijas vai konceptu atveidojums formā, kas ir piemērota apstrādei informācijas sistēmā, tostarp programma, kas piemērota tam, lai informācijas sistēmā izraisītu kādu darbību;
- c) "juridiska persona" ir subjekts, kam saskaņā ar piemērojamiem tiesību aktiem ir juridiskas personas statuss, bet kas neietver nedz valstis vai publiskas struktūras, kas darbojas, īstenojot valsts varu, nedz publisko tiesību starptautiskās organizācijas;
- d) "bez tiesībām" ir šajā direktīvā minēta darbība, tostarp piekļuve, ieviešana vai pārtveršana bez sistēmas vai tās daļas īpašnieka vai cita tiesību subjekta atļaujas vai kas nav atļauta saskaņā ar valsts tiesību aktiem.

### 3. pants

#### Nelikumīga piekļuve informācijas sistēmām

Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka gadījumos, kad tas darīts ar nodomu, piekļuve bez tiesībām visai informācijas sistēmai vai jebkādai tās daļai, pārkāpjot drošības pasākumu, un vismaz gadījumos, kas nav mazsvarīgi, ir sodāma kā noziedzīgs nodarījums.

### 4. pants

#### Nelikumīga ieviešana sistēmā

Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka vismaz gadījumos, kas nav mazsvarīgi, informācijas sistēmas darbības būtiska kavēšana vai pārtraukšana, ievadot datorizētus datus, sūtot, bojājot, dzēšot, pasliktinot, grozot, anulējot šādus datus vai padarot šādus datus nepieejamus, ir sodāma kā noziedzīgs nodarījums, ja tas ir darīts ar nodomu un bez tiesībām.

### 5. pants

#### Nelikumīga ieviešana datos

Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka vismaz gadījumos, kas nav mazsvarīgi, informācijas sistēmas datorizētu datu dzēšana, bojāšana, pasliktināšana, grozīšana, anulēšana vai šādu datu padarīšana par nepieejamiem ir sodāma kā noziedzīgs nodarījums, ja tas ir darīts ar nodomu un bez tiesībām.

### 6. pants

#### Nelikumīga pārtveršana

Dalībvalstis pieņem vajadzīgos pasākumus, lai nodrošinātu, ka vismaz gadījumos, kas nav mazsvarīgi, datu pārtveršana, kas izdarīta ar tehnisku līdzekļu palīdzību, pārtverot publiski nepieejamu datu pārraidi uz, no vai informācijas sistēmā, tostarp elektromagnētisku datu iegūšanu no informācijas sistēmas, kurā atrodas šādi dati, ir sodāma kā noziedzīgs nodarījums, ja tas darīts ar nodomu un bez tiesībām.

### 7. pants

#### Noziedzīgu nodarījumu izdarīšanas rīki

Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka vismaz gadījumos, kas nav mazsvarīgi, kāda no turpmāk minēto rīku izstrāde, pārdošana, iepirkšana izmantošanai, imports, izplatīšana vai citāda veida pieejamības nodrošināšana, ja tā veikta ar nodomu, ir sodāma kā noziedzīgs nodarījums, ja to izdara bez tiesībām un ar nodomu to izmantot, lai izdarītu kādu no 3. līdz 6. pantā minētajiem nodarījumiem:

- a) datorprogramma, kura galvenokārt paredzēta vai pielāgota 3. līdz 6. pantā minēto nodarījumu izdarīšanai;
- b) datorparole, pieejas kods vai līdzīgi dati, ar kuru palīdzību var piekļūt informācijas sistēmai vai tās daļai.

### 8. pants

#### Kūdišana, sekmēšana un atbalstīšana, un mēģinājums

1. Dalībvalstis nodrošina, ka kūdišana izdarīt kādu no 3. līdz 7. pantā minētajiem nodarījumiem vai tādu nodarījumu sekmēšana un atbalstīšana ir sodāma kā noziedzīgs nodarījums.

2. Dalībvalstis nodrošina, ka mēģinājums izdarīt kādu no 4. un 5. pantā minētajiem nodarījumiem ir sodāms kā noziedzīgs nodarījums.

### 9. pants

#### Sodi

1. Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka par 3. līdz 8. pantā minētajiem nodarījumiem ir paredzēti iedarbīgi, samērīgi un atturoši kriminālsodi.

2. Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka 3. līdz 7. pantā minētie nodarījumi vismaz gadījumos, kas nav mazsvarīgi, ir sodāmi ar maksimālo brīvības atņemšanas termiņu – vismaz divi gadi.

3. Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka 4. un 5. pantā minētie nodarījumi, ja tie izdarīti ar nodomu, ir sodāmi ar maksimālo brīvības atņemšanas termiņu – vismaz trīs

gadi, ja ir ietekmēts ievērojams skaits informācijas sistēmu, izmantojot rīku, kas minēts 7. pantā un kas izstrādāts vai pielāgots galvenokārt minētajam mērķim.

4. Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka 4. un 5. pantā minētie nodarījumi ir sodāmi ar maksimālo brīvības atņemšanas termiņu – vismaz pieci gadi, ja:

- a) tie ir izdarīti, darbojoties noziedzīgā organizācijā, kā definēts Pamatlēmumā 2008/841/TI, bet neatkarīgi no tajā paredzētā soda;
- b) tie izraisa nopietnu kaitējumu; vai
- c) tie ir izdarīti pret kādu kritiskās infrastruktūras informācijas sistēmu.

5. Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka gadījumos, kad 4. un 5. pantā minētie nodarījumi ir izdarīti, ļaunprātīgi izmantojot citu personu personas datus, lai iegūtu trešās personas uzticību, un tādējādi nodarot kaitējumu identitātes likumīgajam īpašniekam, to atbilstīgi valsts tiesību aktiem var uzskatīt par atbildību pastiprinošiem apstākļiem, izņemot, ja minētos apstākļus jau aptver cits nodarījums, kurš saskaņā ar valsts tiesību aktiem ir sodāms.

#### 10. pants

##### Juridisko personu atbildība

1. Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka juridiskas personas var saukt pie atbildības par 3. līdz 8. pantā minētajiem nodarījumiem, ko to labā, darbojoties individuāli vai kā juridiskas personas struktūras daļa, izdarījusi kāda persona, kas veic šīs juridiskās personas vadības pienākumus, pamatojoties uz vienu no turpmāk minētā:

- a) pilnvarām pārstāvēt juridisko personu;
- b) pilnvarām pieņemt lēmumus juridiskās personas vārdā;
- c) pilnvarām veikt juridiskās personas iekšējo kontroli.

2. Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka juridiskas personas var saukt pie atbildības, ja 1. punktā minētās personas uzraudzības vai kontroles trūkums ir ļāvis personai, kura ir tās pakļautībā, izdarīt nodarījumu, kas minēts 3. līdz 8. pantā, minētās juridiskās personas labā.

3. Juridisku personu atbildība saskaņā ar 1. un 2. punktu neizslēdz kriminālprocesu pret fiziskām personām, kas ir kāda no 3. līdz 8. pantā minētā nodarījuma izdarītāji, uzskūditāji vai līdzdalībnieki.

#### 11. pants

##### Juridiskām personām piemērojamās sankcijas

1. Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka juridiskai personai, kuru sauc pie atbildības saskaņā ar 10. panta 1. punktu, tiek piemērotas iedarbīgas, samērīgas un atturošas sankcijas, kas ietver naudas sodu kā kriminālsodu vai naudas sodu bez krimināla rakstura un kas var ietvert citas sankcijas, piemēram:

- a) atņemt tiesības saņemt publiskus līdzekļus vai atbalstu;
- b) uz laiku vai pastāvīgi aizliegt veikt komercdarbību;
- c) pakļaut tiesas uzraudzībai;
- d) likvidēt ar tiesas lēmumu;
- e) uz laiku vai pavisam slēgt uzņēmējdarbības veikšanas vietas, kas izmantotas nodarījuma izdarīšanā.

2. Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka juridiskai personai, kuru sauc pie atbildības saskaņā ar 10. panta 2. punktu, tiek piemērotas iedarbīgas, samērīgas un atturošas sankcijas vai citi pasākumi.

#### 12. pants

##### Jurisdikcija

1. Dalībvalstis nosaka savu jurisdikciju attiecībā uz direktīvas 3. līdz 8. pantā minētajiem nodarījumiem, ja:

- a) nodarījums ir pilnīgi vai daļēji izdarīts to teritorijā; vai
- b) nodarījumu izdarījis kāds tās valstspiederīgais, vismaz gadījumos, kad darbība ir nodarījums vietā, kur tā ir izdarīta.

2. Dalībvalsts, nosakot jurisdikciju saskaņā ar 1. punkta a) apakšpunktu, nodrošina, ka tai ir jurisdikcija, ja:

- a) nodarījuma izdarītājs izdara nodarījumu, fiziski atrodoties tās teritorijā, neatkarīgi no tā, vai nodarījums ir izdarīts pret informācijas sistēmu tās teritorijā; vai
- b) nodarījums ir izdarīts pret informācijas sistēmu tās teritorijā, neatkarīgi no tā, vai nodarījuma izdarītājs izdara nodarījumu, fiziski atrodoties tās teritorijā.

3. Dalībvalsts informē Komisiju, ja tā pieņem lēmumu noteikt jurisdikciju par kādu no 3. līdz 8. pantā minētajiem nodarījumiem, kas izdarīts ārpus tās teritorijas, tostarp, ja:

- a) nodarījuma izdarītāja pastāvīgā dzīvesvieta ir tās teritorijā; vai
- b) nodarījums ir izdarīts tādas juridiskās personas labā, kas veic uzņēmējdarbību tās teritorijā.

#### 13. pants

##### Informācijas apmaiņa

1. Lai apmainītos ar informāciju par 3. līdz 8. pantā minētajiem nodarījumiem, dalībvalstis nodrošina, ka tām ir valsts operatīvais kontaktpunkts un ka tās izmanto esošo operatīvo kontaktpunktu tīklu, kas ir pieejams divdesmit četras stundas diennaktī, septiņas dienas nedēļā. Dalībvalstis nodrošina arī to, ka ir ieviestas procedūras, lai steidzamu palīdzības pieprasījumu gadījumā kompetentā iestāde astoņās stundās no saņemšanas var norādīt vismaz, vai uz pieprasījumu tiks sniegta atbilde, kādā veidā tā tiks sniegta, un minēt aptuvenu šādas atbildes sniegšanas laiku.

2. Dalībvalstis informē Komisiju par 1. punktā minētajiem to izraudzītajiem kontaktpunktiem. Komisija nosūta šo informāciju pārējām dalībvalstīm un kompetentajām specializētajām Savienības aģentūrām un struktūrām.

3. Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka ir pieejami atbilstīgi ziņošanas kanāli, lai veicinātu ziņošanu kompetentajām valstu iestādēm par 3. līdz 6. pantā minētajiem nodarījumiem bez nepamatotas kavēšanās.

#### 14. pants

##### Uzraudzība un statistika

1. Dalībvalstis nodrošina tādas sistēmas darbību, ar kuras palīdzību reģistrē, ģenerē un sniedz statistikas datus par nodarījumiem, kas minēti 3. līdz 7. pantā.

2. Statistikas dati, kas minēti 1. punktā, aptver vismaz pastāvošos datus par 3. līdz 7. pantā minēto nodarījumu skaitu, ko reģistrējušas dalībvalstis, un to personu skaitu, pret kurām uzsāks kriminālprocesu un kas notiesātas par 3. līdz 7. pantā minētajiem nodarījumiem.

3. Saskaņā ar šo pantu savāktos datus dalībvalstis nosūta Komisijai. Komisija nodrošina šo statistikas ziņojumu konsolidēta pārskata publicēšanu un iesniegšanu kompetentajām specializētajām Savienības aģentūrām un struktūrām.

#### 15. pants

##### Pamatlēmuma 2005/222/TI aizstāšana

Ar šo Pamatlēmums 2005/222/TI tiek aizstāts attiecībā uz dalībvalstīm, kas piedalās šīs direktīvas pieņemšanā, neskarot dalībvalstu pienākumus attiecībā uz termiņu pamatlēmuma transponēšanai valsts tiesību aktos.

Attiecībā uz dalībvalstīm, kuras piedalās šīs direktīvas pieņemšanā, atsaucies uz Pamatlēmumu 2005/222/TI uzskata par atsaucēm uz šo direktīvu.

#### 16. pants

##### Transponēšana

1. Dalībvalstīs stājas spēkā normatīvie un administratīvie akti, kas vajadzīgi, lai izpildītu šīs direktīvas prasības līdz 2015. gada 4. septembrim.

2. Dalībvalstis nosūta Komisijai to pasākumu tekstu, ar kuriem to tiesību aktos transponē pienākumus, kas tām uzlikti saskaņā ar šo direktīvu.

3. Kad dalībvalstis pieņem minētos pasākumus, tajos ietver atsauci uz šo direktīvu vai arī šādu atsauci pievieno to oficiālai publikācijai. Dalībvalstis nosaka paņēmienus, kā izdarāma šāda atsaucē.

#### 17. pants

##### Ziņošana

Komisija līdz 2017. gada 4. septembrim sniedz ziņojumu Eiropas Parlamentam un Padomei, izvērtējot, cik lielā mērā dalībvalstis veikušas pasākumus, kas vajadzīgi, lai izpildītu šo direktīvu, vajadzības gadījumā pievienojot leģislatīvu aktu priekšlikumus. Komisija arī ņem vērā tehniskās un juridiskās norises kibernetizācijas jomā, jo īpaši attiecībā uz šīs direktīvas darbības jomu.

#### 18. pants

##### Stāšanās spēkā

Šī direktīva stājas spēkā divdesmitajā dienā pēc tās publicēšanas Eiropas Savienības Oficiālajā Vēstnesī.

#### 19. pants

##### Adresāti

Šī direktīva ir adresēta dalībvalstīm saskaņā ar Līgumiem.

Briselē, 2013. gada 12. augustā

Eiropas Parlamenta vārdā –  
priekšsēdētājs  
M. SCHULZ

Padomes vārdā –  
priekšsēdētājs  
L. LINKEVIČIUS