EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA 2013/40/ES

2013 m. rugpjūčio 12 d.

dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR

EUROPOS PARLAMENTAS IR EUROPOS SĄJUNGOS TARYBA,

atsižvelgdami į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 83 straipsnio 1 dalį,

atsižvelgdami į Europos Komisijos pasiūlymą,

teisėkūros procedūra priimamo akto projektą perdavus nacionaliniams parlamentams,

atsižvelgdami į Europos ekonomikos ir socialinių reikalų komiteto nuomonę [1],

laikydamiesi įprastos teisėkūros procedūros [2],

kadangi:

(1) šios direktyvos tikslai yra suderinti valstybių narių baudžiamąją teisę atakų prieš informacines sistemas srityje, nustatant būtiniausias taisykles, susijusias su nusikalstamų veikų apibrėžtimi, ir atitinkamas sankcijas šioje srityje, ir pagerinti valstybių narių kompetentingų institucijų, įskaitant policiją ir kitas specializuotas teisėsaugos tarnybas, taip pat Sąjungos kompetentingų specializuotų agentūrų ir įstaigų, pavyzdžiui, Eurojusto, Europolo ir Europos kovos su elektroniniais nusikaltimais centro bei Europos tinklų ir informacijos apsaugos agentūros (ENISA), bendradarbiavimą;

(2) informacinės sistemos yra vienas iš svarbiausių politinės, socialinės ir ekonominės sąveikos Sąjungoje elementų. Visuomenė itin ir vis labiau yra priklausoma nuo tokių sistemų. Sklandus tų sistemų veikimas ir saugumas Sąjungoje yra ypač svarbūs siekiant vystyti vidaus rinką ir konkurencingą bei novatorišką ekonomiką. Tinkamo informacinių sistemų apsaugos lygio užtikrinimas turėtų būti veiksmingos išsamios prevencinių priemonių sistemos dalis, papildanti baudžiamojoje teisėje nustatytas reagavimo į elektroninius nusikaltimus priemones;

(3) atakų prieš informacines sistemas ir, visų pirma, atakų, susijusių su organizuotu nusikalstamumu, grėsmė Sąjungoje ir visame pasaulyje didėja, ir vis didesnį susirūpinimą kelia galimi teroristų išpuoliai ar politiškai motyvuotos atakos prieš informacines sistemas, kurios yra valstybių narių ir Sąjungos ypatingos svarbos infrastruktūros dalis. Todėl kyla grėsmė, kad nebus sukurta saugesnė informacinė visuomenė ir laisvės, saugumo ir teisingumo erdvė, taigi reikia imtis bendrų Sąjungos lygmens veiksmų ir gerinti bendradarbiavimą ir koordinavimą tarptautiniu lygiu;

(4) Sąjungoje yra ypatingos svarbos infrastruktūros objektų, kurių veiklos sutrikdymas arba sunaikinimas padarytų didelį tarpvalstybinį poveikį. Kadangi tapo aišku, kad reikia stiprinti ypatingos svarbos infrastruktūros objektų apsaugos pajėgumą Sąjungoje, kovos su kibernetinėmis atakomis priemones reikėtų papildyti griežtomis baudžiamosiomis sankcijomis, atitinkančiomis tokių atakų pavojingumą. Ypatingos svarbos infrastruktūros objektais galėtų būti laikomi valstybėse narėse esantis turtas, sistema arba jų dalis, kurie būtini, pavyzdžiui, siekiant palaikyti gyvybines visuomenės funkcijas, visuomenės sveikatą, saugą ir saugumą, ekonominę arba socialinę gerovę, pavyzdžiui, jėgainės, transporto tinklai ar Vyriausybės tinklai, ir kurių veiklos sutrikdymas arba sunaikinimas padarytų didelį poveikį atitinkamai valstybei narei, nes tos funkcijos nebebūtų vykdomos;

(5) akivaizdu, kad daugėja pavojingų ir pakartotinių didelės apimties atakų prieš informacines sistemas, kurios yra ypatingai svarbios valstybėms arba konkrečioms viešojo ar privačiojo sektoriaus funkcijoms. Šią tendenciją papildo vis sudėtingesnių metodų kūrimas, pavyzdžiui, vadinamųjų „botnetų“ kūrimas ir naudojimas – veikla, kurią sudaro keli vienas po kito sekantys etapai, kai kiekvienas atskiras etapas galėtų sukelti didelį pavojų visuomenės interesams. Šiuo atžvilgiu direktyva siekiama, *inter alia*, nustatyti baudžiamąsias sankcijas už etapą, kuomet sukuriamas botnetas, būtent kai įgyjama nuotolinė daugelio kompiuterių kontrolė, pasitelkus prieš tuos kompiuterius nukreiptas kibernetines atakas ir juos užkrėtus žalinga programine įranga. Vėlesniu etapu užkrėstas kompiuterių tinklas, sudarantis botnetą, be kompiuterių naudotojų žinios gali būti naudojamas didelės apimties kibernetinėms atakoms, kurios paprastai gali sukelti didelę žalą, kaip nurodyta šioje direktyvoje. Valstybės narės gali nustatyti, kas yra didelė žala, vadovaudamosi savo nacionaline teise ir praktika – tokia žala gali būti susijusi su visuomenei labai svarbių sisteminių paslaugų sutrikdymu ar patiriamomis didelėmis finansinėmis išlaidomis, arba asmens duomenų ar slapto pobūdžio informacijos praradimu;

(6) didelės apimties kibernetinės atakos gali sukelti didžiulę ekonominę žalą todėl, kad gali sutrikdyti informacinių sistemų veikimą ir komunikaciją, ir todėl, kad gali būti prarasta ar pakeista komerciniu požiūriu svarbi konfidenciali informacija ar kiti duomenys. Ypač daug dėmesio turėtų būti skirta novatoriškų mažų ir vidutinių įmonių informuotumo apie grėsmes, susijusias su tokiomis atakomis, ir jų pažeidžiamumą didinimui, nes tos įmonės yra itin priklausomos nuo tinkamo informacinių sistemų veikimo ir prieigos prie jų, o jų ištekliai informacijos saugumui užtikrinti dažnai yra riboti;

[1] OL C 218, 2011 7 23, p. 130.

[2] 2013 m. liepos 4 d. Europos Parlamento pozicija (dar nepaskelbta Oficialiajame leidinyje) ir 2013 m. liepos 22 d. Tarybos sprendimas.

(7) šioje srityje bendros apibrėžtys yra svarbios, kad valstybėse narėse būtų užtikrintas nuoseklus požiūris į šios direktyvos taikymą;

(8) reikia susitarti dėl bendro požiūrio į nusikalstamos veikos sudėties požymius numatant, kad neteisėta prieiga prie informacinės sistemos, neteisėtas įsikišimas į sistemą, neteisėtas įsikišimas į duomenis ir neteisėtas duomenų perėmimas yra bendrai laikomi nusikalstama veika;

(9) duomenų perėmimas apima pranešimų turinio klausymąsi, stebėjimą ar sekimą, duomenų turinio teikimą arba tiesiogiai, naudojantis prieiga prie informacinių sistemų ir naudojant šias sistemas, arba netiesiogiai, naudojant elektroninę slapto klausymosi įrangą pasitelkus technines priemones, tačiau nebūtinai apsiribojama vien šiais būdais;

(10) valstybės narės turėtų numatyti sankcijas už atakas prieš informacines sistemas. Tos sankcijos turėtų būti veiksmingos, proporcingos ir atgrasančios bei turėtų apimti įkalinimą ir (arba) finansines nuobaudas;

(11) direktyvoje numatomos baudžiamosios sankcijos bent tais atvejais, kurie nėra mažareikšmiai. Valstybės narės gali nustatyti, kas yra mažareikšmis atvejis, vadovaudamosi savo nacionaline teise ir praktika. Atvejis gali būti laikomas mažareikšmiu, pavyzdžiui, kai nusikalstama veika padaryta žala ir (arba) dėl jos kylanti grėsmė viešiesiems arba privatiesiems interesams, pvz., kompiuterių sistemos arba kompiuterinių duomenų vientisumui arba asmens neliečiamumui, teisėms ir kitiems interesams, yra menka arba tokio pobūdžio, kad nėra būtina skirti baudžiamąją sankciją laikantis teisės aktuose nustatytų ribų arba nustatyti baudžiamąją atsakomybę;

(12) grėsmių ir pavojų, kuriuos kelia kibernetinės atakos, bei susijusio informacinių sistemų pažeidžiamumo nustatymas ir pranešimas apie jas yra svarbus veiksmingos prevencijos ir atsako į kibernetines atakas bei informacinių sistemų saugumo gerinimo elementas. Tuo tikslu gali būti naudingos paskatos pranešti apie saugumo spragas. Valstybės narės turėtų stengtis sudaryti sąlygas teisėtai aptikti saugumo spragas ir apie jas pranešti;

(13) tikslinga numatyti griežtesnes sankcijas tais atvejais, kai ataka prieš informacinę sistemą padaryta nusikalstamos organizacijos, kaip apibrėžta 2008 m. spalio 24 d. Tarybos pamatiniame sprendime 2008/841/TVR dėl kovos su organizuotu nusikalstamumu ([1]), kai elektroninė ataka vykdoma plačiu mastu ir todėl dėl jos daromas poveikis daugeliui informacinių sistemų, įskaitant tuos atvejus, kai ataka siekiama sukurti botnetą arba kai ji vykdoma naudojant botnetą ir tokiu būdu padaroma didelė žala, įskaitant atvejus, kai ataka vykdoma per botnetą. Taip pat tikslinga numatyti griežtesnes sankcijas tais atvejais, kai ataka yra nukreipta prieš ypatingos svarbos valstybių narių arba Sąjungos infrastruktūros objektą;

(14) veiksmingų kovos su tapatybės vagyste ir kitomis su tapatybe susijusiomis nusikalstamomis veikomis priemonių nustatymas yra kitas svarbus integruoto požiūrio į kovą su elektroniniais nusikaltimais elementas. Vertinant išsamios horizontaliosios Sąjungos priemonės poreikį, galėtų būti apsvarstyta, ar reikia Sąjungos veiksmų, susijusių su šios rūšies nusikalstama veikla;

(15) 2008 m. lapkričio 27–28 d. Tarybos išvadose nurodyta, kad valstybės narės ir Komisija, atsižvelgdamos į 2001 m. Europos Tarybos konvencijos dėl elektroninių nusikaltimų turinį, turėtų parengti naują strategiją. Ta konvencija yra pamatinis kovos su elektroniniais nusikaltimais, įskaitant atakas prieš informacines sistemas, teisinis pagrindas. Ši direktyva grindžiama ta konvencija. Todėl kuo skubesniam konvencijos ratifikavimo proceso užbaigimui visose valstybėse narėse turėtų būti teikiamas prioritetas;

(16) atsižvelgiant į skirtingus atakų atlikimo būdus ir spartų techninės ir programinės kompiuterių įrangos tobulėjimą, šioje direktyvoje sąvoka „priemonės“ reiškia priemones, naudojamas šioje direktyvoje nustatytoms nusikalstamoms veikoms vykdyti. Tokios priemonės gali reikšti kibernetinėms atakoms rengti naudojamą žalingą programinę įrangą, įskaitant priemones, kuriomis gali būti kuriami botnetai. NET jeigu tokia priemonė yra tinkama ar netgi specialiai skirta vienai iš šioje direktyvoje nustatytų nusikalstamų veikų vykdymui, gali būti, jog ji pagaminta teisėtu tikslu. Remiantis poreikiu išvengti baudžiamosios atsakomybės taikymo tuo atveju, kai tokios priemonės yra pagamintos ir pateiktos rinkai teisėtais tikslais, pavyzdžiui, skirtos informacinių technologijų produktų patikimumo arba informacinių technologijų saugumo testavimui, ne tik bendro ketinimo reikalavimas, bet ir tiesioginio ketinimo panaudoti tas priemones šioje direktyvoje nustatytai vienai ar kelioms nusikalstamoms veikoms vykdyti reikalavimas taip pat turi būti išpildytas;

(17) šia direktyva nesiekiama nustatyti baudžiamosios atsakomybės tais atvejais, kai yra šioje direktyvoje nustatytų nusikalstamų veikų sudėties objektyvių požymių, tačiau veiksmai padaromi netyčia, pavyzdžiui, kai asmuo nežinojo, kad prieiga yra neteisėta arba siekiant atlikti informacinių sistemų tikrinimą arba saugumo užtikrinimą turint tam leidimą, pavyzdžiui, kai įmonė arba pardavėjas paskiria asmenį patikrinti apsaugos sistemos patikimumą. Laikantis šios direktyvos sutartiniai įsipareigojimai arba susitarimai apriboti prieigą prie informacinių sistemų pasitelkiant naudojimo politiką arba veiklos sąlygas, taip pat darbo ginčai dėl prieigos prie darbdavio informacinių sistemų ir jų naudojimo asmeniniais tikslais neturėtų užtraukti baudžiamosios atsakomybės, kai prieiga tokiomis aplinkybėmis būtų laikytina neteisėta ir todėl sudarytų pagrindą baudžiamajai bylai. Ši direktyva nedaro poveikio teisiškai užtikrintai teisei susipažinti su informacija, kaip nustatyta nacionalinės ir Sąjungos teisės aktuose, taip pat ja negali būti remiamasi kaip išimtimi siekiant pateisinti neteisėtą arba savavališką prieigą prie informacijos;

([1]) OL L 300, 2008 11 11, p. 42.

(18) palankesnes sąlygas kibernetinių atakų vykdymui gali sudaryti įvairios aplinkybės, pavyzdžiui, kai nusikalstamos veikos vykdytojas dėl jo ar jos užimamų pareigų apimties turi prieigą prie atitinkamų informacinių sistemų, kurioms gali kilti grėsmė, saugumo sistemų. Nacionalinėje teisėje baudžiamajame procese turėtų būti tinkamai atsižvelgta į tokias aplinkybes;

(19) esant sunkinančioms aplinkybėms valstybės narės, vadovaudamosi jų teisės sistemose nustatytomis taikytinomis taisyklėmis, turėtų nacionalinėje teisėje numatyti sunkinančias aplinkybes. Jos turėtų užtikrinti, kad teisėjai turėtų galimybę atsižvelgti į tokias sunkinančias aplinkybes teisdami nusikalstamų veikų vykdytojus. Teisėjas ir toliau savo nuožiūra turi turėti galimybę įvertinti tas aplinkybes kartu su kitais faktiniais konkrečios bylos elementais;

(20) šia direktyva nereglamentuojamos sąlygos, kurios turėtų būti įvykdytos, kad būtų galima naudotis jurisdikcija bet kurios iš čia nurodytų nusikalstamų veikų atžvilgiu, pavyzdžiui, kad apie nusikalstamą veiką jos padarymo vietoje praneštų nukentėjęs asmuo arba ja apkaltintų valstybė, kurioje įvykdyta veika, arba kad pažeidėjas nebūtų patraukiamas baudžiamojon atsakomybėn nusikalstamos veikos įvykdymo vietoje;

(21) taikant šią direktyvą valstybės ir viešosios institucijos laikydamosi esamų tarptautinių įsipareigojimų, tebėra visapusiškai atsakingos už tai, kad būtų užtikrinta pagarba žmogaus teisėms ir pagrindinėms laisvėms;

(22) šia direktyva didinama tam tikrų tinklų svarba, pavyzdžiui, Didžiojo aštuoneto arba Europos Tarybos sukurtų ištisą parą, septynias dienas per savaitę veikiančių informacinių punktų. Tie informaciniai punktai turėtų teikti veiksmingą pagalbą, tokiu būdu sudarydami palankesnes sąlygas keistis turima atitinkama informacija arba teikti technines konsultacijas ar teisinę informaciją tiriant su informacinėmis sistemomis ir atitinkamais duomenimis susijusias nusikalstamas veikas arba nagrinėjant tokias bylas, kuriose dalyvauja prašančioji valstybė narė. Siekiant užtikrinti sklandų tinklų veikimą, kiekvienas informacinis punktas turėtų turėti pajėgumų skubos tvarka, padedamas, *inter alia*, apmokyto ir pasirengusio personalo, palaikyti ryšius su kitos valstybės narės informaciniu punktu. Atsižvelgiant į tai, kad didelės apimties kibernetinės atakos gali būti įvykdytos labai greitai, valstybės narės turėtų būti pajėgios nedelsiant reaguoti į šio informacinių punktų tinklo skubius prašymus. Tokiais atvejais gali būti tikslinga pateikiant prašymą suteikti informaciją nurodyti kontaktinį telefono numerį, kad būtų užtikrinta, jog prašymą gavusi valstybė narė skubiai imtųsi jį nagrinėti ir informacija būtų suteikta per aštuonias valandas;

(23) siekiant užkirsti kelią atakoms prieš informacines sistemas ir su jomis kovoti itin svarbus yra valdžios institucijų bendradarbiavimas su privačiuoju sektoriumi ir pilietine visuomene. Reikia skatinti ir gerinti paslaugų teikėjų, gamintojų, teisėsaugos įstaigų ir teisminių institucijų bendradarbiavimą ir sykiu visapusiškai laikytis teisinės valstybės principų. Toks bendradarbiavimas galėtų apimti, pavyzdžiui, paslaugų teikėjų teikiamą paramą padedant išsaugoti galimus įrodymus, pateikiant elementus, padedančius nustatyti nusikalstamos veikos vykdytojus ir, taikyti kaip kraštutinę priemonę, atsižvelgiant į nacionalinę teisę, ir praktiką, visišką arba dalinį informacinių sistemų arba funkcijų, kurioms pakenkta arba kurios naudojamos neteisėtai, išjungimą laikantis nacionalinės teisės. Valstybės narės taip pat turėtų apsvarstyti galimybę sukurti bendradarbiavimo ir partnerystės tinklus su paslaugų teikėjais ir gamintojais siekiant keistis informacija, susijusia su nusikalstama veika šios direktyvos taikymo srityje;

(24) būtina rinkti palyginamuosius duomenis apie šioje direktyvoje nustatytas nusikalstamas veikas. Atitinkami duomenys turėtų būti pateikiami kompetentingoms specializuotoms Sąjungos agentūroms ir įstaigoms, pavyzdžiui, Europolui ir ENISA atsižvelgiant į jų uždavinius ir informacijos poreikius, kad būtų surinkta išsamesnės informacijos apie elektroninių nusikaltimų mastą ir tinklų bei informacijos saugumą Sąjungos lygiu ir tokiu būdu būtų ieškoma veiksmingesnių reagavimo būdų. Valstybės narės turėtų perduoti Europolui ir Europos kovos su elektroniniu nusikalstamumu centrui informaciją apie nusikalstamų veikų vykdytojų veiklos būdus, kad būtų atliktas elektroninių nusikaltimų grėsmės įvertinimas ir strateginė analizė pagal 2009 m. balandžio 6 d. Tarybos sprendimą 2009/371/TVR dėl Europos policijos biuro (Europolo) įsteigimo ([1]). Teikiant informaciją gali būti sudarytos palankesnės sąlygos suprasti dabartines ir būsimas grėsmes bei tokiu būdu gali būti prisidėta prie tinkamesnio ir tikslingesnio sprendimų dėl kovos su atakomis prieš informacines sistemas ir jų prevencijos priėmimo proceso;

(25) pagal šią direktyvą Komisija turėtų teikti ataskaitą dėl direktyvos taikymo ir teikti visus būtinus pasiūlymus dėl teisėkūros procedūra priimamų aktų, kuriais remiantis galėtų būti išplėsta jos taikymo sritis atsižvelgiant į pokyčius elektroninių nusikaltimų srityje. Tokie pokyčiai galėtų apimti technologijų pokyčius, kurie suteiktų galimybę, pavyzdžiui, užtikrinti veiksmingesnį vykdymą atakų prieš informacines sistemas srityje arba kuriais būtų sudarytos palankesnės sąlygos tokių atakų prevencijai ar jų poveikio susilpninimui. Tuo tikslu Komisija turėtų atsižvelgti į atitinkamų subjektų ir visų pirma Europolo ir ENISA parengtas turimas analizes ir ataskaitas;

(26) norint veiksmingai kovoti su elektroniniais nusikaltimais būtina padidinti informacinių sistemų atsparumą imantis tinkamų priemonių, kad jos būtų veiksmingiau apsaugotos nuo kibernetinių atakų. Valstybės narės turėtų imtis reikiamų priemonių tam, kad apsaugotų savo

([1]) OL L 121, 2009 5 15, p. 37.

ypatingos svarbos infrastruktūras nuo kibernetinių atakų, be kita ko – apsvarstyti savo informacinių sistemų ir susijusių duomenų apsaugą. Juridinių asmenų vykdomas informacinių sistemų tinkamo lygio apsaugos ir saugumo užtikrinimas, pavyzdžiui, teikiant viešas elektroninių ryšių paslaugas pagal galiojančius Sąjungos teisės aktus privatumo, elektroninių ryšių ir duomenų apsaugos srityje, yra itin svarbus išsamaus požiūrio į veiksmingą kovą su elektroniniais nusikaltimais elementas. Turėtų būti suteikta pakankamo lygio apsauga nuo pagrįstai nustatomos grėsmės ir pažeidžiamumo atsižvelgiant į naujausias konkrečių sektorių žinias ir konkrečias duomenų tvarkymo sąlygas. Tokios apsaugos sąnaudos ir su ja susijusi našta turėtų būti proporcingos žalai, kurią atitinkamiems objektams galėtų padaryti kibernetinė ataka. Valstybės narės raginamos numatyti atitinkamas priemones, kuriomis atsižvelgiant į nacionalinę teisę nustatoma atsakomybė tais atvejais, kai juridinis asmuo akivaizdžiai neužtikrino tinkamo lygio apsaugos nuo kibernetinių atakų;

(27) didelės valstybių narių įstatymų ir baudžiamojo proceso spragos ir skirtumai atakų prieš informacines sistemas srityje gali trukdyti kovoti su organizuotu nusikalstamumu ir terorizmu bei gali apsunkinti veiksmingą policijos ir teisminį bendradarbiavimą šioje srityje. Kadangi šiuolaikinės informacinės sistemos nėra saistomos valstybinių sienų, atakoms prieš tokias sistemas būdingas tarpvalstybinis aspektas, todėl pabrėžiamas poreikis skubiai veikti toliau derinant baudžiamąją teisę šioje srityje. Be to, tinkamai įgyvendinant ir taikant 2009 m. lapkričio 30 d. Tarybos pamatinį sprendimą 2009/948/TVR dėl jurisdikcijos įgyvendinimo kolizijų baudžiamuosiuose procesuose prevencijos ir sprendimo ([1]), turėtų būti sudarytos palankesnės sąlygos koordinuoti baudžiamąjį persekiojimą dėl atakų prieš informacines sistemas. Valstybės narės, bendradarbiaudamos su Sąjunga, taip pat turėtų siekti gerinti tarptautinį bendradarbiavimą, susijusį su informacinių sistemų, kompiuterinių tinklų ir kompiuterinių duomenų saugumu. Tarptautiniuose susitarimuose, susijusiuose su keitimusi duomenimis, turėtų būti tinkamai atsižvelgta į duomenų perdavimo ir saugojimo saugumą;

(28) norint veiksmingai kovoti su elektroniniais nusikaltimais, labai svarbu gerinti visos Sąjungos kompetentingų teisėsaugos įstaigų ir teisminių institucijų bendradarbiavimą. Atsižvelgiant į tai turėtų būti skatinama dėti daugiau pastangų, kad atitinkamoms valdžioms institucijoms būtų teikiamas tinkamas mokymas siekiant gerinti supratimą apie elektroninius nusikaltimus ir jų poveikį, ir skatinamas bendradarbiavimas ir keitimasis geriausios praktikos pavyzdžiais, pavyzdžiui, pasitelkiant specializuotas Sąjungos agentūras ir įstaigas. Tokiu mokymu turėtų būti siekiama, *inter alia*, didinti informuotumą apie įvairias nacionalines teisines sistemas, galimus teisinius ir techninius uždavinius, su kuriais susiduriama vykdant nusikalstamų veikų tyrimą, arba atitinkamų nacionalinių valdžios institucijų kompetencijos pasidalijimą;

(29) šia direktyva gerbiamos pagrindinės žmogaus teisės laisvės ir teisės ir laikomasi principų, visų pirma, pripažintų Europos Sąjungos pagrindinių teisių chartijoje ir Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijoje, įskaitant asmens duomenų apsaugą, teisę į privatų gyvenimą, saviraiškos ir informacijos laisvę, teisę į teisingą bylos nagrinėjimą, nekaltumo prezumpciją ir gynybos teises, taip pat teisėtumo ir nusikalstamos veikos bei sankcijų proporcingumo principų. Visų pirma, šia direktyva siekiama užtikrinti, kad būtų besąlygiškai laikomasi visų tų teisių ir principų, ir ji atitinkamai turi būti įgyvendinama;

(30) asmens duomenų apsauga yra pagrindinė teisė pagal SESV 16 straipsnio 1 dalį ir Europos Sąjungos Pagrindinių teisių chartijos 8 straipsnį. Todėl asmens duomenų tvarkymas įgyvendinant šią direktyvą turėtų visiškai atitikti atitinkamus Sąjungos teisės aktus dėl duomenų apsaugos;

(31) pagal Protokolo dėl Jungtinės Karalystės ir Airijos pozicijos dėl laisvės, saugumo ir teisingumo erdvės, pridėto prie Europos Sąjungos sutarties ir Sutarties dėl Europos Sąjungos veikimo, 3 straipsnį tos valstybės narės pranešė pageidaujančios dalyvauti priimant ir taikant šią direktyvą;

(32) pagal Protokolo dėl Danijos pozicijos, pridėto prie Europos Sąjungos sutarties ir Sutarties dėl Europos Sąjungos veikimo, 1 ir 2 straipsnius Danija nedalyvauja priimant šią direktyvą, todėl ji nėra jai privaloma ar taikoma;

(33) kadangi šios direktyvos tikslų, t. y. užtikrinti, kad visose valstybėse narėse už atakas prieš informacines sistemas būtų taikomos veiksmingos, proporcingos ir atgrasančios baudžiamosios sankcijos, ir gerinti bei skatinti teisminį bendradarbiavimą, valstybės narės negali deramai pasiekti dėl veiksmo masto ir poveikio ir kadangi tų tikslų būtų geriau siekti Sąjungos lygiu, laikydamasi Europos Sąjungos sutarties 5 straipsnyje nustatyto subsidiarumo principo Sąjunga gali patvirtinti priemones. Pagal tame straipsnyje nustatytą proporcingumo principą šia direktyva neviršijama to, kas būtina nurodytiems tikslams pasiekti;

(34) šia direktyva siekiama iš dalies pakeisti ir išplėsti 2005 m. vasario 24 d. Tarybos pamatinio sprendimo 2005/222/TVR dėl atakų prieš informacines sistemas ([2]) nuostatas. Kadangi pakeitimų, kuriuos reikia padaryti, yra daug ir jie yra svarbūs, siekiant aiškumo visas Pamatinis sprendimas 2005/222/TVR turėtų būti pakeistas valstybių narių, dalyvaujančių priimant šią direktyvą, atžvilgiu,

([1]) OL L 328, 2009 12 15, p. 42.

([2]) OL L 69, 2005 3 16, p. 67.

PRIĖMĖ ŠIĄ DIREKTYVĄ:

1 straipsnis

Dalykas

Šia direktyva nustatomos būtiniausios taisyklės, susijusios su nusikalstamų veikų apibrėžtimi, ir sankcijos atakų prieš informacines sistemas srityje. Ja taip pat siekiama sudaryti palankesnes sąlygas tokių nusikalstamų veikų prevencijai ir pagerinti teisminių ir kitų kompetentingų institucijų bendradarbiavimą.

2 straipsnis

Sąvokų apibrėžtys

Šioje direktyvoje vartojamos apibrėžtys:

a) „informacinė sistema“ – prietaisas arba tarpusavyje sujungtų ar susijusių prietaisų grupė, iš kurių vienas arba daugiau pagal programą vykdo automatinį kompiuterinių duomenų tvarkymą, taip pat kompiuteriniai duomenys, saugomi, tvarkomi, išrenkami arba perduodami to prietaiso ar grupės prietaisų jo ar jų eksploatacijos, naudojimo, apsaugos ir priežiūros tikslais;

b) „kompiuteriniai duomenys“ – faktai, informacija ar sąvokos, pateiktos tokia forma, kuri tinkama tvarkyti informacinėje sistemoje, įskaitant programą, tinkamą tam, kad informacinė sistema atliktų funkciją;

c) „juridinis asmuo“ – tokį statusą pagal taikytiną teisę turintis juridinis asmuo, išskyrus valstybes ar valstybinės valdžios funkcijas vykdančias viešąsias institucijas arba viešąsias tarptautines organizacijas;

d) „neturint tam teisės“ – elgesys, nurodytas šioje direktyvoje, įskaitant prieigą, įsikišimą ar duomenų perėmimą, kuriam sistemos ar jos dalies savininkas ar kitas teisės turėtojas nesuteikė leidimo, arba kuris neleidžiamas pagal nacionalinę teisę.

3 straipsnis

Neteisėta prieiga prie informacinių sistemų

Valstybės narės imasi būtinų priemonių užtikrinti, kad už prieigą prie visos informacinės sistemos arba bet kurios jos dalies neturint tam teisės, jei tai padaryta tyčia, būtų baudžiama kaip už nusikalstamą veiką, kai tai padaroma pažeidžiant apsaugos priemonę, bent tais atvejais, kurie nėra mažareikšmiai.

4 straipsnis

Neteisėtas įsikišimas į sistemą

Valstybės narės imasi būtinų priemonių užtikrinti, kad už rimtą informacinės sistemos veikimo sutrikdymą ar nutraukimą įvedant, perduodant, sugadinant, ištrinant, pažeidžiant, pakeičiant arba pašalinant kompiuterinius duomenis, arba užkertant prieigą prie tokių duomenų, jei tai padaryta tyčia ir neturint tam teisės, būtų baudžiama kaip už nusikalstamą veiką, bent tais atvejais, kurie nėra mažareikšmiai.

5 straipsnis

Neteisėtas įsikišimas į duomenis

Valstybės narės imasi būtinų priemonių užtikrinti, kad už informacinėje sistemoje esančių kompiuterinių duomenų ištrynimą, sugadinimą, pažeidimą, pakeitimą ar pašalinimą arba prieigos prie tokių duomenų užkirtimą, jei tai padaryta tyčia ir neturint tam teisės, būtų baudžiama kaip už nusikalstamą veiką, bent tais atvejais, kurie nėra mažareikšmiai.

6 straipsnis

Neteisėtas duomenų perėmimas

Valstybės narės imasi būtinų priemonių užtikrinti, kad už kompiuterinių duomenų, kurie ne viešai perduodami į informacinę sistemą, iš jos ar joje, įskaitant elektromagnetinę spinduliuotę iš tokius kompiuterinius duomenis turinčios informacinės sistemos, perėmimą techninėmis priemonėmis, jei tai padaryta tyčia ir neturint tam teisės, būtų baudžiama kaip už nusikalstamą veiką, bent tais atvejais, kurie nėra mažareikšmiai.

7 straipsnis

Nusikalstamoms veikoms vykdyti naudojamos priemonės

Valstybės narės imasi būtinų priemonių užtikrinti, kad už toliau nurodytų priemonių ar duomenų gamybą, pardavimą, įsigijimą siekiant naudotis, importą, platinimą arba kitu būdu galimybių naudotis viena iš šių priemonių sudarymą būtų baudžiama kaip už nusikalstamą veiką, bent tais atvejais, kurie nėra mažareikšmiai, jei tai padaryta tyčia, neturint tam teisės ir siekiant, kad jie būtų panaudoti 3–6 straipsniuose nurodytoms nusikalstamoms veikoms vykdyti:

a) kompiuterinės programos, skirtos arba pritaikytos pirmiausia siekiant vykdyti bet kurią iš 3–6 straipsniuose nurodytų veikų;

b) kompiuterio slaptažodžio, prieigos kodo arba panašių duomenų, kuriuos naudojant galima prisijungti prie visos informacinės sistemos arba jos dalies.

8 straipsnis

Kurstymas, bendrininkavimas ir kėsinimasis

1. Valstybės narės užtikrina, kad už kurstymą padaryti 3–7 straipsniuose nurodytą veiką ar pagalbą ir bendrininkavimą ją darant būtų baudžiama kaip už nusikalstamą veiką.

2. Valstybės narės užtikrina, kad už pasikėsinimą padaryti 4 ir 5 straipsniuose nurodytą veiką būtų baudžiama kaip už nusikalstamą veiką.

9 straipsnis

Sankcijos

1. Valstybės narės imasi reikiamų priemonių užtikrinti, kad už 3–8 straipsniuose nurodytas nusikalstamas veikas būtų taikomos veiksmingos, proporcingos ir atgrasančios baudžiamosios sankcijos.

2. Valstybės narės imasi būtinų priemonių užtikrinti, kad už 3–7 straipsniuose nurodytas nusikalstamas veikas būtų skiriama maksimali ne trumpesnė kaip dvejų metų laisvės atėmimo bausmė, bent tais atvejais, kurie nėra mažareikšmiai.

3. Valstybės narės imasi būtinų priemonių užtikrinti, kad už 4 ir 5 straipsniuose nurodytas nusikalstamas veikas, kai jos padaromos tyčia, būtų skiriama maksimali ne trumpesnė kaip

trejų metų laisvės atėmimo bausmė, kai dėl 7 straipsnyje nurodytos, būtent tam tikslui skirtos arba pritaikytos priemonės naudojimo nukenčia daug informacinių sistemų.

4. Valstybės narės imasi būtinų priemonių užtikrinti, kad už 4 ir 5 straipsniuose nurodytas nusikalstamas veikas būtų skiriama maksimali ne trumpesnė kaip penkerių metų laisvės atėmimo bausmė tuo atveju, jei:

a) jos padarytos nusikalstamos organizacijos, kaip apibrėžta Pamatiniame sprendime 2008/841/TVR, neatsižvelgiant į jame nurodytą sankcijos dydį;

b) jomis padaroma didelė žala; arba

c) jos nukreiptos prieš ypatingos svarbos infrastruktūros informacinę sistemą.

5. Valstybės narės imasi būtinų priemonių užtikrinti, kad jei 4 ir 5 straipsniuose nurodytos nusikalstamos veikos įvykdomos piktnaudžiaujant kito asmens duomenimis siekiant įgyti trečiosios šalies pasitikėjimą, tokiu būdu padarant žalą teisėtam tapatybės turėtojui, tai pagal nacionalinę teisę būtų laikoma sunkinančiomis aplinkybėmis, išskyrus tuo atveju, jei tos aplinkybės jau yra taikomos kitai nusikalstamai veikai, už kurią baudžiama pagal nacionalinę teisę.

10 straipsnis

Juridinių asmenų atsakomybė

1. Valstybės narės imasi būtinų priemonių užtikrinti, kad juridiniai asmenys galėtų būti patraukti atsakomybėn už 3–8 straipsniuose nurodytas nusikalstamas veikas, kurias jų naudai padarė asmuo, veikęs individualiai arba kaip tokio juridinio asmens struktūros narys ir užimantis to juridinio asmens struktūroje vadovaujamas pareigas, jeigu jis turėjo teisę:

a) remiantis įgaliojimu atstovauti juridiniam asmeniui;

b) juridinio asmens vardu priimti sprendimus;

c) vykdyti kontrolę juridinio asmens struktūroje.

2. Valstybės narės imasi būtinų priemonių užtikrinti, kad juridiniai asmenys galėtų būti laikomi atsakingais, jeigu dėl 1 dalyje minimo asmens priežiūros ar kontrolės stokos buvo sudarytos galimybės prižiūrimam asmeniui vykdyti bet kurią iš 3–8 straipsniuose nurodytų nusikalstamų veikų to juridinio asmens naudai.

3. Juridinių asmenų atsakomybė pagal 1 ir 2 dalis nepanaikina fizinių asmenų, kurie buvo kurios nors iš 3–8 straipsniuose nurodytų nusikalstamų veikų kaltininkai ar kurstytojai, ar bendrininkai, baudžiamosios atsakomybės.

11 straipsnis

Sankcijos juridiniams asmenims

1. Valstybės narės imasi būtinų priemonių užtikrinti, kad juridiniam asmeniui, patrauktam atsakomybėn pagal 10 straipsnio 1 dalį, būtų taikomos veiksmingos, proporcingos ir atgrasomosios sankcijos, kurios apima bausmes arba ne baudžiamojo pobūdžio baudas ir gali apimti kitas sankcijas, pavyzdžiui:

a) teisės į valstybės teikiamas lengvatas arba pagalbą atėmimą;

b) laikiną ar nuolatinį teisės verstis komercine veikla atėmimą;

c) teisminės priežiūros skyrimą;

d) teismo paskirtą likvidavimą;

e) laikiną ar galutinį įmonių, kurios buvo naudojamos nusikalstamai veikai įvykdyti, uždarymą.

2. Valstybės narės imasi būtinų priemonių užtikrinti, kad juridiniam asmeniui, patrauktam atsakomybėn pagal 10 straipsnio 2 dalį, būtų taikomos veiksmingos, proporcingos ir atgrasomosios sankcijos arba kitos priemonės.

12 straipsnis

Jurisdikcija

1. Valstybės narės nustato savo jurisdikciją 3–8 straipsniuose nurodytoms nusikalstamoms veikoms tais atvejais, kai:

a) nusikalstama veika arba jos dalis padaryta jų teritorijoje; arba

b) nusikalstamą veiką padarė vienas iš jų piliečių, bent tais atvejais, kai veiksmas yra nusikalstama veika toje vietoje, kurioje jis buvo įvykdytas.

2. Nustatydama jurisdikciją pagal 1 dalies a punktą, valstybė narė užtikrina, kad jos jurisdikcijai priklausytų atvejai, kai:

a) pažeidėjas nusikalstamą veiką įvykdo fiziškai būdamas jos teritorijoje, nepriklausomai nuo to, ar nusikalstama veika yra nukreipta ar nenukreipta prieš jos teritorijoje esančią informacinę sistemą; arba

b) nusikalstama veika yra nukreipta prieš jos teritorijoje esančią informacinę sistemą nepriklausomai nuo to, ar pažeidėjas nusikalstamą veiką daro fiziškai būdamas jos teritorijoje.

3. Valstybė narė praneša Komisijai, jeigu ji nusprendžia nustatyti papildomą jurisdikciją dėl 3–8 straipsniuose nurodytos nusikalstamos veikos, padarytos už jos teritorijos ribų, įskaitant, kai:

a) pažeidėjo įprastinė gyvenamoji vieta yra jos teritorijoje; arba

b) nusikalstama veika padaryta juridinio asmens, įsisteigusio jos teritorijoje, naudai.

13 straipsnis

Keitimasis informacija

1. Siekdamos keistis informacija apie 3–8 straipsniuose nurodytas nusikalstamas veikas, valstybės narės užtikrina, kad jos turėtų veikiantį nacionalinį informacinį punktą ir, kad jos naudotųsi esamu informacinių punktų, veikiančių ištisą parą be poilsio dienų, tinklu. Valstybės narės taip pat užtikrina, kad jos turėtų procedūras, kad skubių prašymų dėl pagalbos atvejais kompetentingos valdžios institucijos galėtų per ne ilgesnį nei aštuonių valandų laikotarpį nuo prašymo gavimo bent nurodyti, ar į prašymą bus atsakyta, bei kokia forma ir kada bus pateiktas toks atsakymas.

2. Valstybės narės informuoja Komisiją apie paskirtus informacinius punktus, nurodytus 1 dalyje. Komisija šią informaciją perduoda kitoms valstybėms narėms ir kompetentingoms specializuotoms Sąjungos agentūroms ir įstaigoms.

3. Valstybės narės imasi būtinų priemonių, kad užtikrintų galimybę naudotis tinkamais pranešimų teikimo kanalais siekiant sudaryti palankesnes sąlygas nedelsiant pranešti kompetentingoms nacionalinėms valdžios institucijoms apie 3–6 straipsniuose nurodytas nusikalstamas veikas.

14 straipsnis

Stebėjimas ir statistika

1. Valstybės narės užtikrina, kad būtų parengta sistema statistiniams duomenims apie 3–7 straipsniuose nurodytas veikas registruoti, rengti ir teikti.

2. 1 dalyje nurodyti statistiniai duomenys apima bent jau esamus duomenis apie veikų, nurodytų 3–7 straipsniuose, kurias užregistravo valstybės narės, skaičių ir kiek asmenų patraukta baudžiamojon atsakomybėn ir nuteista už 3–7 straipsniuose nurodytas veikas.

3. Pagal šį straipsnį surinktus duomenis valstybės narės perduoda Komisijai. Komisija užtikrina, kad būtų skelbiama bendra šių statistikos ataskaitų apžvalga ir kad ji būtų perduodama kompetentingoms specializuotoms Sąjungos agentūroms ir įstaigoms.

15 straipsnis

Pamatinio sprendimo 2005/222/TVR pakeitimas

Pamatinis sprendimas 2005/222/TVR yra pakeičiamas šia direktyva valstybių narių, dalyvaujančių priimant šią direktyvą, atžvilgiu, nedarant poveikio valstybių narių įsipareigojimams, susijusiems su pamatinio sprendimo perkėlimo į nacionalinę teisę terminu.

Valstybių narių, dalyvaujančių priimant šia direktyvą, atžvilgiu nuorodos į Pamatinį sprendimą 2005/222/TVR laikomos nuorodomis į šią direktyvą.

16 straipsnis

Perkėlimas į nacionalinę teisę

1. Valstybės narės užtikrina, kad įsigaliotų įstatymai ir kiti teisės aktai, būtini, kad šios direktyvos būtų laikomasi ne vėliau kaip nuo 2015 m. rugsėjo 4 d.

2. Valstybės narės perduoda Komisijai priemonių, kuriomis į jų nacionalinę teisę perkeliamos šia direktyva joms nustatytos pareigos, tekstą.

3. Valstybės narės, patvirtindamos tas priemones, daro jose nuorodą į šią direktyvą arba tokia nuoroda daroma jas oficialiai skelbiant. Nuorodos darymo tvarką nustato valstybės narės.

17 straipsnis

Ataskaitų teikimas

Komisija iki 2017 m. rugsėjo 4 d. Europos Parlamentui ir Tarybai pateikia ataskaitą, kurioje įvertinama, kokiu mastu valstybės narės ėmėsi šiai direktyvai įgyvendinti būtinų priemonių, ir, jei būtina, pasiūlymus dėl teisėkūros procedūra priimamų aktų. Komisija taip pat atsižvelgia į techninę ir teisinę raidą elektroninių nusikaltimų srityje, visų pirma kiek tai susiję su šios direktyvos taikymo sritimi.

18 straipsnis

Įsigaliojimas

Ši direktyva įsigalioja dvidešimtą dieną po jos paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

19 straipsnis

Adresatai

Ši direktyva pagal Sutartis skirta valstybėms narėms.

Priimta Briuselyje 2013 m. rugpjūčio 12 d.

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkas	*Pirmininkas*
M. SCHULZ	L. LINKEVIČIUS