EUROPOS KOMISIJA

Briuselis, 2010.9.30
KOM(2010) 517 galutinis

2010/0273 (COD)

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA

dėl atakų prieš informacines sistemas ir dėl Tarybos pamatinio sprendimo 2005/222/TVR panaikinimo

{SEC(2010) 1122 final}
{SEC(2010) 1123 final}

AIŠKINAMASIS MEMORANDUMAS

1. PASIŪLYMO PAGRINDAS IR TIKSLAI

Šio pasiūlymo tikslas – pakeisti 2005 m. vasario 24 d. Tarybos pamatinį sprendimą 2005/222/TVR dėl atakų prieš informacines sistemas[1]. Kaip nurodyta šio pamatinio sprendimo konstatuojamosiose dalyse, siekta gerinti valstybių narių teisminių ir kitų kompetentingų institucijų, įskaitant policijos ir kitas specializuotas teisėsaugos tarnybas, bendradarbiavimą derinant valstybių narių baudžiamosios teisės taisykles atakų prieš informacines sistemas srityje. Pradėti taikyti ES teisės aktai, skirti kovoti su tokiais nusikaltimais, kaip neteisėta prieiga prie informacinių sistemų, neteisėtas įsikišimas į sistemą ir neteisėtas įsikišimas į duomenis, taip pat nustatytos specialios taisyklės dėl juridinių asmenų atsakomybės, jurisdikcijos ir keitimosi informacija. Valstybių narių reikalauta imtis būtinų priemonių, kad iki 2007 m. kovo 16 d. būtų pradėta laikytis šio pamatinio sprendimo nuostatų.

2008 m. liepos 14 d. Komisija paskelbė Pamatinio sprendimo įgyvendinimo ataskaitą[2]. Ataskaitos išvadose nurodyta, kad daugelis valstybių narių padarė didelę pažangą ir pakankamai gerai įgyvendina sprendimą, tačiau kai kurios valstybės narės įgyvendinimo dar neužbaigė. Ataskaitoje taip pat nurodyta, kad „po to, kai priimtas Sprendimas, visoje Europoje įvykdytos atakos parodė, kad kyla naujų pavojų: vienu metu įvykdytos itin didelio masto atakos prieš informacines sistemas ir padidėjo vadinamųjų „zombių“ tinklų naudojimas nusikalstamiems tikslams.“ Priimant sprendimą šioms atakoms nebuvo skirta daug dėmesio. Siekdama reaguoti į šiuos pokyčius, Komisija svarstys veiksmus, kuriais būtų geriau reaguojama į grėsmes (žr. kitą dalį, kurioje paaiškinta, kas yra botnetas).

Tolesnių veiksmų griežčiau kovoti su elektroniniais nusikaltimais svarba buvo pabrėžta 2004 m. Hagos programoje dėl laisvės, saugumo ir teisingumo stiprinimo Europos Sąjungoje ir 2009 m. Stokholmo programoje ir jos veiksmų plane[3]. Be to, nesenai pristatytoje Europos skaitmeninėje darbotvarkėje[4], pirmoje pagal strategiją „Europa 2020“ parengtoje pavyzdinėje iniciatyvoje, pripažinta, kad būtina Europos mastu kovoti su naujų formų nusikaltimų, visų pirma elektroninių nusikaltimų, plitimu. Į pasitikėjimą ir saugumą orientuotų veiksmų srityje Komisija yra pasiryžusi imtis priemonių, skirtų kovoti su kibernetinėmis atakomis prieš informacines sistemas.

2001 m. lapkričio 23 d. pasirašyta Europos Tarybos konvencija dėl elektroninių nusikaltimų (toliau – Konvencija dėl elektroninių nusikaltimų) tarptautiniu mastu šiuo metu yra laikoma išsamiausiu tarptautiniu standartu, nes joje pateikta išsami ir nuosekli sistema, apimanti įvairius su elektroniniais nusikaltimais susijusius aspektus[5]. Visos 27 valstybės narės yra pasirašiusios Konvenciją, tačiau ją ratifikavo tik 15 valstybių narių[6]. Konvencija įsigaliojo 2004 m. liepos 1 d. ES šios konvencijos nėra pasirašiusi. Atsižvelgdama į šios priemonės

---

1 OL L 69, 2005 3 16, p. 68.

2 Komisijos ataskaita Tarybai parengta pagal 2005 m. vasario 24 d. Tarybos pamatinio sprendimo dėl atakų prieš informacines sistemas, COM (2008) 448, 12 straipsnį.

3 OL C 198, 2005 8 12, OL C 115, 2010 5 4 , COM (2010) 171, 2010 4 20.

4 2010 m. gegužės 19 d. Komisijos komunikatas COM (2010) 245.

5 2001 m. lapkričio 23 d. Budapešte pasirašyta Europos Tarybos konvencija dėl elektroninių nusikaltimų, CETS Nr. 185.

6 Konvencijos (CETS Nr. 185) ratifikavimo apžvalga pateikta adresu http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

svarbą, Komisija aktyviai ragina likusias ES valstybes nares kuo greičiau ratifikuoti Konvenciją.

- **Bendrosios aplinkybės**

Pagrindinė elektroninių nusikaltimų priežastis – pažeidžiamumas, kurį lemia įvairūs veiksniai. Minėti reiškiniai nepašalinami ir dėl nepakankamo atsako taikant teisėsaugos mechanizmus, sunkumų taip pat daugėja, nes tam tikros nusikalstamos veikos yra tarpvalstybinio pobūdžio. Dažnai apie tokio pobūdžio nusikaltimus nėra pranešama, iš dalies todėl, kad kai kurie nusikaltimai lieka nepastebėti, o kartais nukentėjusieji (ūkinės veiklos vykdytojai ir įmonės) apie nusikaltimus nepraneša baimindamiesi įgyti blogą reputaciją ir pakenkti įmonės ateities perspektyvoms viešai pranešus apie įmonės pažeidžiamumą.

Be to, dėl valstybių baudžiamosios teisės sistemos ir procedūrų skirtumų tokių nusikaltimų tyrimo ir traukimo baudžiamojon atsakomybėn tvarka gali skirtis, todėl kovoti su tokiais nusikaltimais gali tekti pasitelkiant skirtingas priemones. Dėl informacinių technologijų raidos tokių problemų dar padaugėjo, nes vis lengviau kuriamos ir platinamos priemonės (kenkimo programinė įranga ir botnetai), kaltininkai gali išlikti anonimiški, o atsakomybė spręsti klausimus priklauso skirtingoms jurisdikcijoms. Dėl sunkumų baudžiamojo persekiojimo srityje organizuoti nusikaltėliai gali daug uždirbti mažai rizikuodami.

Šiame pasiūlyme atsižvelgiama į naujus elektroninių nusikaltimų metodus, visų pirma botnetų panaudojimą. Sąvoka „botnetas“ reiškia kompiuterių, kuriuose įdiegta kenkimo programinė įranga (kompiuterio virusai), tinklą. Toks užkrėstų kompiuterių („zombių“) tinklas gali būti naudojamas konkretiems veiksmams atlikti, pavyzdžiui, atakoms prieš informacines sistemas (t. y. kibernetinėms atakoms) rengti. Šie „zombiai“ gali būti kontroliuojami iš kito kompiuterio, dažnai užkrėstų kompiuterių naudotojams visiškai nieko nežinant. Šis kontroliuojantis kompiuteris dar vadinamas komandų ir kontrolės centru. Šį centrą kontroliuojantys asmenys yra pažeidėjai, nes jie naudojasi užkrėstais kompiuteriais atakoms prieš informacines sistemas rengti. Nusikaltėlius susekti labai sunku, nes botnetui priklausantys kompiuteriai, naudojami atakoms rengti, gali būti visai kitoje vietoje nei pažeidėjas.

Botneto pagalba rengiamos atakos dažnai būna didelio masto. Didelio masto atakos yra tokios atakos, kurios rengiamos pasitelkiant priemones, dėl kurių nukenčia daug informacinių sistemų (kompiuterių), arba tokios atakos, dėl kurių patiriama didelė žala, pvz., dėl sutrikusių sistemos paslaugų, finansinių išlaidų, prarastų asmens duomenų ir t. t. Šiame kontekste didelis botnetas yra laikomas tinklu, galinčiu padaryti didelę žalą. Sunku nustatyti botnetų dydį, tačiau apskaičiuota, kad prisijungimų prie didžiausių nustatytų botnetų skaičius buvo nuo 40 000 iki 100 000 (t. y. užkrėstų kompiuterių) per 24 valandas[7].

[7] Prisijungimų skaičius per 24 valandas yra dažnai naudojamas matavimo vienetas botneto dydžiui nustatyti.

- **Pasiūlymo srityje galiojančios nuostatos**

Pamatiniu sprendimu nustatytas ES masto minimalus valstybių narių teisės aktų, pagal kuriuos baudžiama už įvairius elektroninius nusikaltimus, įskaitant neteisėtą prieigą prie informacinės sistemos, neteisėtą įsikišimą į sistemą, neteisėtą įsikišimą į duomenis, kurstymą, bendrininkavimą, kėsinimąsi ir mėginimą daryti tokius nusikaltimus, suderinimo lygis.

Nors valstybės narės iš esmės įgyvendino Pamatinio sprendimo nuostatas, dėl vis didesnio nusikalstamos veikos (kibernetinių atakų) masto ir dažnumo Sprendimas turi tam tikrų trūkumų. Sprendimu suderinamos tik ribotą skaičių nusikalstamų veikų reglamentuojančios nuostatos, tačiau nėra visapusiškai sprendžiama didelio masto atakų visuomenei keliamos potencialios grėsmės problema. Sprendime neatsižvelgiama į nusikaltimų sunkumą ir už juos taikomas sankcijas.

Kitomis vykdomomis arba suplanuotomis ES iniciatyvomis ir programomis taip pat iš dalies sprendžiamos su kibernetinėmis atakomis ar klausimais susijusios problemos, pavyzdžiui, tinklo saugumas ir interneto naudotojų sauga. Šios iniciatyvos apima veiksmus, remiamus pagal tokias programas, kaip „Nusikalstamumo prevencijos ir kovos su nusikalstamumu programa“[8], „Baudžiamojo teisingumo programa“[9], „Saugesnio interneto programa“[10] ir „Ypatingos svarbos informacinės infrastruktūros programa“[11]. Be Pamatinio sprendimo, kita svarbi taikoma teisinė priemonė yra Pamatinis sprendimas 2004/68/TVR dėl kovos su seksualiniu vaikų išnaudojimu ir vaikų pornografija.

Administraciniu lygmeniu kompiuterių užkrėtimas ir jų įtraukimas į botnetus jau yra draudžiamas pagal ES privatumo ir duomenų apsaugos taisykles[12]. Būtent nacionalinės administracinės agentūros jau bendradarbiauja pagal Europos kovos su brukalu institucijų ryšių tinklą. Remiantis šiomis taisyklėmis valstybių narių reikalaujama uždrausti perimti viešųjų ryšių tinklais perduodamus ryšių duomenis ir duomenis, naudojamus teikiant viešas elektroninių ryšių paslaugas, jeigu susiję vartotojai tam nėra davę sutikimo arba nėra teisėto leidimo.

Šio pasiūlymo nuostatos atitinka minėtas taisykles. Valstybės narės turėtų siekti gerinti administracinių ir teisėsaugos institucijų bendradarbiavimą nagrinėjant bylas, pagal kurias taikomos tiek administracinės, tiek baudžiamosios sankcijos.

- **Derėjimas su kitomis Sąjungos politikos sritimis ir tikslais**

Tikslai atitinka ES kovos su organizuotu nusikalstamumu politiką, kuria siekiama didinti kompiuterių tinklų atsparumą, ypatingos svarbos informacijos infrastruktūros ir duomenų apsaugą. Tikslai taip pat atitinka ir Saugesnio interneto programą, sukurtą siekiant skatinti saugesnį naudojimąsi internetu bei naujomis interneto technologijomis, ir kovoti su neteisėtu turiniu.

---

8 Žiūrėkite: http://ec.europa.eu/justice_home/funding/isec/funding_isec_en.htm.

9 Žiūrėkite: http://ec.europa.eu/justice_home/funding/jpen/funding_jpen_en.htm.

10 Žiūrėkite: http://ec.europa.eu/information_society/activities/sip/index_en.htm.

11 Žiūrėkite: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm.

12 Direktyva dėl privatumo ir elektroninių ryšių (OL L 201, 2002 7 31), iš dalies pakeista Direktyva 2009/136/EB (OL L 337, 2009 12 18).

Šis siūlymas kruopščiai išnagrinėtas siekiant užtikrinti, kad jo nuostatos visiškai atitiktų pagrindines teises ir, visų pirma, asmens duomenų apsaugos nuostatas, saviraiškos ir informacijos laisvės, teisės į teisingą bylos nagrinėjimą, nekaltumo prezumpcijos ir teisių į gynybą, taip pat baudžiamųjų nusikaltimų ir sankcijų teisėtumo ir proporcingumo principus.

2. KONSULTACIJOS SU SUINTERESUOTOMIS ŠALIMIS IR POVEIKIO VERTINIMAS

- **Konsultacijos su suinteresuotosiomis šalimis**

Įvairiuose posėdžiuose konsultuotasi su įvairiais šios srities ekspertais aptariant skirtingus kovos su elektroniniais nusikaltimais aspektus, įskaitant tolesnes teismines procedūras (traukimą baudžiamojon atsakomybėn) už šiuos nusikaltimus. Šiuose posėdžiuose visų pirma dalyvavo valstybių narių vyriausybių atstovai ir privačiojo sektoriaus atstovai, specializuoti teisėjai ir prokurorai, tarptautinių organizacijų, Europos agentūrų ir ekspertų įstaigų atstovai. Vėliau nemažai ekspertų ir organizacijų pateikė nuomones ir informaciją.

Po konsultacijų išaiškėjo:

– būtinybė ES imtis veiksmų šioje srityje;

– būtinybė bausti už nusikalstamas veikas, kurios neįtrauktos į dabartinį pamatinį sprendimą, ypač už naujų už formų kibernetines atakas (botnetai);

– būtinybė pašalinti tyrimo ir baudžiamojo persekiojimo kliūtis tarpvalstybinėse bylose.

Į konsultuojantis gautą informaciją atsižvelgta poveikio vertinime.

Tiriamųjų duomenų rinkimas ir naudojimas

Su išorės ekspertais konsultuotasi įvairiuose posėdžiuose su suinteresuotosiomis šalimis.

Poveikio vertinimas

Siekiant tikslo išnagrinėtos įvairios politikos galimybės.

- 1-oji politikos galimybė. *Status Quo* / Nesiimti naujų ES lygmens veiksmų

Ši galimybė reiškia, kad ES nesiims jokių tolesnių veiksmų kovoti su tokio pobūdžio elektroniniais nusikaltimais, t. y. su atakomis prieš informacines sistemas. Pradėti veiksmai bus tęsiami, visų pirma bus tęsiamos programos, kuriomis siekiama stiprinti ypatingos svarbos informacijos infrastruktūros apsaugą ir gerinti viešojo ir privačiojo sektorių bendradarbiavimą kovojant su elektroniniais nusikaltimais.

- 2-oji politikos galimybė. Programos, skirtos griežčiau kovoti su atakomis prieš informacines sistemas, plėtojimas taikant įstatymo galios neturinčias priemones

Įstatymo galios neturinčiomis priemonėmis, be ypatingos svarbos informacijos infrastruktūros apsaugos programos, dėmesys būtų sutelktas į tarpvalstybinį teisėsaugos ir viešojo bei privačiojo sektorių bendradarbiavimą. Šiomis privalomos teisinės galios neturinčiomis priemonėmis turėtų būti siekiama toliau skatinti suderintus ES veiksmus, įskaitant jau esamų ištisą parą be poilsio dienų veikiančių teisėsaugos institucijų informacinių punktų tinklo

stiprinimą; ES viešojo ir privačiojo sektorių informacinių punktų tinklo, įtraukiant elektroninių nusikaltimų ekspertus ir teisėsaugos institucijas sukūrimą; standartinio ES lygio susitarimo dėl paslaugų lygio teisėsaugos institucijoms bendradarbiaujant su privačiojo sektoriaus subjektais parengimą; paramą teisėsaugos institucijų mokymo programų, skirtų elektroninių nusikaltimų tyrimui, rengimui.

- 3-oji politikos galimybė. Pamatiniame sprendime nustatytų taisyklių tikslinis atnaujinimas (nauja direktyva pakeičiamas dabartinis Pamatinis sprendimas) siekiant šalinti didelio masto atakų prieš informacines sistemas (botnetų) grėsmes, taip pat didinti valstybių narių teisėsaugos institucijų informacinių punktų veiksmingumą, kai nusikaltimai daromi slepiant tikrąją nusikaltėlio tapatybę ir kenkiant teisėtam tapatybės turėtojui, taip pat spręsti statistinių duomenų apie kibernetines atakas trūkumo problemą.

Pagal šią galimybę numatoma parengti konkretų tikslinį (t. y. ribotos taikymo srities) teisės aktą, kad būtų užkirstas kelias didelio masto atakoms prieš informacines sistemas. Be tokio griežtesnio teisės akto būtų taikomos ir įstatymo galios neturinčios priemonės, skirtos padėti įgyvendinti teisines priemones ir stiprinti operatyvinį tarpvalstybinį bendradarbiavimą kovojant su tokiomis atakomis. Šių priemonių tikslas – stiprinti parengtį, ypatingos svarbos informacijos infrastruktūros saugumą bei atsparumą ir keistis gerąja patirtimi.

- 4-oji politikos galimybė. Išsamus ES teisės aktas dėl kovos su elektroniniais nusikaltimais

Renkantis šią galimybę reikėtų parengti naują išsamų ES teisės aktą. Be naujų privalomos teisinės galios neturinčių priemonių pagal 2 politikos galimybę ir politikos atnaujinimo pagal 3 politikos galimybę, būtų sprendžiamos kitos teisinės problemos, susijusios su interneto naudojimu. Tokios priemonės aprėptų ne tik atakas prieš informacines sistemas, bet ir tokius klausimus, kaip finansiniai elektroniniai nusikaltimai, neteisėtas interneto turinys, elektroninių įrodymų rinkimas, saugojimas, perkėlimas ir išsamesnės jurisdikcijos taisyklės. Teisės aktas būtų taikomas kartu su Europos Tarybos konvencija dėl elektroninių nusikaltimų, į jį būtų įtrauktos minėtos papildomosios įstatymo galios neturinčios priemonės.

- 5-oji politikos galimybė. Europos Tarybos konvencijos dėl elektroninių nusikaltimų atnaujinimas

Pasirinkus šią galimybę reikėtų iš naujo iš esmės derėtis dėl dabartinės Konvencijos, o tai užtruktų ilgai ir neatitiktų Poveikio vertinime siūlomo laikotarpio, per kurį reikia imtis veiksmų. Be to, nepanašu, kad Susitariančios šalys norėtų iš naujo derėtis dėl Konvencijos. Todėl Konvencijos atnaujinimas nelaikomas įmanoma galimybe, nes neatitinka laikotarpio, per kurį būtina imtis veiksmų.

Tinkamiausia politikos galimybė – įstatymo galios neturinčių priemonių (2 galimybė) ir Pamatinio sprendimo tikslinio atnaujinimo (3 galimybė) derinys

Atsižvelgiant į ekonominio ir socialinio poveikio, taip pat poveikio pagrindinėms teisėms analizę, 2 ir 3 politikos galimybės yra geriausias būdas problemai spręsti ir pasiūlymo tikslams pasiekti.

Rengdama šį pasiūlymą Komisija atliko poveikio vertinimą.

3. TEISINIAI PASIŪLYMO ASPEKTAI

- **Siūlomų veiksmų santrauka**

Direktyvoje, kuria panaikinamas Pamatinis sprendimas 2005/222/TVR, išliks šio sprendimo nuostatos ir bus įtraukti šie nauji elementai:

– Materialinės baudžiamosios teisės srityje šia direktyva:

A. Reglamentuojamos sankcijos už nusikalstamai veikai daryti naudojamų įrenginių ir (arba) priemonių gamybą, pardavimą, įsigijimą siekiant naudotis, importą, platinimą arba galimybių jais naudotis sudarymą kitu būdu.

B. Įtraukiamos nuostatos dėl sunkinančių aplinkybių:

- didelio masto atakų rengimo, botnetų ar panašių priemonių naudojimo problema būtų sprendžiama įtraukiant nuostatas dėl sunkinančių aplinkybių, t. y. botneto kūrimas arba panašių priemonių naudojimas darant Pamatiniame sprendime išvardytus nusikaltimus būtų laikomas sunkinančia aplinkybe;

- kai tokios atakos rengiamos slepiant tikrąją nusikaltėlio tapatybę ir daroma žala teisėtam tapatybės turėtojui. Tokios taisyklės turėtų derėti su baudžiamųjų nusikaltimų ir bausmių teisėtumo ir proporcingumo principais ir galiojančiais asmens duomenų apsaugą reglamentuojančiais teisės aktais[13].

C. Įtraukiamos nuostatos, pagal kurias neteisėtas duomenų perėmimas laikomas nusikalstama veika.

D. Nustatomos priemonės bendradarbiavimui baudžiamosios teisenos srityje gerinti stiprinant ištisą parą be poilsio dienų veikiančių informacinių punktų struktūrą[14]:

- siūloma laikytis įsipareigojimo tenkinti informacinių punktų prašymą suteikti pagalbą per tam tikrą nustatytą laikotarpį (Direktyvos 14 straipsnis). Konvencijoje dėl elektroninių nusikaltimų tokios privalomos nuostatos nėra. Šios priemonės tikslas – užtikrinti, kad informaciniai punktai per nurodytą terminą atsakytų, ar jie galėtų patenkinti prašymą suteikti pagalbą ir kiek laiko reikėtų, kad pagalba būtų suteikta. Nenurodyta, kokio pobūdžio pagalba būtų teikiama.

E. Reaguojama į būtinybę parengti statistinius duomenis apie elektroninius nusikaltimus įpareigojant valstybes nares užtikrinti, kad būtų parengta tinkama statistinių duomenų apie Pamatiniame sprendime nurodytus elektroninius nusikaltimus registravimo, rengimo ir teikimo sistema.

Šioje direktyvoje pateiktos 3, 4 ir 5 straipsniuose išvardytų nusikalstamų veikų (neteisėta prieiga prie informacinių sistemų, neteisėtas įsikišimas į sistemas ir neteisėtas įsikišimas)

---

[13] Pavyzdžiui, 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių), OL L 201, 2002 7 31, p. 37 (šiuo metu peržiūrima), ir Direktyva 95/46/EB dėl bendros duomenų apsaugos.

[14] Informaciniai punktai sukurti Konvencija ir Pamatiniu sprendimu 2005/222/TVR dėl atakų prieš informacines sistemas.

sąvokos, į kurias įtraukta nuostata, pagal kurią perkeliant direktyvą į nacionalinę teisę leidžiama bausti tik tais atvejais, kurie nėra nereikšmingi. Šiuo lankstumo elementu valstybėms narėms siekiama suteikti teisę neįtraukti atvejų, kuriems *in abstracto* būtų taikoma pagrindinė apibrėžtis, bet kurie nelaikomi galinčiais pakenkti saugomiems teisėtiems interesams, pvz., visų pirma jaunuolių pastangoms įrodyti savo kompetenciją informacijos technologijų srityje. Tačiau ši galimybė riboti baudžiamosios atsakomybės taikymą neturėtų reikšti, kad įtraukiami nauji papildomi nusikalstamų veikų, jau įtrauktų į šią direktyvą, sudėties požymiai, nes taip Direktyva būtų taikoma tik pažeidimams, padarytiems sunkinančiomis aplinkybėmis. Perkeldamos šią direktyvą į nacionalinę teisę, valstybės narės neturėtų įtraukti papildomų pagrindinių nusikalstamų veikų sudėties požymių, pvz., ketinimas darant nusikaltimą siekti gauti neteisėtų pajamų arba specialaus poveikio, pvz., padaroma didelė žala, buvimas.

- **Teisinis pagrindas**

Sutarties dėl Europos Sąjungos veikimo 83 straipsnio 1 dalis[15].

- **Subsidiarumo principas**

Europos Sąjungos veiksmams taikomas subsidiarumo principas. Šio pasiūlymo tikslų valstybės narės negali tinkamai pasiekti dėl toliau nurodytų priežasčių.

Elektroniniams nusikaltimams, visų pirma atakoms prieš informacines sistemas, būdingas tarpvalstybinis matmuo, ypač akivaizdus kai rengiamos didelio masto atakos, nes dažnai jungiamieji elementai yra skirtingose vietose ir skirtingose šalyse. Būtini ES veiksmai, visų pirma siekiant kovoti su plintančiomis didelio masto atakomis Europoje ir visame pasaulyje. Imtis ES veiksmų ir atnaujinti Pamatinį sprendimą 2005/222/TVR taip pat paraginta 2008 m. lapkričio mėn. posėdžiavusios Tarybos išvadose[16], nes veikdamos pavieniui valstybės narės negali veiksmingai apsaugoti piliečių nuo elektroninių nusikaltimų.

Pasiūlyme iškeltus tikslus lengviau bus pasiekti bendrais Europos Sąjungos veiksmais dėl toliau nurodytų priežasčių.

Pasiūlymu bus toliau derinamos valstybių narių materialinės ir procesinės baudžiamosios teisės normos, tai padės kovoti su minėtais nusikaltimais. Pirma, taip bus užkirstas kelias nusikaltėliams iš vienos valstybės narės persikelti į kitą valstybę narę, kurioje kibernetines atakas reglamentuojantys teisės aktai yra ne tokie griežti. Antra, dėl bendrų apibrėžčių galima keistis informacija, rinkti ir palyginti svarbius duomenis. Trečia, būtų užtikrintas didesnis prevencijos priemonių veiksmingumas visoje ES ir sustiprintas tarptautinis bendradarbiavimas.

Todėl pasiūlymas atitinka subsidiarumo principą.

- **Proporcingumo principas**

Pasiūlymas atitinka proporcingumo principą dėl toliau nurodytos priežasties.

---

[15] OL C 83, 2010 3 30, p. 49.

[16] 2008 m. lapkričio 27–28 d. Briuselyje surengtame 2987-ajame Teisingumo ir vidaus reikalų tarybos posėdyje parengta „Suderinta darbo strategija ir praktinės kovos su elektroniniais nusikaltimais priemonės“.

Šia direktyva neviršijama to, kas būtina nurodytiems tikslams Europos lygmeniu pasiekti, ir joje nenumatyta jokių veiksmų, kurie nėra būtini siekiant šio tikslo, atsižvelgiant į

baudžiamosios teisės aktų tikslumo būtinybę.

- **Pasirinkta priemonė**

Pasiūlyta priemonė – direktyva.

Kitos priemonės būtų netinkamos dėl šios priežasties:

Teisiniam pagrindui būtina direktyva.

Įstatymo galios neturinčios priemonės ir savireguliacija padėtų pagerinti padėtį tam tikrose srityse, kuriose itin svarbus įgyvendinimas. Tačiau kitose srityse, kuriose reikalingas naujas teisės aktas, nauda būtų nedidelė.

4. POVEIKIS BIUDŽETUI

Pasiūlymo poveikis Sąjungos biudžetui yra nedidelis. Daugiau kaip 90 % numatomų išlaidų (5 913 000 EUR) padengtų valstybės narės; galima prašyti skirti ES finansavimą išlaidoms sumažinti.

5. PAPILDOMA INFORMACIJA

- **Galiojančių teisės aktų panaikinimas**

Priėmus šį pasiūlymą, galiojantis teisės aktas bus panaikintas.

- **Teritorinio taikymo sritis**

Ši direktyva pagal Sutartis skirta valstybėms narėms.

2010/0273 (COD)

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA

dėl atakų prieš informacines sistemas ir dėl Tarybos pamatinio sprendimo 2005/222/TVR panaikinimo

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[17],

teisės akto pasiūlymą perdavus nacionaliniams parlamentams,

atsižvelgdami į Europos ekonomikos ir socialinių reikalų komiteto nuomonę,

atsižvelgdami į Regionų komiteto nuomonę,

laikydamiesi įprastos teisėkūros procedūros,

kadangi:

(1) Šios direktyvos tikslas yra suderinti valstybių narių baudžiamosios teisės taisykles atakų prieš informacines sistemas srityje ir pagerinti valstybių narių teisminių ir kitų kompetentingų institucijų, įskaitant policiją ir kitas specializuotas teisėsaugos tarnybas, bendradarbiavimą.

(2) Atakų prieš informacines sistemas grėsmė didėja, ypač dėl organizuoto nusikalstamumo grėsmės, todėl vis didesnį susirūpinimą kelia galimi teroristų išpuoliai ar atakos dėl politinių motyvų 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 bei teisingumo erdvė, taigi reikia imtis bendrų Europos Sąjungos veiksmų.

(3) Akivaizdu, kad daugėja pavojingų ir pakartotinių didelio masto atakų prieš informacines sistemas, kurios yra ypatingai svarbios valstybėms arba konkrečioms viešojo ar privačiojo sektoriaus funkcijoms. Be šios tendencijos taip pat pastebėta, kad kuriamos vis modernesnės priemonės, kurias nusikaltėliai gali naudoti įvairaus pobūdžio kibernetinėms atakoms rengti.

[17] OL C[…], […], p. […].

(4) Šioje srityje bendros, ypač informacinių sistemų ir kompiuterinių duomenų, sąvokų apibrėžtys yra svarbios, kad valstybėse narėse būtų užtikrintas nuoseklus požiūris taikant šią direktyvą.

(5) 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.

(6) Valstybės narės turėtų nustatyti sankcijas už atakas prieš informacines sistemas. Nustatytos sankcijos turėtų būti veiksmingos, proporcingos ir atgrasančios.

(7) 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[18], kai ataka vykdoma plačiu mastu arba kai nusikalstama veika daroma slepiant tikrąją nusikaltėlio tapatybę ir kenkiant teisėtam tapatybės turėtojui. Taip pat tikslinga numatyti griežtesnes sankcijas tais atvejais, kai tokia ataka padarė didelę žalą arba padarė poveikį esminiams interesams.

(8) 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. Ši konvencija yra orientacinis kovos su elektroniniais nusikaltimais, įskaitant atakas prie informacines sistemas, teisinis pagrindas. Ši direktyva grindžiama šia konvencija.

(9) Atsižvelgiant į skirtingus atakų rengimo būdus ir spartų techninės ir programinės kompiuterių įrangos tobulėjimą, šioje direktyvoje sąvoka „priemonės“ reiškia išvardytiems nusikaltimams daryti naudojamas priemones. Priemonės, pavyzdžiui, reiškia kibernetinėms atakoms rengti naudojamą kenkimo programinę įrangą, įskaitant botnetus.

(10) Šia direktyva nesiekiama nustatyti baudžiamosios atsakomybės tais atvejais, kai nusikalstama veika padaroma netyčia, pavyzdžiui, siekiant atlikti leistiną informacinių sistemų tikrinimą arba siekiant jas apsaugoti.

(11) Šia direktyva didinama tinklų, pavyzdžiui didžiojo aštuoneto arba Europos Tarybos sukurtų ištisą parą be poilsio dienų veikiančių informacinių punktų, skirtų keistis informacija siekiant nedelsiant suteikti pagalbą tiriant su informacinėmis sistemomis ir duomenimis susijusias nusikalstamas veikas arba nagrinėjant tokias bylas, arba renkant nusikalstamos veikos įrodymus elektroniniu formatu, tinklo svarba. Atsižvelgiant į tai, kad didelio masto atakos gali būti įvykdytos labai greitai, valstybės narės turėtų būti pajėgios nedelsiant reaguoti į šio informacinių punktų tinklo skubius prašymus. Teikiant pagalbą turėtų būti sudaromos geresnės sąlygos taikyti tokias priemones arba tiesiogiai jų imtis: techninių konsultacijų teikimas, duomenų išsaugojimas, įrodymų rinkimas, teisinės informacijos teikimas ir įtariamųjų buvimo vietos nustatymas.

---

[18] OL L 300, 2008 11 11, p. 42.

(12) Būtina rinkti duomenis apie nusikalstamas veikas, apibrėžtas šioje direktyvoje, kad būtų surinkta išsamesnės informacijos apie problemos mastą Sąjungos lygiu ir tokiu būdu būtų ieškoma veiksmingesnių problemos sprendimo būdų. Be to, tokie duomenys padės tokioms specializuotoms agentūroms, kaip Europolas ir Europos tinklų ir informacijos apsaugos agentūra, geriau vertinti elektroninių nusikaltimų mastą ir tinklo bei informacijos saugumo padėtį Europoje.

(13) Didelės spragos valstybių narių įstatymuose ir dideli įstatymų skirtumai šioje 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, atakos prieš tokias sistemas dažnai būna tarpvalstybinio pobūdžio, todėl pabrėžiamas poreikis skubiai veikti toliau derinant baudžiamosios teisės aktus šioje srityje. Be to, priėmus Tarybos pamatinį sprendimą 2009/948/TVR dėl jurisdikcijos įgyvendinimo kolizijų baudžiamuosiuose procesuose prevencijos ir sprendimo, būtų sukurtos palankesnės sąlygos derinti atakų prieš informacines sistemas atvejų baudžiamąjį persekiojimą.

(14) Kadangi šios direktyvos tikslų, t. y. užtikrinti, kad valstybėse narėse už atakas prieš informacines sistemas būtų baudžiama taikant veiksmingas, proporcingas ir atgrasančias baudžiamąsias sankcijas, ir gerinti bei skatinti teisminį bendradarbiavimą pašalinant potencialias komplikacijas, valstybės narės negali deramai pasiekti, nes taisyklės turi būti bendros ir suderinamos, ir kadangi dėl to tų tikslų būtų geriau siekti Sąjungos lygmeniu, laikydamasi Sutarties dėl Europos Sąjungos veikimo 5 straipsnyje nustatyto proporcingumo principo Sąjunga gali patvirtinti priemones. Šioje direktyvoje nenumatyta daugiau nei būtina šiems tikslams pasiekti.

(15) Įgyvendinant šią direktyvą tvarkomi asmens duomenys turėtų būti saugomi remiantis duomenų apsaugos taisyklėmis, nustatytomis 2008 m. lapkričio 27 d. Tarybos pamatiniame sprendime 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos[19], kai tokia tvarkymo veikla patenka į šio sprendimo taikymo sritį, ir atsižvelgiant į 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentą (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo[20].

(16) Šia direktyva užtikrinamos pagrindinės teisės ir laikomasi principų, visų pirma pripažintų Europos Sąjungos pagrindinių teisių chartijoje, t. y.: asmens duomenų apsaugos, saviraiškos ir informacijos laisvės, teisės į teisingą bylos nagrinėjimą, nekaltumo prezumpcijos ir gynybos teises, taip pat teisėtumo ir nusikalstamos veikos bei bausmės proporcingumo principų. Visų pirma, šia direktyva siekiama užtikrinti, kad būtų besąlygiškai laikomasi visų šių teisių ir principų, ir ji atitinkamai turi būti įgyvendinama.

(17) [Pagal Protokolo dėl Jungtinės Karalystės ir Airijos pozicijos laisvės, saugumo ir teisingumo srityje, pridėto prie Sutarties dėl Europos Sąjungos veikimo, 1, 2, 3 ir 4 straipsnius Jungtinė Karalystė ir Airija pranešė apie pageidavimą dalyvauti priimant ir taikant šią direktyvą.] ARBA [Nepažeidžiant Protokolo dėl Jungtinės Karalystės ir

---

[19] OL L 350, 2008 12 30, p. 60.
[20] OL L 8, 2001 1 12, p. 1.

Airijos pozicijos laisvės, saugumo ir teisingumo srityje 4 straipsnio Jungtinė Karalystė ir Airija nedalyvaus priimant šią direktyvą, ji nebus joms privaloma ar taikoma].

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

PRIĖMĖ ŠIĄ DIREKTYVĄ:

1 straipsnis
Dalykas

Šia direktyva apibrėžiamos nusikalstamos veikos atakų prieš informacines sistemas srityje ir nustatomos minimalios sankcijų už tokias veikas taisyklės. Ja taip pat siekiama nustatyti bendras tokių atakų prevencijos nuostatas ir gerinti su tokiomis atakomis susijusį bendradarbiavimą baudžiamosios teisenos srityje.

2 straipsnis
Apibrėžtys

Šioje direktyvoje vartojamos tokios sąvokų 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 juose saugomi, tvarkomi, iš jų išrenkami arba jais perduodami kompiuteriniai duomenys su tikslu juos apdoroti, panaudoti, apsaugoti ir prižiūrėti;

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 subjektas, išskyrus valstybes arba kitas valdžios funkcijas vykdančias viešąsias įstaigas, taip pat viešąsias tarptautines organizacijas;

d) „neturint tam teisės“ – prieiga ar įsikišimas, kuriam nesuteikė leidimo sistemos ar jos dalies savininkas, kitas teisės turėtojas, arba kuris neleidžiamas pagal nacionalinės teisės aktus.

3 straipsnis
Neteisėta prieiga prie informacinių sistemų

Valstybės narės imasi būtinų priemonių užtikrinti, kad už tyčinę prieigą prie visos informacinės sistemos arba jos dalies neturint tam teisės būtų baudžiama kaip už nusikalstamą veiką, bent tais atvejais, kurie nėra nereikšmingi.

4 straipsnis

Neteisėtas įsikišimas į sistemą

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

5 straipsnis

Neteisėtas įsikišimas į duomenis

Valstybės narės imasi būtinų priemonių užtikrinti, kad už tyčinį informacinėje sistemoje esančių kompiuterinių duomenų ištrynimą, sugadinimą, pažeidimą, pakeitimą, pašalinimą arba prieigos prie jų užkirtimą, jei tai padaryta neturint tam teisės, būtų baudžiama kaip už nusikaltimą, bent tais atvejais, kurie nėra nereikšmingi.

6 straipsnis

Neteisėtas duomenų perėmimas

Valstybės narės imasi būtinų priemonių užtikrinti, kad už tyčinę veiką, kai tam neturint teisės naudojant technines priemones perimami į informacinę sistemą, iš jos ar joje ne viešai perduodami kompiuteriniai duomenys, įskaitant elektromagnetinę spinduliuotę iš tokius kompiuterinius duomenis turinčios informacinės sistemos, būtų baudžiama kaip už nusikalstamą veiką.

7 straipsnis

Nusikaltimams daryti naudojamos priemonės

Valstybės narės imasi būtinų priemonių užtikrinti, kad už toliau nurodytų priemonių ar duomenų gamybą, pardavimą, įsigijimą siekiant naudotis, importą, turėjimą, platinimą arba galimybių jais naudotis sudarymą kitu būdu būtų baudžiama kaip už nusikalstamą veiką, kai tyčia ir neturint tam teisės siekiama daryti šios direktyvos 3–6 straipsniuose nurodytas veikas:

a) prietaiso, įskaitant kompiuterinę programą, skirto arba pritaikyto visų pirma siekiant daryti bet kurią nusikalstamą veiką, nurodytą 3–6 straipsniuose;

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

8 straipsnis

Kurstymas, bendrininkavimas ir kėsinimasis

1. Valstybės narės užtikrina, kad už kurstymą padaryti 3–7 straipsniuose nurodytą veiką bei bendrininkavimą jį darant būtų baudžiama kaip už nusikalstamą veiką.

2. Valstybės narės užtikrina, kad už pasikėsinimą padaryti 3–6 straipsniuose nurodytas veikas 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.

10 straipsnis

Atsakomybę sunkinančios aplinkybės

1. Valstybės narės imasi būtinų priemonių užtikrinti, kad už 3–7 straipsniuose nurodytas nusikalstamas veikas būtų skiriamos maksimalios ne trumpesnės kaip penkerių metų laisvės atėmimo bausmės, kai nusikalstama veika padaryta nusikalstamos organizacijos, kaip apibrėžta Pamatiniame sprendime 2008/841/TVR.

2. Valstybės narės imasi būtinų priemonių užtikrinti, kad už 3–6 straipsniuose nurodytas nusikalstamas veikas būtų skiriamos maksimalios ne trumpesnės kaip penkerių metų laisvės atėmimo bausmės, kai nusikalstama veika yra padaryta naudojant priemonę, skirtą atakoms, dėl kurių nukenčia daug informacinių sistemų, arba atakoms, dėl kurių patiriama didelė žala, pvz., dėl sutrikusių sistemos paslaugų, finansinių išlaidų arba prarastų asmens duomenų, rengti.

3. Valstybės narės imasi būtinų priemonių užtikrinti, kad už 3–6 straipsniuose nurodytas nusikalstamas veikas būtų skiriamos maksimalios ne trumpesnės kaip *penkerių metų* laisvės atėmimo bausmės, kai nusikaltimas yra padarytas slepiant tikrąją nusikaltėlio tapatybę ir daroma žala teisėtam tapatybės turėtojui.

11 straipsnis

Juridinių asmenų atsakomybė

1. Valstybės narės imasi būtinų priemonių užtikrinti, kad juridiniai asmenys galėtų būti traukiami 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) įgaliojimu atstovauti juridiniam asmeniui;

   b) juridinio asmens vardu priimti sprendimus, arba

   c) vykdyti kontrolę juridinio asmens struktūroje.

2. Valstybės narės imasi būtinų priemonių užtikrinti, kad juridiniai asmenys galėtų būti laikomi atsakingais, jeigu dėl šio straipsnio 1 dalyje minimo asmens priežiūros ar kontrolės stokos jo prižiūrimas asmuo galėjo daryti bet kurią iš 3–8 straipsniuose minimų nusikalstamų veikų to juridinio asmens naudai.

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

12 straipsnis
Sankcijos juridiniams asmenims

1. Valstybės narės imasi būtinų priemonių užtikrinti, kad juridiniam asmeniui, patrauktam atsakomybėn pagal 11 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 11 straipsnio 2 dalį, būtų taikomos veiksmingos, proporcingos ir atgrasančios sankcijos arba priemonės.

13 straipsnis
Jurisdikcija

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

   a) nusikalstama veika arba jos dalis padaryta atitinkamos valstybės narės teritorijoje; arba

   b) nusikalstamą veiką padarė vienas iš jų piliečių arba asmenų, kurio įprastinė gyvenamoji vieta yra atitinkamos valstybės narės teritorijoje; arba

   c) nusikalstama veika padaryta juridinio asmens, kurio pagrindinė buveinė yra atitinkamos valstybės narės teritorijoje, naudai.

2. Nustatydamos jurisdikciją pagal 1 dalies a punktą, valstybės narės užtikrina, kad jos jurisdikcijai priklausytų atvejai, kai:

   a) pažeidėjas nusikalstamą veiką daro 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 atitinkamos valstybės narės teritorijoje esančią informacinę sistemą nepriklausomai nuo to, pažeidėjas nusikalstamą veiką daro fiziškai būdamas jos teritorijoje.

14 straipsnis
Keitimasis informacija

1. Siekdamos keistis informacija apie 3–8 straipsniuose nurodytas nusikalstamas veikas ir laikydamosi duomenų apsaugos taisyklių valstybės narės naudojasi esamu informacinių punktų, veikiančių ištisą parą be poilsio dienų, tinklu. Valstybės narės taip pat užtikrina, kad būtų įtvirtintos procedūros, kad į skubius prašymus būtų reaguojama ne ilgiau kaip per aštuonias valandas. Reaguojant į prašymus nurodoma, ar prašymas bus patenkintas, kokia forma ir kada bus pateiktas atsakymas į prašymą.

2. Valstybės narės informuoja Komisiją apie paskirtus informacinius punktus, per kuriuos keičiamasi informacija apie 3–8 straipsniuose nurodytas nusikalstamas veikas. Komisija šią informaciją perduoda kitoms valstybėms narėms.

15 straipsnis
Stebėjimas ir statistika

1. Valstybės narės užtikrina, kad būtų parengta sistema statistiniams duomenims apie 3–8 straipsniuose nurodytas nusikalstamas veikas registruoti, rengti ir teikti.

2. Šio straipsnio 1 dalyje nurodyti statistiniai duomenys apima bent jau nusikalstamų veikų, nurodytų 3–8 straipsniuose, skaičių, kuris pranešamas valstybėms narėms, ir tolesnes priemones po tokių ataskaitų, taip pat nurodoma, kiek per metus tirta praneštų atvejų, kiek asmenų patraukta baudžiamojon atsakomybėn ir kiek asmenų nuteista už 3–8 straipsniuose nurodytas nusikalstamas veikas.

3. Pagal šio straipsnio nuostatas surinktus duomenis valstybės narės perduoda Komisijai. Valstybės narės pasirūpina, kad būtų skelbiama bendra šių statistikos ataskaitų apžvalga.

16 straipsnis
Pamatinio sprendimo 2005/222/TVR panaikinimas

Šia direktyva Pamatinis sprendimas 2005/222/TVR panaikinamas nepažeidžiant valstybių narių pareigų, susijusių su perkėlimo į nacionalinę teisę terminais.

Nuorodos į panaikintą pamatinį sprendimą laikomos nuorodomis į šią direktyvą.

17 straipsnis
Perkėlimas į nacionalinę teisę

1. Valstybės narės priima šios direktyvos įgyvendinimo įstatymus ir kitus teisės aktus, kurie įsigalioja ne vėliau kaip [po dvejų metų nuo direktyvos priėmimo]. Jos nedelsdamos pateikia Komisijai priimtų nuostatų tekstus ir minėtų nuostatų bei šios direktyvos atitikties lentelę. Priimdamos tas nuostatas, valstybės narės daro jose

nuorodą į šią direktyvą arba tokia nuoroda daroma jas oficialiai skelbiant. Valstybės narės nustato tokios nuorodos darymo tvarką.

2. Valstybės narės pateikia Komisijai šios direktyvos taikymo srityje priimtų pagrindinių nacionalinės teisės nuostatų tekstą.

18 straipsnis
Ataskaitų teikimas

1. Iki [KETVERI METAI NUO PRIĖMIMO] ir paskui kas trejus metus Komisija Europos Parlamentui ir Tarybai pateikia šios direktyvos taikymo valstybėse narėse ataskaitą, įskaitant visus būtinus pasiūlymus.

2. Valstybės narės pateikia Komisijai visą informaciją, reikalingą šio straipsnio 1 dalyje nurodytai ataskaitai parengti. Be kita ko, pateikiamas išsamus šiai direktyvai įgyvendinti priimtų teisėkūros ir ne teisėkūros priemonių aprašas.

19 straipsnis
Įsigaliojimas

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

20 straipsnis
Adresatai

Ši direktyva pagal Sutartis skirta valstybėms narėms.

Priimta Briuselyje

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkas	*Pirmininkas*