EIROPAS KOMISIJA

Briselē, 30.9.2010
COM(2010) 517 galīgā redakcija

2010/0273 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES DIREKTĪVA

par uzbrukumiem informācijas sistēmām, un ar ko atceļ Padomes Pamatlēmumu 2005/222/TI

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

PASKAIDROJUMA RAKSTS

1. PRIEKŠLIKUMA PAMATOJUMS UN MĒRĶI

Priekšlikuma mērķis ir aizstāt Padomes 2005. gada 24. februāra Pamatlēmumu 2005/222/TI par uzbrukumiem informācijas sistēmām[1]. Pamatlēmuma mērķis, kā norādīts tā apsvērumos, bija uzlabot tiesu un citu kompetento iestāžu, tostarp policijas un citu specializētu tiesībaizsardzības dienestu sadarbību, tuvinot dalībvalstu krimināltiesību noteikumus, kas attiecas uz uzbrukumiem informācijas sistēmām. Ar to tika ieviests ES līmeņa tiesiskais regulējums attiecībā uz tādiem nodarījumiem kā nelikumīga piekļuve informācijas sistēmām, nelikumīga iejaukšanās sistēmā un nelikumīga iejaukšanās datos, kā arī īpaši noteikumi par juridisko personu atbildību, jurisdikciju un informācijas apmaiņu. Dalībvalstīm bija jāveic vajadzīgie pasākumi, lai līdz 2007. gada 16. martam īstenotu šā pamatlēmuma noteikumus.

Komisija 2008. gada 14. jūlijā publicēja ziņojumu par pamatlēmuma īstenošanu[2]. Ziņojuma secinājumos tika norādīts, ka vairumā dalībvalstu ir sasniegts ievērojams progress un īstenošanas līmenis ir relatīvi labs, taču dažās dalībvalstīs īstenošana vēl nebija pabeigta. Turklāt ziņojumā teikts, ka "nesenie visā Eiropā notikušie uzbrukumi kopš Pamatlēmuma pieņemšanas ir parādījuši, ka ir radušies vairāki jauni draudi, jo īpaši plašu vienlaicīgu uzbrukumu informācijas sistēmām parādīšanās un tā saukto robottīklu (*botnets*) aizvien pieaugošā izmantošana noziedzīgiem mērķiem". Pamatlēmuma pieņemšanas laikā šiem uzbrukumiem nebija pievērsta galvenā uzmanība. Reaģējot uz šiem notikumiem, Komisija apsvērs rīcību, kuras mērķis būs atrast labāku risinājumu, kā reaģēt uz šiem draudiem (robottīkla skaidrojumu skatīt nākamajā sadaļā).

Turpmākas rīcības cīņai pret kibernoziedzību īpašā nozīme ir uzsvērta 2004. gada Hāgas programmā brīvības, drošības un tiesiskuma stiprināšanai Eiropas Savienībā, kā arī 2009. gada Stokholmas programmā un tās attiecīgajā rīcības plānā[3]. Turklāt nesen iesniegtajā Eiropas digitalizācijas programmā[4], kas ir pirmais "Eiropa 2020" stratēģijas ietvaros pieņemtais priekšlikums, ir atzīta nepieciešamība Eiropas līmenī vērsties pret jauna veida noziedzības izplatīšanās problēmu, jo īpaši pret kibernoziedzību. Komisija savā darbības laukā uzticības un drošības jomā ir apņēmusies veikt pasākumus, lai apkarotu kiberuzbrukumus informācijas sistēmām.

Starptautiskā līmenī par pašlaik vispilnīgāko starptautisko standartu tiek uzskatīta 2001. gada 23. novembrī parakstītā Eiropas Padomes Konvencija par kibernoziedzību (Kibernoziedzības konvencija), jo tā sniedz vispusīgu un saskaņotu regulējumu, kas aptver visdažādākos ar kibernoziedzību saistītos aspektus[5]. Līdz šim konvenciju ir parakstījušas visas 27 dalībvalstis, taču ratificējušas to ir tikai 15 dalībvalstis[6]. Konvencija stājās spēkā 2004. gada 1. jūlijā. ES nav parakstījusi konvenciju. Ņemot vērā šī akta nozīmi, Komisija aktīvi rosina arī pārējās ES dalībvalstis pēc iespējas ātrāk ratificēt šo konvenciju.

---

1 OV L 69, 16.3.2005., 68. lpp.

2 Komisijas ziņojums Padomei, pamatojoties uz 12. pantu Padomes 2005. gada 24. februāra pamatlēmumā par uzbrukumiem informācijas sistēmām, COM (2008) 448.

3 OV C 198, 12.8.2005., OV C 115, 4.5.2010., COM(2010) 171, 20.4.2010.

4 Komisijas 2010. gada 19. maija Paziņojums COM(2010) 245.

5 Eiropas Padomes konvencija par kibernoziedzību, Budapešta 23.11.2001., *CETS* Nr. 185.

6 Pārskatu par konvencijas (*CETS* Nr. 185) ratifikācijas gaitu skatīt: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

- **Vispārīgais konteksts**

Attiecībā uz kibernoziedzību galvenais šā fenomena cēlonis ir neaizsargātība, ko rada vairāki faktori. Tiesībaizsardzības mehānismu nepietiekamās reaģēšanas spējas veicina šā fenomena izplatīšanos un problēmu saasināšanos, jo atsevišķi nodarījumu veidi pārsniedz valstu robežas. Ziņošana par šāda veida nodarījumiem bieži vien ir nepilnīga, jo daži nodarījumi vispār paliek nepamanīti, un daļēji arī tāpēc, ka nodarījumu upuri (uzņēmumi un citi tautsaimniecības nozares pārstāvji) neziņo par tiem, jo baidās pasliktināt savu reputāciju un turpmākās uzņēmējdarbības izredzes, ja sabiedrībai kļūs zināma viņu neaizsargātība.

Turklāt dažādās valstu materiāltiesiskās un procedurālās krimināltiesību normas var radīt atšķirības tajā, kā tiek izmeklēti šie nodarījumi un kā personas tiek sauktas pie atbildības par tiem, tādējādi atšķiras arī pieeja šiem nodarījumiem. Informācijas tehnoloģiju attīstības rezultātā šīs problēmas ir kļuvušas vēl nopietnākas, jo ir vieglāk izgatavot un izplatīt nodarījumu izdarīšanas rīkus (destruktīvu programmatūru un robottīklus) un likumpārkāpēji var saglabāt anonimitāti, turklāt atbildība tiek sadalīta dažādām jurisdikcijām. Ņemot vērā grūtības saukt pie atbildības par šiem nodarījumiem, organizētā noziedzība var gūt ievērojamus ienākumus bez liela riska.

Šajā priekšlikumā ir ņemtas vērā kibernoziegumu izdarīšanas jaunākās metodes, jo īpaši robottīklu izmantošana. Ar terminu "robottīkls" apzīmē ar destruktīvu programmatūru (datorvīrusu) inficētu datoru kopumu. Šādam inficētu datoru (spoku) kopumam var likt veikt īpašas darbības, piemēram uzbrukt informācijas sistēmām (kiberuzbrukumi). Šos "spokus" var kontrolēt kāds cits dators, bieži vien bez inficēto datoru lietotāju ziņas. Šo "kontrolējošo" datoru sauc arī par "vadības un kontroles centru". Personas, kas kontrolē šo centru, ir vieni no likumpārkāpējiem, jo viņi izmanto inficētos datorus, lai sāktu uzbrukumus informācijas sistēmām. Ir ļoti grūti izsekot nodarījuma izdarītājus, jo datori, kas veido robottīklu un veic uzbrukumu, un nodarījuma izdarītājs var atrasties dažādās vietās.

Robottīklu veiktie uzbrukumi bieži vien ir plaša mēroga uzbrukumi. Plaša mēroga uzbrukumi ir vai nu tādi, ko var veikt izmantojot rīkus, kas ietekmē ievērojamu skaitu informācijas sistēmu (datoru), vai kas rada ievērojamu kaitējumu, proti, sistēmas pakalpojumu pārtraukumu, finansiālas izmaksas, personas datu zudumu utt. Šajā saistībā "liels robottīkls" it tāds, kas spēj radīt nopietnu kaitējumu. Ir grūti definēt robottīklu lielumu, taču tiek lēsts, ka lielākie līdz šim pieredzētie robottīkli aptver 40 000 līdz 100 000 savienojumu (tas ir, inficētu datoru) 24 stundu laikposmā[7].

[7] Savienojumu skaits 24 stundu laikposmā ir parasti izmantota robottīklu lieluma mērvienība.

- **Spēkā esošie noteikumi šā priekšlikuma jomā**

ES līmenī ar pamatlēmumu tiek ieviests minimālais dalībvalstu tiesību aktu tuvināšanas līmenis, lai noteiktu par krimināli sodāmiem vairākus kibernoziegumus, tostarp nelikumīgu piekļuvi informācijas sistēmai, nelikumīgu iejaukšanos sistēmā, nelikumīgu iejaukšanos datos, šo nodarījumu kūdīšanu, sekmēšanu un atbalstīšanu, kā arī nodarījuma izdarīšanas mēģinājumu.

Kaut arī dalībvalstis ir īstenojušas pamatlēmuma noteikumus, tajā ir vairākas nepilnības, ņemot vērā šo nodarījumu (kiberuzbrukumu) plašumu un skaita pieaugumu. Pamatlēmums tuvina tiesību aktus tikai attiecībā uz dažiem nodarījumiem, bet nerisina pilnībā jautājumu par liela mēroga uzbrukumu iespējamiem draudiem sabiedrībai. Turklāt nav pievērsta pietiekama uzmanība šo nodarījumu smagumam un sankcijām.

Citi spēkā esošie vai plānotie ES priekšlikumi un programmas jau zināmā mērā risina problēmas saistībā ar kiberuzbrukumiem vai tādiem jautājumiem kā tīklu drošums un interneta lietotāju drošība. Šeit jāmin pasākumi, ko atbalsta "Noziedzības profilakses un apkarošanas"[8] programmas, "Krimināltiesību"[9] programmas, "Drošāka interneta"[10] programmas un "Īpaši svarīgas informācijas infrastruktūras iniciatīvas"[11] ietvaros. Turklāt papildus minētajam pamatlēmumam vēl viens ar šo jomu saistīts spēkā esošs tiesību akts ir Pamatlēmums 2004/68/TI par bērnu seksuālās izmantošanas un bērnu pornogrāfijas apkarošanu.

Administratīvā līmenī datoru inficēšana, pārvēršot tos "robottīklos", jau ir aizliegta saskaņā ar ES privātuma un datu aizsardzības noteikumiem[12]. Jānorāda, ka valstu administratīvie dienesti jau sadarbojas Eiropas Surogātpasta apkarošanas iestāžu saziņas tīkla ietvaros. Saskaņā ar šiem noteikumiem dalībvalstu pienākums ir nodrošināt, ka ziņojumu pārtveršana bez attiecīgo lietotāju piekrišanas vai likumīgas atļaujas publiskos sakaru tīklos un publiski pieejamos elektronisko sakaru pakalpojumos ir aizliegta.

Šis priekšlikums pilnībā atbilst minētajiem noteikumiem. Dalībvalstīm būtu jāpievērš uzmanība administratīvo un tiesībaizsardzības iestāžu sadarbības uzlabošanai lietās, kurās iespējamas gan administratīvas, gan krimināla sankcijas.

- **Atbilstība pārējiem ES politikas virzieniem un mērķiem**

Mērķi atbilst ES politikai organizētās noziedzības apkarošanas, datortīklu pretestības spēju palielināšanas, īpaši svarīgas informācijas infrastruktūras aizsardzības un datu aizsardzības jomās. Šie mērķi atbilst arī programmai „Drošāks internets”, ko izstrādāja, lai veicinātu interneta un jaunu tiešsaistes tehnoloģiju drošāku izmantošanu un cīnītos pret nelikumīgu saturu.

---

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

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

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

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

12 Direktīva par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (OV L 201, 31.7.2002.) ar grozījumiem, kas izdarīti ar Direktīvu 2009/136/EK (OV L 337, 18.12.2009.).

Šis priekšlikums ir īpaši rūpīgi izpētīts, lai nodrošinātu, ka tā noteikumi ir pilnīgā saskaņā ar pamattiesībām un jo īpaši ar datu aizsardzību, vārda un informācijas brīvību, tiesībām uz taisnīgu tiesu, nevainīguma prezumpciju un tiesībām uz aizstāvību, kā arī ar tiesiskuma principu un nodarījuma un soda samērīguma principu krimināltiesībās.

2. APSPRIEŠANĀS AR IEINTERESĒTAJĀM PERSONĀM UN IETEKMES NOVĒRTĒJUMS

- **Apspriešanās ar ieinteresētajām personām**

Ir notikusi apspriešanās ar plašu attiecīgās jomas ekspertu loku sanāksmēs, kas veltītas vairākiem dažādiem kibernoziedzības apkarošanas aspektiem, tostarp arī šo nodarījumu tiesiskajam novērtējumam (saukšanai pie krimināllatbildības). To vidū jo īpaši jāmin dalībvalstu valdību un privātā sektora pārstāvji, šajā jomā specializējušies tiesneši un prokurori, starptautiskas organizācijas, Eiropas aģentūras un ekspertu struktūras. Vairāki eksperti un organizācijas pēc tam ir nosūtījuši apsvērumus un snieguši informāciju.

Galvenie apspriešanās rezultāti ir šādi:

– nepieciešama ES rīcība šajā jomā;

– nepieciešams par krimināls odāmiem atzīt nodarījumu veidus, kas nav iekļauti pašreizējā pamatlēmumā, jo īpaši jaunus kiberuzbrukumu veidus (robottīklus);

– nepieciešams novērst šķēršļus izmeklēšanai un saukšanai pie krimināllatbildības pārrobežu lietās.

Ietekmes novērtējumā ir ņemta vērā apspriešanās laikā sniegtā informācija.

Ekspertu atzinumu pieprasīšana un izmantošana

Dažādo sanāksmju ar ieinteresētajām personām laikā ir gūti neatkarīgu ekspertu atzinumi.

Ietekmes novērtējums

Tika izskatīti dažādi politikas risinājumi, lai sasniegtu izvirzīto mērķi.

- 1. politikas risinājums. Iepriekšējā stāvokļa saglabāšana /ES līmenī netiek veikti jauni pasākumi

Šis risinājums nozīmē, ka ES neveiks nekādus turpmākus pasākumus, lai apkarotu šo īpašo kibernoziedzības veidu, tas ir, uzbrukumus informācijas sistēmām. Pašreizējie pasākumi turpināsies, jo īpaši programmas, ar kurām veicina īpaši svarīgas informācijas infrastruktūras aizsardzību un publiskā un privātā sektora sadarbību cīņai pret kibernoziedzību.

- 2. politikas risinājums. Programmas izstrāde, lai stiprinātu centienus atvairīt uzbrukumus informācijas sistēmām ar neleģislatīvu pasākumu palīdzību

Neleģislatīvo pasākumu ietvaros papildus īpaši svarīgas informācijas infrastruktūras aizsardzības programmai galvenā uzmanība būtu pievērsta pārrobežu tiesībaizsardzības pasākumiem un publiskā un privātā sektora sadarbībai. Šo ieteikuma tiesību mērķis būtu veicināt turpmāku saskaņotu rīcību ES līmenī, tostarp tiesībaizsardzības iestāžu

kontaktpunktu 24/7 tīkla stiprināšanu. publiskā un privātā sektora kontaktpunktu ES tīkla izveide, iesaistot ekspertus kibernoziedzības jomā un tiesībaizsardzības iestādes; standarta ES nolīguma par pakalpojumu kvalitāti izstrāde tiesībaizsardzības iestāžu sadarbībai ar privātā sektora pārstāvjiem; un atbalsts kibernoziegumu izmeklēšanā iesaistīto tiesībaizsardzības iestāžu mācību programmām.

- 3. politikas risinājums. Mērķtiecīga pamatlēmuma noteikumu atjaunināšana (aizstājot pamatlēmumu ar jauno direktīvu), lai vērstos pret plaša mēroga uzbrukumiem informācijas sistēmām (robottīkliem) un risinātu dalībvalstu tiesībaizsardzības iestāžu kontaktpunktu efektivitātes jautājumus gadījumos, kad uzbrukumi tiek veikti, slēpjot izdarītāja patieso identitāti un kaitējot identitātes likumīgajam īpašniekam, kā arī lai risinātu jautājumu par kiberuzbrukumu statistikas datu trūkumu.

Šis risinājums paredz īpašu, mērķtiecīgu (tas ir, ļoti konkrētu) tiesību aktu ieviešanu plaša mēroga uzbrukumu informācijas sistēmām novēršanai. Šos īpašos tiesību aktus papildinātu neleģislatīvi pasākumi pret šiem uzbrukumiem vērstās operatīvās pārrobežu sadarbības veicināšanai, kas atvieglotu tiesību aktos paredzēto pasākumu īstenošanu. Šo pasākumu mērķis būtu uzlabot īpaši svarīgas informācijas infrastruktūras sagatavotību, drošību un pretestības spējas un apmainīties ar paraugprakses piemēriem.

- 4. politikas risinājums. Vispusīga kibernoziedzības apkarošanas ES tiesiskā regulējuma ieviešana

Šis risinājums nozīmētu jaunu visaptverošu ES tiesisko regulējumu. Papildus 2. politikas risinājumā minētajiem ieteikuma tiesību pasākumiem un 3. politikas risinājumā minētajai atjaunināšanai šis risinājums pievērstos arī citām ar interneta lietošanu saistītām tiesiskām problēmām. Šādi pasākumi attiektos ne tikai uz uzbrukumiem informācijas sistēmām, bet arī uz tādiem jautājumiem kā finanšu kibernoziedzība, nelikumīgs interneta saturs, elektronisko pierādījumu vākšana/glabāšana/pārsūtīšana un sīki izstrādāti noteikumi par jurisdikciju. Tiesiskais regulējums darbotos paralēli ar Eiropas Padomes konvenciju par kibernoziedzību un tajā būtu ietverti iepriekšminētie neleģislatīvie pasākumi.

- 5. politikas risinājums. Eiropas Padomes konvencijas par kibernoziedzību atjaunināšana

Šā risinājuma ietvaros būtu nepieciešams no jauna risināt sarunas par konvencijas saturu, kas ir ilgstošs process un neatbilst rīcības laikposmam, kas ierosināts ietekmes novērtējumā. Starptautiskā līmenī, šķiet, trūkst vēlmes no jauna risināt sarunas par konvenciju. Konvencijas atjaunināšana tādējādi nav uzskatāma par reālu risinājumu, jo tas nav īstenojams rīcībai atvēlētajā laikposmā.

Vēlamais politiskais risinājums. Neleģislatīvo pasākumu (2. risinājums) un mērķtiecīgas pamatlēmuma atjaunināšanas (3. risinājums) apvienojums.

Saskaņā ar analīzi par ekonomisko un sociālo ietekmi un ietekmi uz pamattiesībām 2. un 3. risinājums ir vispiemērotākā pieeja, lai risinātu šo problēmu un sasniegtu priekšlikuma mērķus.

Lai sagatavotu šo priekšlikumu, Komisija veica tā ietekmes novērtējumu.

3. PRIEKŠLIKUMA JURIDISKIE ASPEKTI

- **Ierosināto pasākumu kopsavilkums**

Ar direktīvu atceļ pamatlēmumu 2005/222/TI, pārņemot tā noteikumus un pievienojot šādus jaunus elementus.

– Vispārīgo materiālo krimināltiesību jomā ar direktīvu:

A. nosaka par sodāmu nodarījumu izdarīšanai izmantojamo ierīču/rīku ražošanu, pārdošanu, iepirkšanu izmantošanai, importu, izplatīšanu vai citāda veida pieejamības nodrošināšanu;

B. ievieš atbildību pastiprinošus apstākļus:

- plaša mēroga uzbrukums – ieviešot jaunu atbildību pastiprinošu apstākli, tiktu aptverti robottīkli vai tamlīdzīgi rīki tādā nozīmē, ka robottīkla vai tamlīdzīga rīka izveide būtu atbilstību pastiprinošs apstāklis, ja tiek izdarīti pamatlēmumā uzskaitītie nodarījumi,

- uzbrukums izdarīts, slēpjot izdarītāja patieso identitāti un kaitējot identitātes likumīgajam īpašniekam. Visiem šiem noteikumiem ir jāatbilst tiesiskuma un nodarījuma un soda samērīguma principam krimināltiesībās, tāpat tiem jābūt saskaņā ar spēkā esošajiem tiesību aktiem par personas datu aizsardzību[13];

C. ievieš "nelikumīgas pārtveršanas" noziedzīga nodarījuma sastāvu;

D. ievieš pasākumus, lai uzlabotu sadarbību Eiropā krimināltiesību jomā, stiprinot 24/7 kontaktpunktu struktūru[14]:

- ir ierosināts pienākums konkrētā termiņā izpildīt operatīvo kontaktpunktu palīdzības lūgumus (noteikts direktīvas 14. pantā). Kibernoziedzības konvencijā šāda veida saistoša noteikuma nav. Šī pasākuma mērķis ir nodrošināt, ka kontaktpunkti konkrētā termiņā norāda, vai tie spēj rast risinājumu palīdzības lūgumam un kad lūgumu izteikušais kontakpunkts var sagaidīt, ka risinājums tiks atrasts. Risinājuma saturs netiek noteikts;

E. risina jautājumu par kibernoziedzības statistikas datu sniegšanu, paredzot dalībvalstīm pienākumu nodrošināt piemērotas sistēmas izveidi, ar kuras palīdzību fiksē, ģenerē un sniedz statistikas datus par pamatlēmumā minētajiem nodarījumiem.

Direktīvā noziedzīgu nodarījumu definīcijās, kas uzskaitītas 3., 4., 5. pantā (nelikumīga piekļuve informācijas sistēmai, nelikumīga iejaukšanās sistēmā, nelikumīga iejaukšanās datos) ir iekļauts noteikums, kas, transponējot direktīvu valsts tiesību aktos, ļauj paredzēt, ka krimināllatbildība iestājas tikai "gadījumos, kas nav mazsvarīgi". Šāda veida rīcības brīvība ir

---

[13] Piemēram, Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīva 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (Privātuma un elektronisko komunikāciju direktīva) (OV L 201., 31.7.2002., 37. lpp.) (pašlaik tiek pārskatīta) un vispārīgā datu aizsardzības Direktīva 95/46/EK.

[14] Ieviesta pamatojoties uz Konvenciju un Pamatlēmumu 2005/222/TI par uzbrukumiem informācijas sistēmām.

paredzēta, lai dalībvalstis no kriminālatbildības piemērošanas jomas varētu izslēgt nodarījumus, kas teorētiski atbilst definīcijā paredzētajām noziedzīga nodarījuma sastāva pazīmēm, bet kurus uzskata par tādiem, kas nenodara kaitējumu ar likumu aizsargātajām interesēm, jo īpaši tas attiecas uz jauniešu darbībām, cenšoties pierādīt savas prasmes informācijas tehnoloģiju jomā. Taču šai iespējai ierobežot kriminālatbildības piemērošanas jomu nebūtu jānoved pie tā, ka papildus direktīvā jau paredzētajam tiek ieviesti noziedzīga nodarījuma sastāva papildu elementi, jo tādējādi varētu izveidoties situācija, ka kriminālatbildība tiek piemērota tikai tādiem nodarījumiem, kas izdarīti atbildību pastiprinošos apstākļos. Transponējot direktīvu, dalībvalstīm būtu jo īpaši jāatturas no papildu kvalificējošo pazīmju pievienošanas pamatnodarījumiem, pievienojot, piemēram, nolūku gūt nelikumīgu peļņu no noziedzīga nodarījuma vai tādas īpašas sekas kā ievērojamu zaudējumu izraisīšana.

- **Juridiskais pamats**

Līguma par Eiropas Savienības darbību 83. panta 1. punkts[15].

- **Subsidiaritātes princips**

Eiropas Savienības pasākumiem piemērojams subsidiaritātes princips. Dalībvalstis nevar pilnībā sasniegt priekšlikuma mērķus turpmāk minēto iemeslu dēļ.

Kibernoziedzību un, jo īpaši uzbrukumus informācijas sistēmām, raksturo ievērojama pārrobežu dimensija, kas īpaši raksturīga plaša mēroga uzbrukumiem, jo uzbrukumā iesaistītie elementi bieži vien atrodas dažādās vietās un dažādās valstīs. Tāpēc ir nepieciešama ES līmeņa rīcība, jo īpaši, lai spētu turēties līdzi aizvien pieaugošajam plaša mēroga uzbrukumu skaitam Eiropā un pasaulē. Padomes secinājumos 2008. gada novembrī[16] ir izteikts aicinājums rīkoties ES līmenī un atjaunināt Pamatlēmumu 2005/222/TI, jo dalībvalstis vienas pašas nespēj pietiekami efektīvi aizsargāt pilsoņus pret kibernoziedzību.

Priekšlikuma mērķus var labāk sasniegt ar Eiropas Savienības mēroga rīcību šādu iemeslu dēļ.

Ar šo priekšlikumu tiek vēl vairāk saskaņotas dalībvalstu materiālās krimināltiesības un kriminālprocesa noteikumi, kas pozitīvi ietekmēs cīņu pret šiem noziegumiem. Pirmkārt, tas ir veids, kā novērst noziedznieku pārvietošanos uz tām dalībvalstīm, kurās kiberuzbrukumu tiesiskais regulējums ir iecietīgāks. Otrkārt, kopīgas definīcijas padara iespējamu informācijas apmaiņu un attiecīgo datu vākšanu un salīdzināšanu. Treškārt, paaugstinās preventīvo pasākumu efektivitāte visā ES un starptautiskā sadarbība.

Tāpēc priekšlikums atbilst subsidiaritātes principam.

- **Proporcionalitātes princips**

Priekšlikums ir saskaņā ar proporcionalitātes principu šāda iemesla dēļ.

---

15 OV C 83, 30.3.2010., 49. lpp.

16 "Par saskaņotu darba stratēģiju un konkrētiem pasākumiem cīņā pret kibernoziedzību", TIESLIETU un IEKŠLIETU Padomes 2987. tikšanās Briselē 2008. gada 27.–28. novembrī.

Šī direktīva nepārsniedz minimumu, kas nepieciešams minēto mērķu sasniegšanai Eiropas līmenī, un to, kas ir vajadzīgs šim nolūkam, ņemot vērā nepieciešamību nodrošināt tiesību aktu precizitāti krimināltiesību jomā.

- **Juridisko instrumentu izvēle**

Ierosinātais instruments: direktīva.

Citi instrumenti nebūtu piemēroti šāda iemesla dēļ.

Juridiskajā pamatā ir paredzēta direktīva.

Neleģislatīvie pasākumi un pašregulācija varētu uzlabot situāciju atsevišķās jomās, kur īstenošanai ir izšķiroša nozīme. Tomēr citās jomās, kurās nepieciešami jauni tiesību akti, ieguvumi būtu nenozīmīgi.

4. IETEKME UZ BUDŽETU

Priekšlikuma ietekme uz Savienības budžetu ir neliela. Vairāk nekā 90 % no paredzamajām EUR 5 913 000 izmaksām segtu dalībvalstis, un tās var izmantot ES līdzekļus izmaksu samazināšanai.

5. PAPILDU INFORMĀCIJA

- **Spēkā esošo tiesību aktu atcelšana**

Pieņemot priekšlikumu, tiks atcelti spēkā esoši tiesību akti.

- **Teritoriālā darbības joma**

Saskaņā ar Līgumiem šī direktīva ir adresēta dalībvalstīm.

2010/0273 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES DIREKTĪVA

par uzbrukumiem informācijas sistēmām, un ar ko atceļ 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[17],

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu,

ņemot vērā Reģionu komitejas atzinumu,

rīkojoties saskaņā ar parasto likumdošanas procedūru,

tā kā:

(1) Šīs direktīvas uzdevums ir tuvināt dalībvalstu krimināltiesību noteikumus par uzbrukumiem informācijas sistēmām un uzlabot tiesu un citu kompetento iestāžu, tostarp policijas un citu specializētu tiesībaizsardzības dienestu sadarbību.

(2) Uzbrukumi informācijas sistēmām, jo īpaši organizētas noziedzības aktivitāšu rezultātā, kļūst arvien draudīgāki, un pieaug bažas par iespējamiem teroristiskiem vai politiski motivētiem uzbrukumiem informācijas sistēmām, kas ir dalībvalstu un Savienības īpaši svarīgās infrastruktūras sastāvdaļa. Tas apdraud drošākas informācijas sabiedrības un brīvības, drošības un tiesiskuma telpas izveidi, un tādējādi ir nepieciešama rīcība Eiropas Savienības līmenī.

(3) Ir vērojama tendence, ka plaša mēroga uzbrukumi informācijas sistēmām, kas ir īpaši svarīgas valstīm vai īpašām publiskā vai privātā sektora funkcijām, kļūst aizvien bīstamāki un atkārtojas aizvien biežāk. Šī tendenci pavada aizvien modernāku rīku attīstība, ko noziedznieki var izmantot dažādu kiberuzbrukumu izdarīšanai.

(4) Definīciju, jo īpaši informācijas sistēmu un datorizētu datu definīciju, vienotība šajā jomā ir svarīga, lai nodrošinātu saskaņotu pieeju šīs direktīvas piemērošanai dalībvalstīs.

(5) Jāpanāk kopīga pieeja noziedzīgu nodarījumu pazīmēm, ieviešot vienotus noziedzīgu nodarījumu sastāvus attiecībā uz nelikumīgu piekļuvi informācijas sistēmai,

[17] OV C […], […], […] lpp.

nelikumīgu iejaukšanos sistēmā, nelikumīgu iejaukšanos datos un nelikumīgu pārtveršanu.

(6) Dalībvalstīm jāparedz sodi par uzbrukumiem informācijas sistēmām. Šiem sodiem jābūt iedarbīgiem, samērīgiem un tādiem, kas attur no nodarījuma izdarīšanas.

(7) Ir atbilstīgi noteikt bargākas sankcijas, ja uzbrukumu informācijas sistēmai ir veikusi noziedzīga organizācija 2008. gada 24. oktobra Padomes Pamatlēmumā 2008/841/TI par cīņu pret organizēto noziedzību[18] sniegtās definīcijas nozīmē, kā arī ja tas ir plaša mēroga uzbrukums vai nodarījums ir veikts, slēpjot izdarītāju patieso identitāti un kaitējot identitātes likumīgajam īpašniekam. Tāpat ir lietderīgi nodrošināt iespēju piemērot bargākus sodus, ja šāds uzbrukums ir radījis nopietnus zaudējumus vai skāris būtiskas intereses.

(8) Padomes 2008. gada 27.-28. novembra secinājumos ir norādīts, ka dalībvalstīm un Komisijai būtu jāizstrādā jauna stratēģija, ņemot vērā 2001. gada Eiropas Padomes konvenciju par kibernoziedzību. Šī konvencija ir atsauces tiesiskais regulējums kibernoziedzības, tostarp uzbrukumu informācijas sistēmām, apkarošanai. Šī direktīva ir izstrādāta, pamatojoties uz minēto konvenciju.

(9) Ņemot vērā, ka uzbrukumu iespējams veikt dažādos veidos, un to, cik ātri attīstās aparatūra un programmatūra, Direktīvā izmantots termins "rīki, ko var izmantot direktīvā uzskaitīto noziedzīgo nodarījumu izdarīšanai". Rīki nozīmē, piemēram, destruktīvu programmatūru, tostarp arī robottīklus, ko izmanto kiberuzbrukumu izdarīšanai.

(10) Direktīva nav domāta, lai paredzētu krimināLatbildību gadījumos, kad nodarījumi ir izdarīti bez krimināla nolūka, piemēram, atļauta testēšana vai informācijas sistēmas aizsardzība.

(11) Direktīvā uzsvērta tādu informācijas apmaiņas tīklu nozīme kā G8 vai Eiropas Padomes kontaktpunktu tīkls, kas ir pieejami divdesmit četras stundas diennaktī un septiņas dienas nedēļā, lai nodrošinātu tūlītēju palīdzību ar informācijas sistēmām saistītu noziedzīgu nodarījumu izmeklēšanai vai tiesvedībai, vai noziedzīga nodarījuma pierādījumu vākšanai elektroniska formā. Ņemot vērā, cik ātri iespējams veikt plaša mēroga uzbrukumus, dalībvalstīm būtu jāspēj nekavējoties sniegt atbildi uz šī kontaktpunktu tīkla steidzamiem lūgumiem. Šādam atbalstam būtu jāietver šādu pasākumu atvieglošanu vai tiešu veikšanu: tehnisku konsultāciju sniegšana, datu saglabāšana, pierādījumu vākšana, juridiskas informācijas sniegšana un aizdomās turēto atrašanās vietas noteikšana.

(12) Ir nepieciešams vākt datus par nodarījumiem, kas minēti šajā direktīvā, lai iegūtu pilnīgāku pārskatu par šo problēmu Savienības līmenī, un tādējādi veicinātu efektīvāku atbildes mehānismu izstrādi. Šie dati turklāt palīdzēs īpašajām aģentūrām, kā Eiropols un Eiropas Tīklu un informācijas drošības aģentūra, labāk novērtēt kibernoziedzības izplatības apjomu un stāvokli tīklu un informācijas drošības jomā Eiropā.

---

[18] OV L 300, 11.11.2008., 42. lpp.

(13) Ievērojami trūkumi un atšķirības dalībvalstu tiesību aktos uzbrukumu informācijas sistēmām jomā var kavēt organizētās noziedzības un terorisma apkarošanu un sarežģīt efektīvu policijas un tiesu iestāžu sadarbību. Modernās informācijas sistēmas ir starptautiskas un tās nesaista robežas, tas nozīmē, ka uzbrukumiem šādām sistēmām ir pārrobežu raksturs, kas vēl vairāk izceļ steidzamo vajadzību tuvināt krimināltiesību aktus šajā jomā. Turklāt, pēc Padomes Pamatlēmuma 2009/948/TI par jurisdikcijas īstenošanas konfliktu novēršanu un atrisināšanu kriminālprocesā pieņemšanas, būtu jāuzlabojas koordinēšanai, saucot pie atbildības saistībā ar uzbrukumiem informācijas sistēmām.

(14) Dalībvalstis nespēj pilnībā sasniegt šīs direktīvas mērķi, proti, nodrošināt, ka uzbrukumi informācijas sistēmām visās dalībvalstīs ir sodāmi, piemērojot efektīvus, samērīgus un atturošus kriminālsodus, un uzlabot un veicināt tiesu iestāžu sadarbību, likvidējot iespējamos sarežģījumus, jo noteikumiem jābūt vienotiem un saderīgiem, tādējādi mērķi labāk var sasniegt Savienības līmenī un Savienība var pieņemt pasākumus saskaņā ar subsidiaritātes principu, kā noteikts Eiropas Savienības līguma 5. pantā. Šī direktīva nepārsniedz to, kas ir vajadzīgs šo mērķu sasniegšanai.

(15) Personas dati, ko apstrādā saistībā ar šīs direktīvas īstenošanu, būtu jāaizsargā saskaņā ar datu aizsardzības noteikumiem, kas paredzēti Padomes 2008. gada 27. novembra Pamatlēmumā 2008/977/TI par tādu personas datu aizsardzību, ko apstrādā, policijas un tiesu iestādēm sadarbojoties krimināllietās[19] attiecībā uz tām apstrādes darbībām, kas ietilpst šī pamatlēmuma piemērošanas jomā, un Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regulā (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti[20].

(16) Direktīvā ir ievērotas pamattiesības un Eiropas Savienības Pamattiesību hartā atzītie principi, tostarp personas datu aizsardzība, vārda un informācijas brīvība, tiesības uz taisnīgu tiesu, nevainīguma prezumpcija un tiesības uz aizstāvību, kā arī tiesiskuma princips un nodarījuma un soda samērīguma princips krimināltiesībās. Šo tiesību un principu pilnīga ievērošana ir īpašs šīs direktīvas mērķis un tā ir attiecīgi jāīsteno.

(17) [Saskaņā ar 1., 2., 3. un 4. pantu Protokolā par Apvienotās Karalistes un Īrijas nostāju saistībā ar brīvības, drošības un tiesiskuma telpu, kas pievienots Līgumam par Eiropas Savienības darbību, Apvienotā Karaliste un Īrija ir informējušas par savu vēlmi piedalīties šīs direktīvas pieņemšanā un piemērošanā.] VAI [Neskarot minētā protokola 4. pantu par Apvienotās Karalistes un Īrijas nostāju saistībā ar brīvības, drošības un tiesiskuma telpu, Apvienotā Karaliste un Īrija nepiedalīsies šīs direktīvas pieņemšanā, un tādēļ šī direktīva nebūs tām saistoša un nebūs jāpiemēro].

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

---

19 OV L 350, 30.12.2008., 60. lpp.
20 OV L 8, 12.1.2001., 1. lpp.

IR PIEŅĒMUŠI ŠO DIREKTĪVU.

1. pants
Priekšmets

Ar šo direktīvu definē noziedzīgus nodarījumus uzbrukumu informācijas sistēmām jomā un izveido minimuma noteikumus attiecībā uz sodiem par šiem nodarījumiem. Tās mērķis ir arī ieviest vienotus noteikumus šādu uzbrukumu novēršanai un uzlabot sadarbību šajā jautājumā krimināltiesību jomā Eiropā.

2. pants
Definīcijas

Šajā direktīvā piemēro šādas definīcijas:

a) "informācijas sistēma" ir jebkura ierīce vai savstarpēji savienotu vai saistītu ierīču kopums, no kurām viena vai vairākas ierīces saskaņā ar programmu veic automātisku datorizētu datu apstrādi, kā arī datorizēti dati, ko minētās ierīces glabā, apstrādā, iegūst vai sūta to darbībai, izmantošanai, aizsardzībai un uzturēšanai;

b) "datorizēti dati" ir jebkurš faktu, informācijas vai konceptu atveidojums formā, kas piemērota apstrādei informācijas sistēmā, tostarp programma, kas piemērota tam, lai informācijas sistēmā izraisītu kādu darbību;

c) "juridiska persona" ir jebkurš subjekts, kam ir šāds statuss attiecīgos tiesību aktos, izņemot valstis vai citas valsts struktūras, kas īsteno valsts varu, un starptautiskas sabiedriskās organizācijas;

d) "bez tiesībām" ir piekļuve vai iejaukšanās bez īpašnieka vai bez sistēmas vai tās daļas cita tiesību subjekta atļaujas, vai tāda piekļuve vai iejaukšanās, kas nav atļauta saskaņā ar attiecīgās valsts tiesību aktiem.

3. pants
Nelikumīga piekļuve informācijas sistēmām

Katra dalībvalsts veic vajadzīgos pasākumus, lai nodrošinātu, ka vismaz gadījumos, kas nav mazsvarīgi, tīša piekļuve bez atļaujas visai informācijas sistēmai vai jebkādai tās daļai ir sodāma kā noziedzīgs nodarījums.

4. pants
Nelikumīga iejaukšanās sistēmā

Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka vismaz gadījumos, kas nav mazsvarīgi, informācijas sistēmas darbības tīša, būtiska kavēšana vai pārtraukšana, ievadot, sūtot, bojājot, dzēšot, pasliktinot, grozot, anulējot vai padarot nepieejamus datorizētus datus, ir sodāma kā noziedzīgs nodarījums, ja to veic bez atļaujas.

5. pants

Nelikumīga iejaukšanās datos

Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka vismaz gadījumos, kas nav mazsvarīgi, informācijas sistēmas datorizētu datu tīša dzēšana, bojāšana, pasliktināšana, grozīšana, anulēšana vai padarīšana par nepieejamiem ir sodāma kā noziedzīgs nodarījums.

6. pants

Nelikumīga pārtveršana

Dalībvalstis pieņem nepieciešamos pasākumus, lai nodrošinātu, ka tīša datu pārtveršana bez atļaujas, ko veic ar tehnisku līdzekļu palīdzību no informācijas sistēmas vai informācijas sistēmas ietvaros veiktas datorizētu datu pārsūtīšanas laikā, ja tā nav publiska, ietverot informācijas sistēmas elektromagnētiskās emisijas, kas satur šādus datorizētus datus, ir sodāma kā noziedzīgs nodarījums.

7. pants

Noziedzīgu nodarījumu izdarīšanas rīki

Dalībvalstis veic nepieciešamos pasākumus, lai nodrošinātu, ka turpmāk minēto priekšmetu ražošana, pārdošana, iepirkšana izmantošanai, imports, izplatīšana vai citāda veida pieejamības nodrošināšana ir sodāma kā noziedzīgs nodarījums, ja to izdara tīši un bez atļaujas nolūkā izdarīt kādu no nodarījumiem, kas minēti 3.–6. pantā:

a) iekārta, tostarp datorprogramma, kura galvenokārt paredzēta vai pielāgota 3.–6. pantā minēto noziedzīgo nodarījumu izdarīšanai,

b) datorparole, pieejas kods vai līdzīgi dati, ar kuru palīdzību var piekļūt informācijas sistēmai vai tās daļai.

8. pants

Kūdīšana, sekmēšana, atbalstīšana un mēģinājums

1. Dalībvalstis nodrošina, ka 3.–7. pantā minēta nodarījuma kūdīšana, sekmēšana un atbalstīšana ir sodāma kā noziedzīgs nodarījums.

2. Dalībvalstis nodrošina, ka mēģinājums izdarīt 3.–6. pantā minētos nodarījumus, ir sodāms kā noziedzīgs nodarījums.

9. pants

Sodi

1. Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka par 3.– 8. pantā minētajiem noziedzīgajiem nodarījumiem ir paredzēti efektīvi, samērīgi un atturoši krimināsodi.

2. Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka par 3.–7. pantā minētajiem nodarījumiem maksimālais krimināsods ir brīvības atņemšana uz vismaz diviem gadiem.

10. pants

Atbildību pastiprinoši apstākļi

1. Dalībvalstis veic nepieciešamos pasākumus, lai nodrošinātu, ka par 3.–7. pantā minētajiem nodarījumiem paredzētais maksimālais kriminālsods ir brīvības atņemšana uz vismaz pieciem gadiem, ja tie izdarīti noziedzīgas organizācijas ietvaros saskaņā ar 2008. gada 24. oktobra Pamatlēmumā 2008/841/TI sniegto definīciju.

2. Dalībvalstis veic nepieciešamos pasākumus, lai nodrošinātu, ka par 3.–6. pantā minētajiem nodarījumiem paredzētais maksimālais kriminālsods ir brīvības atņemšana uz vismaz pieciem gadiem, ja tie izdarīti, izmantojot rīku, kas domāts tādu uzbrukumu sākšanai, kas ietekmē ievērojamu skaitu informācijas sistēmu, vai rada ievērojamu kaitējumu, piemēram, sistēmas pakalpojumu pārtraukumu, finansiālas izmaksas vai personas datu zudumu.

3. Dalībvalstis veic nepieciešamos pasākumus, lai nodrošinātu, ka par 3.–6. pantā minētajiem nodarījumiem maksimālais kriminālsods ir brīvības atņemšana uz vismaz pieciem gadiem, ja tie izdarīti, slēpjot izdarītāju patieso identitāti un kaitējot identitātes likumīgajam īpašniekam.

11. pants

Juridisko personu atbildība

1. Dalībvalstis veic nepieciešamos pasākumus, lai nodrošinātu, ka juridiskas personas var saukt pie atbildības par 3.–8. pantā minētajiem nodarījumiem, ko to labā, darbojoties individuāli vai kā juridiskas personas struktūras daļa, izdarījusi kāda persona, kas veic šās juridiskās personas vadības pienākumus, pamatojoties uz:

   a) tiesībām pārstāvēt juridisko personu;

   b) pilnvarām pieņemt lēmumus juridiskās personas vārdā;

   c) pilnvarām veikt juridiskās personas iekšējo kontroli.

2. Katra dalībvalsts veic nepieciešamos pasākumus, lai nodrošinātu, ka juridiskas personas var saukt pie atbildības, ja 1. punktā minētās personas veiktās uzraudzības vai kontroles trūkuma dēļ bijis iespējams, ka nodarījumu, kas minēts 3.–8. pantā, attiecīgās juridiskās personas labā izdara persona, kas ir tās pakļautībā.

3. Juridiskās personas atbildība saskaņā ar 1. un 2. punktu neizslēdz kriminālvajāšanu pret fiziskām personām, kas ir jebkuru 3.–8. pantā minēto nodarījumu izpildītāji, uzkūdītāji vai līdzdalībnieki.

12. pants

Sodi juridiskām personām

1. Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka juridiskai personai, kuru sauc pie atbildības saskaņā ar 11. panta 1. punktu, var piemērot efektīvus, samērīgus

un atturošus sodus, kas ietver naudas sodu kā krimināl sodu vai cita veida sodu un var ietvert citādus sodus, kas paredz, piemēram,

a) atņemt tiesības saņemt valsts pabalstus 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 11. panta 2. punktu, ir piemērojami efektīvi, samērīgi un atturoši sodi vai pasākumi.

13. pants
Jurisdikcija

1. Direktīvas 3.–8. pantā minētie nodarījumi ir dalībvalsts jurisdikcijā, ja:

a) nodarījums ir pilnīgi vai daļēji izdarīts attiecīgās dalībvalsts teritorijā; vai

b) nodarījuma izdarītājs ir attiecīgās dalībvalsts valstspiederīgais vai persona, kuras pastāvīgā dzīvesvieta ir tās teritorijā; vai

c) nodarījums ir izdarīts par labu juridiskai personai, kuras galvenais birojs ir attiecīgās dalībvalsts teritorijā.

2. Dalībvalstis, nosakot jurisdikciju saskaņā ar 1. punkta a) apakšpunktu, nodrošina, ka to jurisdikcijā ietilpst gadījumi, kad:

a) likumpārkāpējs izdara nodarījumu, fiziski atrodoties attiecīgās dalībvalsts teritorijā, neatkarīgi no tā, vai nodarījums ir izdarīts pret informācijas sistēmu tās teritorijā; vai

b) nodarījums ir izdarīts pret informācijas sistēmu attiecīgās dalībvalsts teritorijā, neatkarīgi no tā, vai likumpārkāpējs izdara nodarījumu, fiziski atrodoties tās teritorijā;

14. pants
Informācijas apmaiņa

1. Lai apmainītos ar informāciju par 3.–8. pantā minētajiem nodarījumiem, saskaņā ar datu aizsardzības noteikumiem dalībvalstis izmanto pastāvošo operatīvo kontaktpunktu tīklu, kas ir pieejams divdesmit četras stundas diennaktī un septiņas dienas nedēļā. Dalībvalstis nodrošina, ka ir ieviestas procedūras, lai tās varētu atbildēt uz steidzamiem lūgumiem maksimums astoņu stundu laikā. Šādā atbildē vismaz norāda, vai, kādā veidā un kad tiks sniegts palīdzības lūguma risinājums.

2. Dalībvalstis informē Komisiju par to nozīmētajiem kontaktpunktiem informācijas apmaiņai par nodarījumiem, kas minēti 3.–8. pantā. Komisija nosūta šo informāciju citām dalībvalstīm.

15. pants
Uzraudzība un statistika

1. Dalībvalstis nodrošina sistēmas izveidi, ar kuras palīdzību reģistrē, ģenerē un sniedz statistikas datus par nodarījumiem, kas minēti 3.–8. pantā.

2. Statistikas informācija, kas minēta 1. punktā, aptver vismaz šādus datus: dalībvalstīm paziņoto 3.–8. pantā minēto nodarījumu skaitu un rīcību, kas sekojusi, reaģējot uz šiem paziņojumiem, norāda arī izmeklēto lietu skaitu par katru gadu, personu skaitu, pret kurām uzsākts kriminālprocess, un personu skaitu, kas notiesātas par 3.–8. pantā minētajiem nodarījumiem.

3. Saskaņā ar šo pantu savāktos datus dalībvalstis nosūta Komisijai. Dalībvalstis nodrošina šo statistikas ziņojumu konsolidēta pārskata publicēšanu.

16. pants
Pamatlēmuma 2005/222/TI atcelšana

Ar šo atceļ Pamatlēmumu 2005/222/TI, neskarot dalībvalstu pienākumus attiecībā uz termiņiem transponēšanai valsts tiesību aktos.

Atsauces uz atsaukto pamatlēmumu uzskata par atsaucēm uz šo direktīvu.

17. pants
Transponēšana

1. Normatīvie un administratīvie akti, kas vajadzīgi, lai izpildītu šīs direktīvas prasības, dalībvalstīs stājas spēkā vēlākais līdz [divi gadi kopš pieņemšanas]. Tās tūlīt dara zināmus Komisijai minēto noteikumu tekstus, kā arī minēto noteikumu un šīs direktīvas atbilstības tabulu. Kad dalībvalstis pieņem minētos noteikumus, tajos ietver atsauci uz šo direktīvu vai šādu atsauci pievieno to oficiālai publikācijai. Dalībvalstis nosaka, kā izdarāma šāda atsauce.

2. Dalībvalstis dara zināmus Komisijai galvenos valsts tiesību aktu noteikumus, ko tās pieņem jomā, uz kuru attiecas šī direktīva.

18. pants
Ziņojumu sniegšana

1. [ČETRUS GADUS PĒC PIEŅEMŠANAS] un turpmāk ik pēc trīs gadiem Komisija iesniedz Eiropas Parlamentam un Padomei ziņojumu par šīs direktīvas piemērošanu dalībvalstīs, tostarp visus vajadzīgos priekšlikumus.

2. Dalībvalstis nosūta Komisijai visu informāciju, kas ir vajadzīga, lai sagatavotu 1. punktā minēto ziņojumu. Šajā informācijā ietver sīku aprakstu par leģislatīvajiem un citiem pasākumiem, kas pieņemti īstenojot šo direktīvu.

19. pants
Stāšanās spēkā

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

20. pants
Adresāti

Saskaņā ar Līgumiem šī direktīva ir adresēta dalībvalstīm.

Briselē,

Eiropas Parlamenta vārdā –	*Padomes vārdā –*
priekšsēdētājs	*priekšsēdētājs*