

(Tiesību akti, kas pieņemti saskaņā ar Līguma par Eiropas Savienību VI sadaļu)

PADOMES PAMATLĒMUMS 2005/222/TI

(2005. gada 24. februāris)

par uzbrukumiem informācijas sistēmām

EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienību, un jo īpaši tā 29. pantu, 30. panta 1. punkta a) apakšpunktu, 31. panta 1. punkta e) apakšpunktu un 34. panta 2. punkta b) apakšpunktu,

ņemot vērā Komisijas priekšlikumu,

ņemot vērā Eiropas Parlamenta atzinumu⁽¹⁾,

tā kā:

- (1) Šā pamatlēmuma mērķis ir uzlabot tiesu un citu kompetento iestāžu, tostarp policijas un citu specializētu tiesībsargāšanas dienestu sadarbību, tuvinot dalībvalstu krimināltiesību noteikumus, kas attiecas uz uzbrukumiem informācijas sistēmām.
- (2) Ir zināms, ka ir notikuši uzbrukumi informācijas sistēmām, jo īpaši pēc organizētas noziedzības draudiem, un pastāv arvien lielākas bažas par iespējamām teroristu uzbrukumiem informācijas sistēmām, kas ir daļa dalībvalstu kritiskās infrastruktūras. Tie apdraud drošākas informācijas sabiedrības un brīvības, drošības un tiesiskuma telpas izveidi un tādējādi prasa rīcību Eiropas Savienības līmenī.
- (3) Efektīva atbilde uz tādiem draudiem prasa visaptverošu pieeju tīklu un informācijas drošībai, kā uzsvērts e-Eiropas rīcības plānā, Komisijas paziņojumā "Tīklu un informācijas drošība: priekšlikums Eiropas politikas pieejai" un Padomes 2002. gada 28. janvāra Rezolūcijā par kopīgu pieeju un konkrētām darbībām tīklu un informācijas drošības jomā⁽²⁾.
- (4) Vajadzība vēl vairāk apzināties problēmas, kas saistītas ar informācijas drošību, kā arī sniegt praktisku palīdzību, ir uzsvērtā arī Eiropas Parlamenta 2001. gada 5. septembra Rezolūcijā.

(5) Ievērojami trūkumi un atšķirības dalībvalstu tiesību aktos šajā jomā var likt šķēršļus organizētās noziedzības un terorisma apkarošanai un var sarežģīt efektīvu policiju un tiesu sadarbību attiecībā uz uzbrukumiem informācijas sistēmām. Tas, ka modernās informācijas sistēmas ir starptautiskas un bez robežām, nozīmē, ka uzbrukumi šādām sistēmām bieži vien ir uzbrukumi pāri robežām, kas pastiprina steidzamo vajadzību tuvināt krimināltiesību aktus šajā jomā.

(6) Padomes un Komisijas rīcības plāns par to, kā vislabāk īstenot Amsterdamas Līguma noteikumus par brīvības, drošības un tiesiskuma telpu⁽³⁾, Eiropadomes sanāksme Tampērē 1999. gada 15.–16. oktobrī, Eiropadomes sanāksme Santa Maria da Feira 2000. gada 19.–20. jūnijā, Komisija "Progresā ziņojumā" un Eiropas Parlaments 2000. gada 19. maija Rezolūcijā norāda vai aicina uz tiesību aktu pieņemšanu augsto tehnoloģiju noziegumu apkarošanai, ietverot vienotas definīcijas, apsūdzību celšanas un sodus.

(7) Jāpapildina starptautisko organizāciju veiktais darbs, jo īpaši Eiropas Padomes darbs, tuvinot krimināltiesību aktus, kā arī G8 darbs attiecībā uz starptautisku sadarbību augsto tehnoloģiju noziedzības jomā, Eiropas Savienībā nodrošinot kopīgu pieeju šajā jomā. Šo aicinājumu precizēja Komisijas paziņojumā Padomei, Eiropas Parlamentam, Ekonomikas un sociālo lietu komitejai un Reģionu komitejai par "Drošākas informācijas sabiedrības izveidi, uzlabojot informācijas infrastruktūru drošību un apkarojot datornoziegumus".

(8) Būtu jātuvināta krimināltiesību akti par uzbrukumiem informācijas sistēmām, lai nodrošinātu visciešāko iespējamo policijas un tiesu sadarbību attiecībā uz noziedzīgiem nodarījumiem, kas saistīti ar uzbrukumiem informācijas sistēmām, un veicinātu organizētās noziedzības un terorisma apkarošanu.

⁽¹⁾ OV C 300 E, 11.12.2003., 26. lpp.

⁽²⁾ OV C 43, 16.2.2002., 2. lpp.

⁽³⁾ OV C 19, 23.1.1999., 1. lpp.

- (9) Visas dalībvalstis ir ratificējušas 1981. gada 28. janvārī pieņemto Eiropas Padomes Konvenciju personu aizsardzībai attiecībā uz personisko datu automātisko apstrādi. Personas dati, kas apstrādāti, īstenojot šo pamatlēmumu, būtu jāaizsargā saskaņā ar minētās konvencijas principiem.
- (10) Ir svarīgi, ka šajā jomā ir vienotas definīcijas, jo īpaši informācijas sistēmu un datorizētu datu definīcija, lai dalībvalstīs nodrošinātu konsekventu pieeju, piemērojot šo pamatlēmumu.
- (11) Jāpanāk kopīga pieeja noziedzīgu nodarījumu pazīmēm, par noziedzīgiem nodarījumiem kopīgi atzīstot nelikumīgu piekļuvi informācijas sistēmai, nelikumīgu iejaukšanos sistēmā un nelikumīgu iejaukšanos datos.
- (12) Lai apkarotu datornoziedzīgumus, katrai dalībvalstij būtu jānodrošina efektīva tiesu sadarbība attiecībā uz noziedzīgiem nodarījumiem, kā pamatā ir 2., 3., 4. un 5. pantā minētie uzvedības veidi.
- (13) Jāizvairās no tā, lai pārāk daudzus gadījumus, jo īpaši maznozīmīgus gadījumus, atzītu par kriminālnoziedzīgiem, kā arī jāizvairās no tā, lai tiesību subjektus un pilnvarotas personas atzītu par kriminālatbildīgām personām.
- (14) Dalībvalstīm jāparedz sodi par uzbrukumiem informācijas sistēmām. Šādi sodi ir efektīvi, samērīgi un preventīvi.
- (15) Ir lietderīgi paredzēt smagākus sodus, ja uzbrukumu informācijas sistēmai veic krimināla organizācija, kā noteikts Vienotajā rīcībā 98/733/TI (1998. gada 21. decembris) par dalības kriminālās organizācijās uzskatīšanu Eiropas Savienības dalībvalstīs par noziedzīgu nodarījumu⁽¹⁾. Tāpat ir lietderīgi nodrošināt iespēju piemērot smagākus sodus, ja šāds uzbrukums ir radījis nopietnus zaudējumus vai skāris būtiskas intereses.
- (16) Būtu arī jāparedz dalībvalstu savstarpējas sadarbības pasākumi, lai nodrošinātu efektīvu rīcību pret uzbrukumiem informācijas sistēmām. Tāpēc, lai apmainītos ar informāciju, dalībvalstīm būtu jāizmanto pastāvošais operatīvo kontaktpunktu tīkls, kurš minēts Padomes 2001. gada 25. jūnija Ieteikumā par kontaktpunktiem, ar ko uztur augsto tehnoloģiju noziedzības apkarošanas dienestu 24 stundas diennaktī⁽²⁾.
- (17) Dalībvalstis nespēj pilnībā sasniegt šā pamatlēmuma mērķi, proti, nodrošināt, ka pret uzbrukumiem informācijas sistēmām visās dalībvalstīs ievieš sankcijas, piemērojot efektīvus, samērīgus un preventīvus kriminālsodus un uzlabojot un veicinot tiesu sadarbību, likvidējot iespējamus sarežģījumus, jo noteikumiem jābūt kopīgiem un saderīgiem, un tos var vieglāk sasniegt Savienības līmenī, Savienība var pieņemt pasākumus saskaņā ar subsidiaritātes principu, kā izklāstīts EK dibināšanas līguma 5. pantā. Saskaņā ar proporcionalitātes principu, kas izklāstīts minētajā pantā, šajā pamatlēmumā nosaka tikai to, kas vajadzīgs, lai sasniegtu šo mērķi.
- (18) Šajā pamatlēmumā ir ievērotas pamattiesības un respektēti principi, kas atzīti Līguma par Eiropas Savienību 6. pantā un atspoguļoti Eiropas Savienības Pamattiesību hartā, jo īpaši tās II un VI nodaļā,

IR PIEŅĒMUSI ŠO PAMATLĒMUMU.

1. pants

Definīcijas

Šajā pamatlēmumā 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 fakts, 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;

⁽¹⁾ OV L 351, 29.12.1998., 1. lpp.

⁽²⁾ OV C 187, 3.7.2001., 5. lpp.

- 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.

2. pants

Nelikumīga piekļuve informācijas sistēmām

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

2. Jebkura dalībvalsts var pieņemt lēmumu, ka par 1. punktā minēto rīcību ceļ apsūdzību tikai tad, ja pārkāpums ir izdarīts, pārkāpjot drošības pasākumu.

3. pants

Nelikumīga iejaukšanās sistēmā

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

4. pants

Nelikumīga iejaukšanās datos

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

5. pants

Kūdišana, palīdzēšana un atbalstīšana un nodarījuma izdarīšanas mēģinājums

1. Katra dalībvalsts nodrošina, ka kūdišana, palīdzēšana un atbalstīšana, kas saistīta ar 2., 3. un 4. pantā minēto nodarījumu, ir sodāma kā noziedzīgs nodarījums.

2. Katra dalībvalsts nodrošina, ka mēģinājums izdarīt 2., 3. un 4. pantā minētos nodarījumus, ir sodāms kā noziedzīgs nodarījums.

3. Katra dalībvalsts var pieņemt lēmumu nepiemērot 2. punktu 2. pantā minētajiem nodarījumiem.

6. pants

Sodi

1. Katra dalībvalsts veic vajadzīgos pasākumus, lai nodrošinātu, ka 2., 3., 4. un 5. pantā minētie nodarījumi ir sodāmi, piemērojot efektīvus, samērīgus un preventīvus kriminālsodus.

2. Katra dalībvalsts veic vajadzīgos pasākumus, lai nodrošinātu, ka 3. un 4. pantā minētie nodarījumi ir sodāmi, piemērojot kriminālsodus, kas maksimāli ir vismaz 1 līdz 3 gadi ieslodzījuma.

7. pants

Atbildību pastiprinoši apstākļi

1. Katra dalībvalsts veic vajadzīgos pasākumus, lai nodrošinātu, ka 2. panta 2. punktā minētais nodarījums un 3. un 4. pantā minētais nodarījums ir sodāms, piemērojot kriminālsodus, kas maksimāli ir vismaz 2 līdz 5 gadi ieslodzījuma, ja nodarījums veikts saistībā ar kriminālu organizāciju, kā definēts Vienotajā rīcībā 98/733/TI, neatkarīgi no tur minētā sodu līmeņa.

2. Dalībvalsts var veikt arī 1. punktā minētos pasākumus, ja nodarījums ir radījis nopietnus zaudējumus vai skāris būtiskas intereses.

8. pants

Juridisku personu atbildība

1. Katra dalībvalsts veic vajadzīgos pasākumus, lai nodrošinātu, ka juridiskas personas var saukt pie atbildības par 2., 3., 4. un 5. pantā minētajiem nodarījumiem, ko to labā, darbojoties atsevišķi vai kā juridiskās personas struktūras daļa, veikusi jebkura persona, kam juridiskā personā ir vadošs stāvoklis, kā pamatā ir:

- a) pilnvaras pārstāvēt juridisko personu; vai
- b) pilnvaras pieņemt lēmumus juridiskās personas vārdā; vai
- c) pilnvaras veikt kontroli juridiskajā personā.

2. Neatkarīgi no 1. punktā paredzētajiem gadījumiem katra dalībvalsts veic vajadzīgos pasākumus, lai nodrošinātu, ka juridisko personu var saukt pie atbildības tad, ja 1. punktā minētās personas pārraudzības vai kontroles trūkums ir darījis iespējamu to, ka 2., 3., 4. un 5. pantā minēto nodarījumu veic šīs juridiskās personas labā tai pakļauta persona.

3. Juridiskas personas atbildība saskaņā ar 1. un 2. punktu neizslēdz kriminālvajāšanu pret fiziskām personām, kas 2., 3., 4. un 5. pantā minēto nodarījumu izdarīšanā ir iesaistītas kā izdarītāji, kūdītāji vai līdzdalībnieki.

9. pants

Juridiskām personām piemērojamie sodi

1. Katra dalībvalsts veic vajadzīgos pasākumus, lai nodrošinātu, ka juridiskā persona, kas ir saukta pie atbildības saskaņā ar 8. panta 1. punktu, ir sodāma, tai piemērojot efektīvus, samērīgus un preventīvus sodus, kuri ietver naudas sodu, kas ir vai nav kriminālsods, un var ietvert citus sodus, piemēram:

- a) valsts pabalstu vai atbalsta saņemšanas tiesību atņemšanu;
- b) īslaicīgu vai pastāvīgu aizliegumu veikt komercdarbību;
- c) pakļaušanu tiesas uzraudzībai vai
- d) likvidēšanu tiesas ceļā.

2. Katra dalībvalsts veic vajadzīgos pasākumus, lai nodrošinātu, ka juridiska persona, kas ir saukta pie atbildības saskaņā ar 8. panta 2. punktu, ir sodāma, tai piemērojot efektīvus, samērīgus un preventīvus sodus vai pasākumus.

10. pants

Jurisdikcija

1. Katra dalībvalsts ievieš tās jurisdikciju attiecībā uz 2., 3., 4. un 5. pantā minētajiem nodarījumiem, ja nodarījums ir izdarīts:

- a) pilnīgi vai daļēji tās teritorijā; vai
- b) to ir izdarījis tās valstspiederīgais; vai
- c) tas ir izdarīts par labu juridiskai personai, kuras galvenais birojs ir šīs dalībvalsts teritorijā.

2. Katra dalībvalsts, nosakot tās jurisdikciju saskaņā ar 1. punkta a) apakšpunktu, nodrošina, ka jurisdikcija ietver gadījumus, kad:

- a) likumpārkāpējs veic nodarījumu, kamēr viņš fiziski atrodas attiecīgās dalībvalsts teritorijā, neatkarīgi no tā, vai nodarījums ir veikts pret informācijas sistēmu attiecīgās dalībvalsts teritorijā vai ne; vai
 - b) nodarījumu veic pret informācijas sistēmu attiecīgās dalībvalsts teritorijā, neatkarīgi no tā, vai likumpārkāpējs veic nodarījumu, kamēr viņš fiziski ir attiecīgās dalībvalsts teritorijā vai ne.
3. Dalībvalsts, kas saskaņā ar tās tiesību aktiem vēl neizdod savus valstspiederīgos vai nenodod tos citas valsts jurisdikcijā,

veic vajadzīgos pasākumus, lai noteiktu tās jurisdikciju un attiecīgos gadījumos veiktu kriminālvajāšanu attiecībā uz 2., 3., 4. un 5. pantā minētajiem nodarījumiem, ja šos nodarījumus izdarījuši tās valstspiederīgie ārpus šīs dalībvalsts teritorijas.

4. Ja nodarījums ir vairāk nekā vienas dalībvalsts jurisdikcijā un ja kāda no attiecīgām valstīm var likumīgi veikt kriminālvajāšanu, ņemot par pamatu tos pašus faktus, tad attiecīgās dalībvalstis sadarbojas, lai pieņemtu lēmumu par to, kura no tām veiks likumpārkāpēju kriminālvajāšanu, lai pēc iespējas centralizētu tiesvedību vienā dalībvalstī. Lai to panāktu, dalībvalstis var izmantot jebkuras Eiropas Savienībā izveidotās organizācijas vai mehānisma palīdzību, lai veicinātu sadarbību starp šo valstu tiesu iestādēm un šo iestāžu darbības koordināciju. Secīgi var ņemt vērā šādus faktorus:

— dalībvalsts ir tā, kuras teritorijā izdarīti nodarījumi, saskaņā ar 1. punkta a) apakšpunktu un 2. punktu,

— dalībvalsts ir tā, kuras valstspiederīgais ir izdarītājs,

— dalībvalsts ir tā, kurā izdarītājs ir atrasts.

5. Dalībvalsts var pieņemt lēmumu nepiemērot vai tikai konkrētos gadījumos vai apstākļos piemērot 1. panta b) apakšpunktā un 1. panta c) apakšpunktā izklāstītos jurisdikcijas noteikumus.

6. Dalībvalstis informē Padomes Ģenerālsēkretariātu un Komisiju, ja tās pieņem lēmumu piemērot 5. punktu, vajadzības gadījumā norādot konkrētos gadījumus vai apstākļus, kādos lēmumu piemēro.

11. pants

Informācijas apmaiņa

1. Lai apmainītos ar informāciju par 2., 3., 4. un 5. pantā minētajiem nodarījumiem, saskaņā ar datu aizsardzības noteikumiem dalībvalstis nodrošina, ka tās padara pastāvošo operatīvo kontaktpunktu tīklu pieejamu divdesmit četras stundas dienā naktī un septiņas dienas nedēļā.

2. Katra dalībvalsts informē Padomes Ģenerālsēkretariātu un Komisiju par tās noteikto kontaktpunktu informācijas apmaiņai par nodarījumiem attiecībā uz uzbrukumiem informācijas sistēmām. Ģenerālsēkretariāts šo informāciju nosūta pārējām dalībvalstīm.

12. pants

Īstenošana

1. Dalībvalstis veic vajadzīgos pasākumus, lai līdz 2007. gada 16. martam izpildītu šo pamatlēmumu.

2. Līdz 2007. gada 16. martam dalībvalstis nosūta Padomes Ģenerālsēkretariātam un Komisijai to visu noteikumu tekstus, ar ko to tiesību aktos transponē saistības, kuras tām uzliek šis pamatlēmums. Līdz 2007. gada 16. septembrim, pamatojoties uz ziņojumu, ko sagatavo, izmantojot šo informāciju, un rakstisku Komisijas ziņojumu, Padome izvērtē to, ciktāl dalībvalstis ir ievērojušas šo pamatlēmumu.

13. pants

Stāšanās spēkā

Šis pamatlēmums stājas spēkā nākamajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Briselē, 2005. gada 24. februārī

Padomes vārdā —

priekšsēdētājs

N. SCHMIT