EUROOPA KOMISJON

Brüssel 30.9.2010
KOM(2010) 517 lõplik

2010/0273 (COD)

Ettepanek

EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV,

milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega tunnistatakse kehtetuks nõukogu raamotsus 2005/222/JSK

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

SELETUSKIRI

1. ETTEPANEKU PÕHJUSED JA EESMÄRGID

Ettepanekuga asendatakse nõukogu 24. veebruari 2005. aasta raamotsus 2005/222/JSK infosüsteemide vastu suunatud rünnete kohta[1]. Nimetatud raamotsuse eesmärk, nagu see on esitatud põhjendustes, on arendada koostööd kohtuasutuste ja muude pädevate asutuste, sealhulgas liikmesriikide politsei- ja muude spetsialiseeritud õiguskaitseasutuste vahel liikmesriikide kriminaalõiguse ühtlustamise kaudu infosüsteemide vastu suunatud rünnete valdkonnas. Tegemist on ELi õigusaktiga, milles käsitletakse selliseid süütegusid nagu ebaseaduslik sisenemine infosüsteemidesse, ebaseaduslik süsteemi häirimine ja ebaseaduslik andmetesse sekkumine ning mis sisaldab erieeskirju juriidiliste isikute vastutuse, jurisdiktsiooni ja teabevahetuse kohta. Liikmesriigid pidid raamotsuse järgimiseks vajalikud meetmed võtma hiljemalt 16. märtsiks 2007.

14. juulil 2008 avaldas komisjon aruande[2] raamotsuse rakendamise kohta. Aruande kokkuvõttes märgiti, et enamikus liikmesriikides on tehtud olulisi edusamme ning rakendamise tase on suhteliselt hea, kuigi teatavates liikmesriikides ei ole rakendamist veel lõpule viidud. Aruandes märgiti, et hiljutised „ründed, mis on tabanud eri liikmesriike pärast raamotsuse vastuvõtmist, eriti infosüsteemide vastu suunatud suuremahulised üheaegsed ründed ja nn botnettide [Termin on muutunud. Uus termin on *robotivõrk*] kuritegeliku kasutamise suurenemine, osutavad mitmele uuele ohule" (vt robotivõrgu selgitus järgmises osas). Raamotsuse vastuvõtmisel ei pööratud sellistele rünnetele tähelepanu. Selleks et võtta arvesse toimunud arengut, kaalub komisjon meetmeid, mis võimaldaksid ohule senisest paremini reageerida.

2004. aasta Haagi programmis (vabaduse, turvalisuse ja õiguse tugevdamine Euroopa Liidus) ning 2009. aasta Stockholmi programmis ja selle tegevuskavas[3] rõhutati küberkuritegevuse vastase võitluse tõhustamiseks võetavate täiendavate meetmete tähtsust. Ka hiljuti esitatud Euroopa digitaalses tegevuskavas,[4] mis on esimene suurprojekt ELi 2020. aasta strateegia raames, tunnistatakse vajadust tegeleda Euroopa tasandil uute kuriteoliikidega, eelkõige küberkuritegevusega. Usalduse ja turvalisuse valdkonnas keskendub komisjon meetmetele, mille abil võideldakse infosüsteemide vastu suunatud küberrünnakute vastu.

Rahvusvahelisel tasandil peetakse praegu kõige täielikumaks rahvusvaheliseks standardiks 23. novembril 2001. aastal allakirjutatud Euroopa Nõukogu küberkuritegevuse konventsiooni,[5] kuna sellega on kehtestatud küberkuritegevuse erinevaid aspekte hõlmav üldine ja ühtne raamistik. Tänaseks on kõik 27 liikmesriiki konventsioonile alla kirjutanud, kuid ratifitseerinud on selle vaid 15[6]. Konventsioon jõustus 1. juulil 2004. EL ei ole konventsioonile alla kirjutanud. Arvestades konventsiooni olulisust, kutsub komisjon ka ülejäänud ELi liikmesriike üles konventsiooni võimalikult kiiresti ratifitseerima.

---

1 ELT L 69, 16.3.2005, lk 68.

2 Komisjoni aruanne nõukogule. Esitatud nõukogu 24. veebruari 2005. aasta raamotsuse (infosüsteemide vastu suunatud rünnete kohta) artikli 12 alusel (KOM(2008) 448 (lõplik)).

3 ELT C 198, 12.8.2005; ELT C 115, 4.5.2010; KOM (2010) 171, 20.4.2010.

4 Komisjoni teatis, KOM(2010) 245, 19.5.2010.

5 Euroopa Nõukogu küberkuritegevuse konventsioon, Budapest, 23.11.2001 (ETS nr 185).

6 Vt ülevaade konventsiooni (ETS nr 185) ratifitseerimisest: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

- **Üldine taust**

Küberkuritegevuse puhul on probleemi peamiseks põhjuseks mitmest asjaolust tulenev kaitsetus. Puudulikud õiguskaitsemehhanismid aitavad kaasa kõnealuse probleemi levikule ja süvenemisele, sest süütegude teatavad liigid on piiriülesed. Küberkuritegevusest sageli ei teatata, osalt seetõttu, et teatavaid kuritegusid ei märgata, ent ka seetõttu, et ohvrid (majandustegevuses osalejad ja ettevõtjad) ei soovi endale halba mainet ja kardavad, et nende kaitsetuse avalikustamine mõjutab nende edasisi ärilisi väljavaateid.

Ka lahknevused liikmesriikide kriminaalõiguses ja -menetluses võivad põhjustada erinevusi uurimises ja süüdistuse esitamises, tuues endaga kaasa kuritegude erineva käsitlemise. Infotehnoloogia areng on süvendanud nimetatud probleeme, sest on teinud vahendite (kurivara ja robotivõrk) tootmise ja levitamise senisest lihtsamaks, pakkudes samal ajal teo toimepanijatele anonüümsust ja hajutades vastutuse mitme jurisdiktsiooni vahel. Arvestades süüdistuse esitamise keerukust, saab organiseeritud kuritegevuse raames teenida vähese riskiga märkimisväärset kasumit.

Käesolevas ettepanekus võetakse arvesse uusi küberkuritegude toimepanemise meetodeid, eriti robotivõrgu kasutamist. Mõiste „robotivõrk” viitab arvutite võrgule, mis on nakatatud kurivaraga (arvutiviirus). Selline nakatatud arvutite (zombid) võrk võidakse käivitada konkreetse ülesande täitmiseks, näiteks infosüsteemide vastu suunatud rünneteks (küberründed). Zombisid võib kontrollida teine arvuti, kuigi sageli ei ole nakatatud arvuti kasutaja sellest teadlik. Kontrollivat arvutit tuntakse ka „käske edastava ja kontrolliva keskuse” nime all. Sellist keskust kontrollivad isikud kuuluvad teo toimepanijate hulka, kuna nad kasutavad infosüsteemide vastu suunatud rünnete jaoks võõraid arvuteid. Süüteo täideviijat on väga keeruline leida, kuna robotivõrku ühendatud arvutid, mis teostavad rünnet, võivad asuda mujal kui teo toimepanija.

Robotivõrgu abil teostatavad ründed on sageli suuremahulised. Suuremahuliseks ründeks peetakse rünnet, mille teostamiseks kasutatakse teatavaid vahendeid ja mis mõjutab kas arvestatavat hulka infosüsteeme (arvuteid) või põhjustab märkimisväärse kahju (näiteks süsteemiteenuste pakkumise katkemine, finantskulu või isikuandmete kadumine). Suuremahulise ründega põhjustatud kahju mõjutab olulisel määral sihtmärgi toimimist ja/või selle töökeskkonda. Sellises kontekstis mõistetakse „suure robotivõrgu” all robotivõrku, mis suudab põhjustada raske kahju. Robotivõrkude suurust on keeruline hinnata, kuid suurimad teadaolevad robotivõrgud koosnesid 24 tunni jooksul hinnanguliselt 40 000 – 100 000 ühendusest[7] (st nakatatud arvutist).

[7] Ühenduste arv 24 tunni jooksul on sageli kasutatav mõõtühik, mille abil väljendatakse robotivõrgu suurust.

- **Ettepaneku valdkonnas kehtivad õigusnormid**

ELi tasandil kasutati raamotsust liikmesriikide õigusaktide minimaalseks ühtlustamiseks, et kriminaliseerida mitmed küberkuriteod, sealhulgas ebaseaduslik sisenemine infosüsteemidesse, ebaseaduslik süsteemi häirimine, ebaseaduslik andmetesse sekkumine ning nimetatud süütegudele kallutamine, kaasaaitamine ja selliste süütegude katse.

Kuigi liikmesriigid on raamotsust üldiselt järginud, on raamotsusel süütegude (küberründed) ulatuse ja arvu muutumist arvestades mitmeid puudusi. Raamotsusega ühtlustatakse ainult üksikuid süütegusid käsitlevaid õigusakte, kuid selles ei käsitleta täiel määral suuremahulise ründega kaasnevat võimalikku ohtu ühiskonnale. Samuti ei ole selles piisaval määral kajastatud kuritegude raskusastet ega nende suhtes kehtestatavaid sanktsioone.

Küberrünnetega seotud probleeme ning selliseid küsimusi nagu võrguturve ja Interneti kasutajate turvalisus käsitletakse teataval määral ka muudes ELi kehtivates ja kavandatud algatustes ja programmides. Nimetatud küsimustega seotud meetmed on ette nähtud programmides „Kuritegevuse ennetamine ja selle vastu võitlemine”,[8] „Kriminaalõigus”,[9] „Turvalisema Interneti programm”[10] ja „Elutähtsa infoinfrastruktuuri kaitse”[11]. Lisaks nimetatud raamotsusele on teiseks oluliseks kehtivaks õigusaktiks raamotsus 2004/68/JSK laste seksuaalse ekspluateerimise ja lapsporno vastu võitlemise kohta.

Haldustasandil on arvutite nakatamine ja nende sidumine robotivõrguks eraelu puutumatust ja andmekaitset käsitlevate ELi eeskirjadega[12] juba keelatud ning liikmesriikide haldusasutused teevad koostööd rämpsposti vastu võitlevate asutuste Euroopa kontaktvõrgustiku kaudu. Nimetatud eeskirjade kohaselt peavad liikmesriigid keelustama avalike sidevõrkude ja avalikult kättesaadavate elektrooniliste sideteenuste kaudu edastatava teabe pealtkuulamise, kui asjaomane kasutaja ei ole selleks nõusolekut andnud või kui puudub õiguslik alus.

Käesolev ettepanek vastab nimetatud eeskirjadele. Liikmesriigid peaksid tähelepanu pöörama haldus- ja õiguskaitseasutuste koostöö parandamisele küsimustes, mis on seotud nii haldus- kui ka kriminaalsanktsioonidega.

- **Kooskõla Euroopa Liidu muude tegevuspõhimõtete ja eesmärkidega**

Eesmärgid on kooskõlas ELi poliitikaga, milles käsitletakse organiseeritud kuritegevuse vastast võitlust, arvutivõrkude vastupidavuse suurendamist, elutähtsa infoinfrastruktuuri kaitsmist ja andmekaitset. Eesmärgid on kooskõlas ka „Turvalisema Interneti programmiga”, mis on loodud Interneti ja uute sidustehnoloogiate turvalisema kasutamise edendamiseks ning ebaseadusliku sisuga materjalide vastu võitlemiseks.

Käesolevat ettepanekut analüüsiti põhjalikult, et tagada selle sätete täielik kooskõla põhiõigustega ning eelkõige isikuandmete kaitsega, sõna- ja teabevabadusega, õigusega

---

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

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

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

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

12 Direktiiv 201/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) (EÜT L 201, 31.07.2002), muudetud direktiiviga 2009/136/EÜ (ELT L 337, 18.12.2009).

õiglasele kohtulikule arutamisele, süütuse presumptsiooni ja kaitseõigusega ning kuritegude ja karistuste seaduslikkuse ja proportsionaalsuse põhimõttega.

2. KONSULTEERIMINE HUVITATUD ISIKUTEGA JA MÕJU HINDAMINE

- **Konsulteerimine huvitatud isikutega**

Paljude asjaomase valdkonna ekspertidega konsulteeriti mitmel koosolekul, kus käsitleti küberkuritegevuse vastase võitluse erinevaid aspekte, sealhulgas selliste kuritegude suhtes võetavaid kohtulikke järelmeetmeid (süüdistuse esitamist). Ekspertide hulka kuulusid eelkõige liikmesriikide valitsuste ja erasektori esindajad, spetsialiseerunud kohtunikud ja prokurörid, rahvusvahelised organisatsioonid, ELi ametid ja ekspertorganisatsioonid. Seejärel saatsid mitmed eksperdid ja organisatsioonid pöördumisi ja esitasid teavet.

Konsultatsiooni raames rõhutati peamiselt järgmisi vajadusi:

– võtta kõnealuses valdkonnas meetmeid ELi tasandil;

– kriminaliseerida süütegude liigid, mida kehtiv raamotsus ei hõlma, eelkõige küberrünnete uued vormid (robotivõrgud);

– kõrvaldada takistused piiriüleste juhtumite uurimiselt ja nende eest süüdistuse esitamiselt.

Mõju hindamisel on arvesse võetud konsultatsiooni ajal saadud tagasisidet.

Eksperdiarvamuste kogumine ja kasutamine

Välisekspertide arvamusi koguti sidusrühmadega peetud mitmetel koosolekutel.

Mõju hindamine

Hinnati mitmeid poliitikavõimalusi eesmärgi saavutamiseks.

- 1. poliitikavõimalus: säilitada praegune olukord ehk jätta ELi tasandil uued meetmed võtmata

Selle võimaluse korral edasisi meetmeid küberkuritegevuse kõnealuse konkreetse liigi, st infosüsteemide vastu suunatud rünnete suhtes ELi tasandil ei võetaks. Käimasolevaid meetmeid, eelkõige programme, mille eesmärk on tugevdada elutähtsa infoinfrastruktuuri kaitset ning parandada avaliku ja erasektori koostööd küberkuritegevuse vastases võitluses, jätkataks.

- 2. poliitikavõimalus: töötada välja programm, et tugevdada muude kui õiguslike meetmete abil jõupingutusi infosüsteemide vastu suunatud rünnete vastu võitlemiseks

Lisaks programmile „Elutähtsa infoinfrastruktuuri kaitse” võetaks muid kui õiguslikke meetmeid, mille raames keskendutaks õiguskaitseasutuste ning avaliku ja erasektori piiriülesele koostööle. Selliste soovituslike vahenditega tuleks edendada ELi tasandil koordineeritud lisategevust. Näiteks tuleks tugevdada õiguskaitseasutuste seitse päeva nädalas ööpäev läbi töötavate kontaktpunktide võrgustikku, luua avaliku ja erasektori kontaktpunktide ELi võrgustik, mis hõlmaks ka küberkuritegevuse alaseid eksperte ja õiguskaitseasutusi, töötada välja ELi teenustaseme tüüpkokkulepe õiguskaitsealaseks koostööks erasektori

ettevõtjatega ning toetada küberkuritegevuse uurimist käsitlevate koolitusprogrammide koostamist õiguskaitseasutuste jaoks.

- 3. poliitikavõimalus: ajakohastada sihipäraselt raamotsuse (st kehtivat raamotsust asendava uue direktiivi) eeskirju, et käsitleda infosüsteemide vastu suunatud suuremahuliste rünnetega (robotivõrgud) kaasnevat ohtu, suurendada liikmesriikide õiguskaitseasutuste kontaktpunktide tõhusust, kui selline rünne on toime pandud süüteo täideviija tegelikku identiteeti varjates ja tegeliku identiteedi omanikku kahjustades, ning hakata koguma statistilisi andmeid küberrünnakute kohta

Selle võimaluse korral kehtestataks konkreetne (st piiratud) õigusakt, mille eesmärk on ära hoida infosüsteemide vastu suunatud suuremahulised ründed. Lisaks sellisele jõulisele õigusaktile võetaks kõnealuste rünnete vastu suunatud piiriülese operatiivkoostöö tugevdamiseks ka muid kui õiguslikke meetmeid, mis hõlbustaksid õiguslike meetmete rakendamist. Meetmete eesmärk oleks suurendada elutähtsa infoinfrastruktuuri valmisolekut, turvalisust ja vastupidavust ning vahetada parimaid tavasid.

- 4. poliitikavõimalus: kehtestada küberkuritegevuse vastane ulatuslik ELi õigusakt

Selle võimaluse korral kehtestataks uus ulatuslik ELi õigusakt. Lisaks 2. poliitikavõimaluse raames kirjeldatud soovituslike meetmete võtmisele ja 3. poliitikavõimaluse raames kavandatud eeskirjade ajakohastamisele lahendataks käesoleva võimaluse raames ka muid Interneti kasutamisega seotud õiguslikke probleeme. Kõnealune võimalus ei hõlmaks mitte ainult infosüsteemide vastu suunatud meetmeid, vaid selle raames käsitletaks ka selliseid küsimusi nagu finantsalane küberkuritegevus, Internetis olevad ebaseadusliku sisuga materjalid, elektrooniliste tõendite kogumine, säilitamine ja edastamine ning senisest üksikasjalikumad jurisdiktsiooni käsitlevad sätted. Õigusakt kehtiks paralleelselt Euroopa Nõukogu küberkuritegevuse konventsiooniga ja sellega kaasneksid eespool nimetatud muud kui õiguslikud meetmed.

- 5. poliitikavõimalus: ajakohastada Euroopa Nõukogu küberkuritegevuse konventsiooni

Selle võimaluse raames tuleks kehtiva konventsiooni üle pidada uusi läbirääkimisi, mis on aeganõudev protsess ja ei vasta mõjuhinnangus kavandatud tegevuse ajakavale. Näib, et rahvusvahelisel tasandil puudub ka soov hakata konventsiooni üle läbirääkimisi pidama. Seega ei saa konventsiooni ajakohastamist pidada teostatavaks võimaluseks, kuna seda ei ole võimalik teha nõutava ajakava raames.

Eelistatud poliitikavõimalus: muude kui õiguslike meetmete (2. võimalus) ja raamotsuse sihipärase ajakohastamise (3. võimalus) kombinatsioon

Pärast majandusliku ja sotsiaalse ning põhiõigustele avalduva mõju analüüsimist leiti, et 2. ja 3. võimalus pakuvad parimat viisi lahendada asjaomast probleemi ja saavutada ettepaneku eesmärke.

Käesoleva ettepaneku koostamiseks korraldas komisjon mõju hindamise.

3. ETTEPANEKU ÕIGUSLIK KÜLG

- **Kavandatud meetmete kokkuvõte**

Direktiivis, millega tunnistatakse kehtetuks raamotsus 2005/222/JSK, säilitatakse praegused sätted ning sellesse lisatakse järgmised uued osad:

– kriminaalõigus üldiselt:

A. direktiiviga keelatakse toota, müüa, kasutamiseks hankida, importida, levitada ja muul viisil kättesaadavaks teha süütegude toimepanemiseks kasutatavaid seadmeid ja vahendeid;

B. direktiivi lisatakse järgmised raskendavad asjaolud:

- suuremahulised ründed: uus raskendav asjaolu hõlmab robotivõrku ja samalaadseid vahendeid, muutes nende kasutamise kehtivas raamotsuses loetletud kuritegude toimepanemisel raskendavaks asjaoluks;

- kui kõnealune rünne on toime pandud süüteo täideviija tegelikku identiteeti varjates ja tegeliku identiteedi omanikku kahjustades. Kõik sellised eeskirjad peaksid olema kooskõlas kuritegude ja karistuste seaduslikkuse ja proportsionaalsuse põhimõttega ning kooskõlas isikuandmete kaitset käsitlevate õigusaktidega[13];

C. direktiiviga kriminaliseeritakse teabe ebaseaduslik pealtkuulamine;

D. direktiiviga nähakse ette meetmed, et aidata kaasa Euroopa kriminaalõigusalasele koostööle, tugevdades selleks seitse päeva nädalas ööpäev läbi töötavate kontaktpunktide struktuuri[14]:

- kehtestatakse kohustus vastata abitaotlusele kindlaks määratud tähtaja jooksul operatiivse kontaktpunkti kaudu (direktiivi artikkel 14). Sellist siduvat sätet küberkuritegevuse konventsioonis ei ole. Sellise kohustusega tagatakse, et kontaktpunktid teatavad kindla tähtaja jooksul, kas ja mis ajaks nad saavad abitaotluse rahuldada. Teate tegelikku sisu ei ole täpsustatud;

E. direktiiviga rahuldatakse vajadus küberkuritegusid käsitlevate statistiliste andmete järele, kuna selliste andmete esitamine muudetakse liikmesriikidele kohustuslikuks, et tagada nõuetekohane süsteem kehtivas raamotsuses nimetatud süütegusid ja uut lisatud süütegu – teabe ebaseaduslik pealtkuulamine – käsitlevate statistiliste andmete salvestamiseks, koostamiseks ja esitamiseks.

Direktiivi artiklites 3, 4 ja 5 nimetatud kuritegude (ebaseaduslik sisenemine infosüsteemi, ebaseaduslik süsteemi häirimine ja ebaseaduslik andmetesse sekkumine) määratlused

---

[13] Näiteks Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) (EÜT L 201, 31.07.2002, lk 37–47 (praegu läbivaatamisel) ning üldine andmekaitsedirektiiv 95/46/EÜ.

[14] Loodud küberkuritegevuse konventsiooni ja raamotsusega 2005/222/JSK infosüsteemide vastu suunatud rünnete kohta.

sisaldavad sätet, mille kohaselt võib direktiivi ülevõtmisel liikmesriigi õigusse kriminaliseerida vaid kõnealuste kuritegude „olulised juhtumid". Selline paindlikkus on ette nähtud selleks, et liikmesriigid saaksid jätta reguleerimisalast välja juhtumid, mis on *in abstracto* hõlmatud põhimääratlusega, kuid mida ei peeta õiguslikult kaitstud huvi kahjustavaks, näiteks noorte teatavad teod, mis pannakse toime infotehnoloogilise pädevuse näitamiseks. Võimalus piirata tegude kriminaliseerimist ei tohiks endaga siiski kaasa tuua täiendava kuriteokoosseisu kehtestamist, kuna see looks olukorra, millega on hõlmatud ainult raskendavatel asjaoludel toimepandud süüteod. Direktiivi ülevõtmisel liikmesriigi õigusesse peaksid liikmesriigid hoiduma eelkõige täiendavate kuriteokoosseisude kehtestamisest kergemate süütegude puhul, nagu kindel soov saada kuritegelikul teel ebaseaduslikku tulu, ja sellise konkreetse mõjuga seotud nõude lisamisest nagu märkimisväärse kahju põhjustamine.

- **Õiguslik alus**

Euroopa Liidu toimimise lepingu[15] artikli 83 lõige 1.

- **Subsidiaarsuse põhimõte**

Subsidiaarsuse põhimõtet kohaldatakse Euroopa Liidu meetmete suhtes. Liikmesriigid ei suuda ettepaneku eesmärke täielikult saavutada järgmistel põhjustel.

Küberkuritegevusel ja eelkõige infosüsteemide vastu suunatud rünnetel on märkimisväärne piiriülene mõõde, mis on eriti ilmne suuremahuliste rünnete puhul, kuna rünnet ühendavad lülid asuvad sageli teises asukohas ja teises riigis. See eeldab ELi meedet, eelkõige selleks, et jälgida suuremahuliste rünnetega seotud arengut Euroopas ja maailmas. Ka nõukogu 2008. aasta novembri järeldustes[16] kutsuti üles võtma ELi meedet ja ajakohastama raamotsust 2005/222/JSK, sest liikmesriigid üksi ei suuda kodanikke küberkuritegude eest tõhusalt kaitsta.

Euroopa Liidu meetmega saavutatakse ettepaneku eesmärgid paremini järgmistel põhjustel.

Ettepanekuga jätkatakse liikmesriikide kriminaalõiguse ja -menetluse eeskirjade ühtlustamist, millel on positiivne mõju asjaomaste kuritegude vastasele võitlusele. Esiteks takistatakse sel viisil teo toimepanijate liikumist liikmesriikidesse, kus küberrünnakuid käsitlevad õigusaktid on leebemad. Teiseks võimaldavad ühtsed eeskirjad vahetada teavet ning koguda ja võrrelda asjaomaseid andmeid. Kolmandaks tõhustatakse nii ennetusmeetmeid kogu ELis kui ka rahvusvahelist koostööd.

Seepärast on ettepanek kooskõlas subsidiaarsuse põhimõttega.

- **Proportsionaalsuse põhimõte**

Ettepanek on proportsionaalsuse põhimõttega kooskõlas järgmisel põhjusel.

Käesolev direktiiv ei lähe nimetatud eesmärkide saavutamiseks Euroopa Liidu tasandil vajalikust kaugemale, võttes seejuures arvesse vajadust kehtestada täpsed kriminaalõiguse alased õigusaktid.

---

15 ELT C 83/49, 30.3.2010.

16 Nõukogu järeldused küberkuritegevuse vastase võitluse kooskõlastatud tööstrateegia ja konkreetsete meetmete kohta, justiits- ja siseküsimuste nõukogu 2987. istung Brüsselis, 27.–28.11.2008.

- **Vahendi valik**

Kavandatav vahend: direktiiv.

Muud meetmed ei oleks asjakohased järgmisel põhjusel:

õiguslik alus eeldab direktiivi.

Muud kui õiguslikud meetmed ja isereguleerimine parandaksid olukorda teatavates valdkondades, kus oluline on rakendamine. Samal ajal teistes valdkondades, kus olulised on uued õigusaktid, oleks saadav kasu mõõdukas.

4. MÕJU EELARVELE

Ettepaneku mõju ELi eelarvele on väike. Hinnangulisest kulust (5 913 000 eurot) rohkem kui 90 % kannaksid liikmesriigid, kes saavad kulude vähendamiseks taotleda ELi vahendeid.

5. TÄIENDAV TEAVE

- **Senise õigusakti kehtetuks tunnistamine**

Ettepaneku vastuvõtmisega kaasneb senise õigusakti kehtetuks tunnistamine.

- **Territoriaalne kohaldamisala**

Käesolev direktiiv on vastavalt aluslepingutele adresseeritud liikmesriikidele.

2010/0273 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV,

milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega tunnistatakse kehtetuks nõukogu raamotsus 2005/222/JSK

EUROOPA PARLAMENT JA EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut,

eriti selle artikli 83 lõiget 1,

võttes arvesse Euroopa Komisjoni ettepanekut[17],

olles edastanud seadusandliku akti eelnõu riikide parlamentidele,

võttes arvesse Euroopa Majandus- ja Sotsiaalkomitee arvamust,

võttes arvesse Regioonide Komitee arvamust,

toimides seadusandliku tavamenetluse kohaselt

ning arvestades järgmist:

(1) Käesoleva direktiivi eesmärk on ühtlustada liikmesriikide kriminaalõigust infosüsteemide vastu suunatud rünnete valdkonnas ning arendada koostööd kohtuasutuste ja muude pädevate asutuste, sealhulgas liikmesriikide politsei- ja muude spetsialiseeritud õiguskaitseasutuste vahel.

(2) Infosüsteemide vastu suunatud, eelkõige organiseeritud kuritegevuse ohust tulenevate rünnete oht aina suureneb ning seega mure infosüsteemide kui liikmesriikide ja ELi elutähtsa infrastruktuuri osa vastu suunatud võimalike terrori- või poliitiliselt ajendatud rünnakute pärast kasvab. See on ohuks nii infoühiskonna turvalisemaks muutmisele kui ka vabadusel, turvalisusel ja õigusel rajaneva ala saavutamisele ning nõuab seega Euroopa Liidu tasandi meedet.

(3) On tõendeid, et üha ohtlikumaid ja korduvaid suuremahulisi ründeid suunatakse järjest enam infosüsteemide vastu, mis on riikidele või avaliku või erasektori toimimise seisukohalt äärmiselt olulised. Lisaks sellele arendatakse välja üha keerukamaid vahendeid, mida kurjategijad saavad kasutada eri liiki küberrünneteks.

(4) Ühised eeskirjad selles valdkonnas, eelkõige seoses infosüsteemide ja arvutiandmetega, on olulised tagamaks liikmesriikides järjekindlat lähenemisviisi käesoleva direktiivi kohaldamisel.

---

[17] ELT C […], […], lk […].

(5) Tuleb tagada ühine lähenemisviis kuriteokoosseisu suhtes, kriminaliseerides selleks kõikjal ELis ebaseadusliku infosüsteemi sisenemise, ebaseadusliku süsteemi häirimise, ebaseadusliku andmetesse sekkumise ja teabe ebaseadusliku pealtkuulamise.

(6) Liikmesriigid peaksid infosüsteemide vastu suunatud rünnete eest ette nägema karistused. Sätestatavad karistused peaksid olema tõhusad, proportsionaalsed ja hoiatavad.

(7) Asjakohane on näha ette keskmisest rangemad karistused juhuks, kui infosüsteemide vastu suunatud ründe on toime pannud kuritegelik ühendus, nagu see on määratletud nõukogu 24. oktoobri 2008. aasta raamotsuses 2008/841/JSK (organiseeritud kuritegevuse vastase võitluse kohta)[18], kui rünne on suuremahuline või kui süütegu on toime pandud süüteo täideviija tegelikku identiteeti varjates ja tegeliku identiteedi omanikku kahjustades. Samuti on asjakohane sätestada keskmisest rangemad karistused juhuks, kui sellise ründega on põhjustatud raske kahju või mõjutatud olulisi huve.

(8) Nõukogu 27.–28. novembri 2008. aasta järeldustes märgiti, et liikmesriigid ja komisjon peaksid välja töötama uue strateegia, võttes arvesse Euroopa Nõukogu küberkuritegevuse 2001. aasta konventsiooni. Nimetatud konventsiooniga on kehtestatud küberkuritegevuse, sealhulgas infosüsteemide vastu suunatud rünnete vastase võitluse õiguslik raamistik. Käesolev direktiiv tugineb nimetatud konventsioonile.

(9) Arvestades rünnete erinevaid toimepaneku viise ning tark- ja riistvara kiiret arengut, viidatakse käesolevas direktiivis vahenditele, mille abil on võimalik käesolevas direktiivis loetletud kuritegusid toime panna. Vahendite all mõistetakse näiteks kurivara, sealhulgas robotivõrke, mida kasutatakse küberrünnete toimepanemiseks.

(10) Käesoleva direktiiviga ei nähta ette kriminaalvastutust juhul, kui süütegu on toime pandud kriminaalse tahtluseta, näiteks infosüsteemi volitatud testimise ja kaitsmise korral.

(11) Käesoleva direktiiviga tugevdatakse võrgustike, näiteks G8 ning teabevahetuseks loodud Euroopa Nõukogu seitse päeva nädalas ööpäev läbi töötava kontaktpunktide võrgustiku tähtsust, et tagada abi kiire osutamine seoses infosüsteemide ja andmetega seotud kuritegude uurimise ja menetlusega ning kuriteo kohta elektroonilises vormis tõendite kogumisega. Arvestades suuremahuliste rünnete leviku võimalikku kiirust, peaksid liikmesriigid olema võimelised viivitamata vastama nimetatud kontaktpunktide võrgustiku kaudu esitatud kiireloomulistele taotlustele. Taotletav abi peaks hõlmama tehnilist nõustamist, andmete säilitamist, tõendite kogumist, õigusteabe andmist ja kahtlustatavate asukoha kindlakstegemist ning nimetatud tegevustele kaasaaitamist.

(12) Selleks et saada ELi tasandil probleemist senisest parem ülevaade ja aidata kaasa senisest tõhusamate lahenduste väljatöötamisele, on käesoleva direktiivi kohaselt vaja koguda andmeid süütegude kohta. Andmeid saavad kasutada ka spetsialiseeritud asutused, näiteks Europol ning Euroopa Võrgu- ja Infoturbeamet, et hinnata senisest täpsemini küberkuritegevuse ulatust ning võrgu- ja infoturbe olukorda Euroopas.

---

[18] ELT L 300, 11.11.2008, lk 42.

(13) Märkimisväärsed lüngad ja erinevused liikmesriikide infosüsteemide vastu suunatud rünnete valdkonna õigusaktides võivad takistada organiseeritud kuritegevuse ja terrorismi vastast võitlust ning raskendada tõhusat politsei- ja õigusalast koostööd kõnealuses valdkonnas. Tänapäevaste infosüsteemide riikidevahelise ja piirideta olemuse tõttu on selliste süsteemide vastu suunatud rünnetel sageli piiriülene mõõde, mis rõhutab kiireloomulist vajadust asjaomase valdkonna kriminaalõiguse edasise ühtlustamise järele. Lisaks sellele peaks nõukogu raamotsus 2009/948/JSK (kohtualluvuskonflikti vältimise ja lahendamise kohta kriminaalmenetluses) hõlbustama infosüsteemide vastu suunatud rünnete eest süüdistuse esitamise kooskõlastamist.

(14) Kuna käesoleva direktiivi eesmärke, nimelt tagada kõikides liikmesriikides tõhusad, proportsionaalsed ja hoiatavad kriminaalkaristused infosüsteemide vastu suunatud rünnete eest ning arendada ja soodustada õigusalast koostööd võimalike probleemide kõrvaldamise teel, ei suuda liikmesriigid piisaval määral saavutada, kuna eeskirjad peavad olema ühised ja üksteisega kooskõlas, ning need on paremini saavutatavad ELi tasandil, võib EL võtta meetmeid kooskõlas Euroopa Liidu lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega. Käesolev direktiiv ei lähe nimetatud eesmärkide saavutamiseks vajalikust kaugemale.

(15) Käesoleva direktiivi rakendamise eesmärgil töödeldud isikuandmeid tuleks kaitsta vastavalt nõukogu 27. novembri 2008. aasta raamotsusele 2008/977/JSK (kriminaalasjades tehtava politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta[19]), kui töötlustoimingud kuuluvad käesoleva direktiivi reguleerimisalasse, ning Euroopa Parlamendi ja nõukogu 18. detsembri 2000. aasta määrusele (EÜ) nr 45/2001 (üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta[20]).

(16) Käesolevas direktiivis austatakse põhiõigusi ja järgitakse eelkõige Euroopa Liidu põhiõiguste hartas tunnustatud põhimõtteid, sealhulgas isikuandmete kaitset, sõna- ja teabevabadust, õigust õiglasele kohtulikule arutamisele, süütuse presumptsiooni ja kaitseõigust ning kuritegude ja karistuste seaduslikkuse ja proportsionaalsuse põhimõtet. Eelkõige on käesoleva direktiivi eesmärk tagada nimetatud õiguste täielik austamine ja sellest tuleb direktiivi järgimisel ka lähtuda.

(17) [Euroopa Liidu toimimise lepingule lisatud protokolli (Ühendkuningriigi ja Iirimaa seisukoha kohta vabadusel, turvalisusel ja õigusel rajaneva ala suhtes) artiklite 1, 2, 3 ja 4 kohaselt on Ühendkuningriik ja Iirimaa teatanud oma soovist osaleda käesoleva direktiivi vastuvõtmisel ja kohaldamisel] VÕI [Ilma et see piiraks protokolli (Ühendkuningriigi ja Iirimaa seisukoha kohta vabadusel, turvalisusel ja õigusel rajaneva ala suhtes) artikli 4 kohaldamist, ei osale Ühendkuningriik ega Iirimaa käesoleva direktiivi vastuvõtmisel ning see ei ole nende suhtes siduv ega kohaldatav].

(18) Euroopa Liidu toimimise lepingule lisatud Taani seisukohta käsitleva protokolli artiklite 1 ja 2 kohaselt ei osale Taani käesoleva direktiivi vastuvõtmisel, mistõttu see ei ole tema suhtes siduv ega kohaldatav,

---

19 ELT L 350, 30.12.2008, lk 60.

20 EÜT L 8, 12.1.2001, lk 1.

ON VASTU VÕTNUD KÄESOLEVA DIREKTIIVI:

Artikkel 1
Sisu

Käesoleva direktiiviga määratletakse infosüsteemide vastu suunatud rünnete valdkonna kuriteod ja kehtestatakse miinimumeeskirjad selliste kuritegude eest määratavate karistuste kohta. Samuti on direktiivi eesmärk kehtestada üldsätted, millega hoitakse sellised ründed ära ja aidatakse kõnealuses valdkonnas kaasa Euroopa kriminaalõigusalasele koostööle.

Artikkel 2
Mõisted

Käesolevas direktiivis kasutatakse järgmisi mõisteid:

a) „infosüsteem” – seade või omavahel ühendatud või seotud seadmete rühm, mille hulgast üks või mitu seadet teostavad vastavalt programmile arvutiandmete automaattöötlust; samuti nimetatud seadme või seadmete rühma salvestatud, töödeldud, välja võetud ja edastatud arvutiandmed, mis on vajalikud kõnealuse seadme või seadmete rühma toimimiseks, kasutamiseks, kaitseks ja hoolduseks;

b) „arvutiandmed” – faktide, teabe või mõistete esitamine infosüsteemis töötlemiseks sobivas vormis, sealhulgas programm, mille abil saab infosüsteemi panna ülesannet täitma;

c) „juriidiline isik” – üksus, millel on vastavalt kohaldatavale õigusele juriidilise isiku staatus, välja arvatud riigid ja riigivõimu teostavad avalik-õiguslikud asutused ning avalik-õiguslikud rahvusvahelised organisatsioonid;

d) „õigusliku aluseta” – süsteemi sisenemine ja selle häirimine ilma süsteemi või selle osa omaniku või selle suhtes muu õiguse valdaja loata või rikkudes riiklikke õigusakte.

Artikkel 3
Ebaseaduslik sisenemine infosüsteemi

Liikmesriik võtab vajalikud meetmed tagamaks, et õigusliku aluseta tahtlik sisenemine infosüsteemi või selle osasse on vähemalt oluliste juhtumite puhul kriminaalkorras karistatav.

Artikkel 4
Ebaseaduslik süsteemi häirimine

Liikmesriik võtab vajalikud meetmed tagamaks, et infosüsteemi töö tahtlik takistamine ja katkestamine arvutiandmete sisestamise, edastamise, kahjustamise, kustutamise, rikkumise, muutmise, sulustamise ja ligipääsmatuks muutmise teel juhul, kui tegu pannakse toime ilma õigusliku aluseta, on vähemalt raskemate juhtumite puhul kriminaalkorras karistatav.

Artikkel 5

Ebaseaduslik andmetesse sekkumine

Liikmesriik võtab vajalikud meetmed tagamaks, et infosüsteemis olevate arvutiandmete tahtlik kustutamine, kahjustamine, rikkumine, muutmine, sulustamine ja ligipääsmatuks muutmine juhul, kui tegu pannakse toime ilma õigusliku aluseta, on vähemalt raskete juhtumite puhul kriminaalkorras karistatav.

Artikkel 6

Teabe ebaseaduslik pealtkuulamine

Liikmesriik võtab vajalikud meetmed tagamaks, et infosüsteemi, sellest süsteemist või selle süsteemi piires, sealhulgas infosüsteemi elektromagnetkiirguse abil mitteavalikult edastatavate arvutiandmete tahtlik pealtkuulamine tehniliste vahendite abil on kriminaalkorras karistatav, kui tegu pannakse toime ilma õigusliku aluseta.

Artikkel 7

Süüteo toimepanemisel kasutatud vahendid

Liikmesriik võtab vajalikud meetmed tagamaks, et järgmiste seadmete ja andmete tootmine, müük, kasutamiseks hankimine, importimine, omamine, levitamine ja muul viisil kättesaadavaks tegemine on kriminaalkorras karistatav, kui tegu on toime pandud tahtlikult ja ilma õigusliku aluseta eesmärgiga panna toime mõni artiklites 3–6 nimetatud süütegu:

a) seade, sealhulgas arvutiprogramm, mis on loodud või kohandatud eelkõige artiklites 3–6 nimetatud süütegude toimepanemiseks;

b) arvuti salasõna, juurdepääsukood ja samalaadsed andmed, mille abil on võimalik siseneda infosüsteemi või selle osasse.

Artikkel 8

Süüteole kihutamine, kaasaaitamine ja süüteokatse

1. Liikmesriik tagab, et artiklites 3–7 nimetatud süütegudele kihutamine ja kaasaaitamine on kriminaalkorras karistatav.

2. Liikmesriik tagab, et artiklites 3–6 nimetatud süütegude katsed on kriminaalkorras karistatavad.

Artikkel 9

Karistused

1. Liikmesriik võtab vajalikud meetmed tagamaks, et artiklites 3–8 nimetatud süütegude eest karistatakse tõhusate, proportsionaalsete ja hoiatavate kriminaalkaristustega.

2. Liikmesriik võtab vajalikud meetmed tagamaks, et artiklites 3–7 nimetatud süütegude eest määratakse kriminaalkaristus, mille maksimummäär on vähemalt kaheaastane vangistus.

Artikkel 10

Raskendavad asjaolud

1. Liikmesriik võtab vajalikud meetmed tagamaks, et artiklites 3–7 nimetatud süütegude eest määratakse kriminaalkaristus, mille maksimummäär on vähemalt viieaastane vangistus, kui selline süütegu on toime pandud raamotsuses 2008/841/JSK määratletud kuritegeliku ühenduse raames.

2. Liikmesriik võtab vajalikud meetmed tagamaks, et artiklites 3–6 nimetatud süütegude eest määratakse kriminaalkaristus, mille maksimummäär on vähemalt viieaastane vangistus, kui selline süütegu on toime pandud arvestatavat hulka infosüsteeme mõjutavate või märkimisväärset kahju (näiteks süsteemiteenuste pakkumise katkemine, finantskulu või isikuandmete kadumine) põhjustavate rünnete jaoks loodud vahendi kasutamise abil.

3. Liikmesriik võtab vajalikud meetmed tagamaks, et artiklites 3–6 nimetatud süütegude eest määratakse kriminaalkaristus, mille maksimummäär on vähemalt viieaastane vangistus, kui selline süütegu on toime pandud süüteo täideviija tegelikku identiteeti varjates ja tegeliku identiteedi omanikku kahjustades.

Artikkel 11

Juriidilise isiku vastutus

1. Liikmesriik võtab vajalikud meetmed tagamaks, et juriidilist isikut saab vastutusele võtta artiklites 3–8 nimetatud süütegude eest, mille on tema kasuks toime pannud eraisikuna või juriidilise isiku organi liikmena tegutsenud isik, kes on juriidilise isiku juures juhtival kohal ühel järgmistest alustest:

   a) õigus esindada juriidilist isikut;

   b) õigus teha juriidilise isiku nimel otsuseid;

   c) õigus kontrollida juriidilist isikut.

2. Liikmesriik võtab vajalikud meetmed tagamaks, et juriidilist isikut saab vastutusele võtta juhul, kui lõikes 1 osutatud isiku järelevalve või kontrolli puudumise tõttu on osutunud võimalikuks, et kõnealuse juriidilise isiku alluvuses olev isik on tema kasuks pannud toime mõne artiklites 3–8 nimetatud süüteo.

3. Juriidilise isiku lõigete 1 ja 2 kohane vastutus ei vabasta kriminaalmenetlusest füüsilist isikut, kes on mõne artiklites 3–8 nimetatud süüteo täideviija või sellele kaasaaitaja.

Artikkel 12

Juriidilise isiku suhtes kohaldatavad karistused

1. Liikmesriik võtab vajalikud meetmed tagamaks, et artikli 11 lõike 1 kohaselt vastutusele võetud juriidilise isiku suhtes kohaldatakse tõhusaid, proportsionaalseid ja hoiatavaid karistusi, mille hulka kuuluvad kriminaalõiguslikud ja muud trahvid ning võivad kuuluda muud sanktsioonid, näiteks:

a) riiklike hüvitiste või abi saamise õigusest ilmajätmine;

b) ajutine või alaline ettevõtluskeeld;

c) kohtuliku järelevalve alla võtmine;

d) sundlõpetamine;

e) süüteo toimepanekuks kasutatud üksuste ajutine või lõplik sulgemine.

2. Liikmesriik võtab vajalikud meetmed tagamaks, et artikli 11 lõike 2 kohaselt vastutusele võetud juriidilise isiku suhtes kohaldatakse tõhusaid, proportsionaalseid ja hoiatavaid karistusi ning meetmeid.

Artikkel 13
Jurisdiktsioon

1. Liikmesriik kehtestab oma jurisdiktsiooni artiklites 3–8 nimetatud süütegude suhtes, kui süütegu on pandud toime:

a) osaliselt või tervikuna asjaomase liikmesriigi territooriumil või

b) asjaomase liikmesriigi kodaniku poolt või isiku poolt, kelle peamine elukoht asub selle liikmesriigi territooriumil, või

c) juriidilise isiku huvides, kelle peakontor asub asjaomase liikmesriigi territooriumil.

2. Jurisdiktsiooni kehtestamisel kooskõlas lõike 1 punktiga a tagab liikmesriik, et jurisdiktsioon hõlmab juhtumeid, mille puhul:

a) teo toimepanija viibib süüteo toimepanemise ajal füüsiliselt asjaomase liikmesriigi territooriumil, olenemata sellest, kas süütegu on suunatud selle liikmesriigi territooriumil asuva infosüsteemi vastu või mitte, või

b) süütegu on suunatud asjaomase liikmesriigi territooriumil asuva infosüsteemi vastu, olenemata sellest, kas teo toimepanija viibib süüteo toimepanemise ajal selle liikmesriigi territooriumil.

Artikkel 14
Teabevahetus

1. Liikmesriik kasutab kooskõlas andmekaitse-eeskirjadega artiklites 3–8 nimetatud süütegudega seotud teabe vahetamiseks operatiivsete kontaktpunktide võrgustikku, mis on tema käsutuses seitse päeva nädalas ööpäev läbi. Samuti tagab liikmesriik menetlused, mis võimaldavad tal vastata kiireloomulistele taotlustele hiljemalt kaheksa tunni jooksul. Sellises vastuses tuleb vähemalt märkida, kas, millises vormis ja millal abitaotlusele vastatakse.

2. Liikmesriik teatab komisjonile oma määratud kontaktpunktist, mille kaudu vahetatakse artiklites 3–8 nimetatud süütegude alast teavet. Komisjon edastab selle teabe teistele liikmesriikidele.

Artikkel 15

Järelevalve ja statistika

1. Liikmesriik tagab süsteemi artiklites 3–8 nimetatud süütegusid käsitlevate statistiliste andmete salvestamiseks, koostamiseks ja esitamiseks.

2. Lõikes 1 nimetatud statistika hõlmab vähemalt liikmesriigile teatatud, artiklites 3–8 nimetatud süütegude arvu ja sellisele teatamisele järgnenud meetmeid, samuti esitatakse selle raames igal aastal teatatud uuritud juhtumite arv, selliste isikute arv, kellele on esitatud süüdistus, ja artiklites 3–8 nimetatud süütegude eest süüdimõistetud isikute arv.

3. Liikmesriik edastab käesoleva artikli kohaselt kogutud andmed komisjonile. Liikmesriik tagab ka statistiliste aruannete koondülevaate avaldamise.

Artikkel 16
Raamotsuse 2005/222/JSK kehtetuks tunnistamine

Raamotsus 2005/222/JSK tunnistatakse kehtetuks, ilma et see piiraks liikmesriigi kohustusi, mis on seotud direktiivi liikmesriigi õigusesse ülevõtmise tähtaegadega.

Viiteid kehtetuks tunnistatud raamotsusele tõlgendatakse viidetena käesolevale direktiivile.

Artikkel 17
Liikmesriigi õigusesse ülevõtmine

1. Liikmesriik jõustab käesoleva direktiivi järgimiseks vajalikud õigus- ja haldusnormid hiljemalt [kahe aasta jooksul alates direktiivi vastuvõtmisest]. Liikmesriik edastab kõnealuste normide teksti ning kõnealuste normide ja käesoleva direktiivi vahelise vastavustabeli viivitamata komisjonile. Kui liikmesriigid need normid vastu võtavad, lisavad nad nendesse normidesse või nende normide ametliku avaldamise korral nende juurde viite käesolevale direktiivile. Sellise viitamise viisi näevad ette liikmesriigid.

2. Liikmesriigid edastavad komisjonile käesoleva direktiiviga reguleeritavas valdkonnas nende poolt vastuvõetud põhiliste õigus- ja haldusnormide teksti.

Artikkel 18
Aruandlus

1. Komisjon esitab [NELJA AASTA JOOKSUL ALATES DIREKTIIVI VASTUVÕTMISEST] ja seejärel iga kolme aasta järel Euroopa Parlamendile ja nõukogule aruande käesoleva direktiivi järgimise kohta liikmesriikides ning vajaduse korral asjakohase ettepaneku.

2. Liikmesriik edastab komisjonile lõikes 1 osutatud aruande koostamiseks kogu vajaliku teabe. Teave sisaldab käesoleva direktiivi järgimiseks võetud õiguslike ja muude meetmete üksikasjalikku kirjeldust.

Artikkel 19
Jõustumine

Käesolev direktiiv jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Artikkel 20
Adressaadid

Käesolev direktiiv on vastavalt aluslepingutele adresseeritud liikmesriikidele.

Brüssel,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*