(Euroopa Liidu lepingu VI jaotise kohaselt vastuvõetud aktid)

NÕUKOGU RAAMOTSUS 2005/222/JSK,

24. veebruar 2005,

infosüsteemide vastu suunatud rünnete kohta

EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu lepingut, eriti selle artiklit 29, artikli 30 lõike 1 punkti a, artikli 31 lõike 1 punkti e ja artikli 34 lõike 2 punkti b,

võttes arvesse komisjoni ettepanekut,

võttes arvesse Euroopa Parlamendi arvamust, [1]

ning arvestades järgmist:

(1) Käesoleva raamotsuse eesmärgiks on arendada koostööd kohtuasutuste ja muude pädevate asutuste, sealhulgas liikmesriikide politsei- ja muude spetsialiseeritud õiguskaitseorganite vahel liikmesriikide kriminaalõiguse ühtlustamise kaudu infosüsteemide vastu suunatud rünnete valdkonnas.

(2) On tõendeid infosüsteemide vastu suunatud, eelkõige organiseeritud kuritegevuse ohust tulenevate rünnete kohta ja mure infosüsteemide kui liikmesriikide olulise infrastruktuuri osa vastu suunatud potentsiaalsete terrorirünnakute pärast kasvab. See on ohuks turvalisema infoühiskonna ning vabadusel, turvalisusel ja õigusel rajaneva ala saavutamisel ning nõuab seega reageerimist Euroopa Liidu tasandil.

(3) Nimetatud ohtudele reageerimiseks on vaja terviklikku lähenemist võrgu- ja infoturbele, nagu rõhutatakse e-Euroopa tegevuskavas, komisjoni teatises "Võrgu- ja infoturve: Euroopa lähenemisviisi ettepanek" ning nõukogu 28. jaanuari 2002. aasta resolutsioonis võrgu- ja andmeturbe valdkonna ühise lähenemisviisi ja erimeetmete kohta. [2]

(4) Vajadust suurendada teadlikkust infoturbega seotud probleemide suhtes ja anda praktilist abi rõhutati ka Euroopa Parlamendi 5. septembri 2001 resolutsioonis.

(5) Märkimisväärsed lüngad ja erinevused liikmesriikide kõnealuse valdkonna õigusaktides võivad takistada organiseeritud kuritegevuse ja terrorismi vastast võitlust ning raskendada tõhusat politsei- ja õigusalast koostööd infosüsteemide vastu suunatud rünnete valdkonnas. Kaasaegsete infosüsteemide riikidevahelise ja piirideta olemuse tõttu on ründed nimetatud süsteemide vastu sageli piiriülese iseloomuga, rõhutades seega kiireloomulist vajadust antud valdkonna kriminaalõiguse edasise ühtlustamise järele.

(6) Nõukogu ja komisjoni tegevuskavas selle kohta, kuidas kõige paremini rakendada Amsterdami lepingu vabadusel, turvalisusel ja õiglusel rajanevat ala käsitlevaid sätteid, [3] Euroopa Ülemkogu 15. ja 16. oktoobri 1999. aasta Tampere istungil ja Euroopa Ülemkogu 19. ja 20. juuni 2000. aasta Santa Maria da Feira istungil, komisjoni "tulemustabelis" ning Euroopa Parlamendi 19. mai 2000. aasta resolutsioonis tõdetakse vajadust kõrgtehnoloogiaga seotud kuritegevuse vastu suunatud seadusandliku tegevuse, sealhulgas ühiste määratluste, inkrimineerimiste ja sanktsioonide järele ning kutsutakse üles sellist tegevust ellu viima.

(7) Tuleb täiendada rahvusvaheliste organisatsioonide tööd, eelkõige Euroopa Nõukogu tööd kriminaalõiguse ühtlustamisel ja G8 tööd riikidevahelise koostöö arendamisel kõrgtehnoloogiaga seotud kuritegevuse valdkonnas, luues selleks Euroopa Liidus antud valdkonda käsitleva ühise lähenemisviisi. Nimetatud üleskutset arendati edasi komisjoni poolt nõukogule, Euroopa Parlamendile, majandus- ja sotsiaalkomiteele ning regioonide komiteele adresseeritud teatises "Turvalisema infoühiskonna poole, parandades infoinfrastruktuuride turvalisust ja võideldes arvutikuritegevuse vastu".

(8) Infosüsteemide vastu suunatud ründeid käsitlevat kriminaalõigust tuleks ühtlustada, et tagada võimalikult tihe politsei- ja õigusalane koostöö infosüsteemide vastu suunatud rünnetega seotud kuritegude valdkonnas ning aidata kaasa organiseeritud kuritegevuse ja terrorismi vastasele võitlusele.

([1]) ELT C 300 E, 11.12.2003, lk 26.
([2]) EÜT C 43, 16.2.2002, lk 2.
([3]) EÜT C 19, 23.1.1999, lk 1.

(9) Kõik liikmesriigid on ratifitseerinud 28. jaanuari 1981. aasta Euroopa Nõukogu isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni. Käesoleva raamotsuse kohaldamise kontekstis töödeldud isikuandmed peaksid olema kaitstud vastavalt nimetatud konventsiooni põhimõtetele.

(10) Ühised määratlused selles valdkonnas, eelkõige seoses infosüsteemide ja arvutiandmetega, on olulised tagamaks liikmesriikides järjekindlat lähenemisviisi käesoleva raamotsuse kohaldamisel.

(11) Tuleb saavutada ühine lähenemisviis kuritegude koosseisu tunnuste suhtes, määratledes selleks ühised süüteod seoses ebaseadusliku infosüsteemi sisenemisega, ebaseadusliku süsteemi sekkumisega ja ebaseadusliku andmetesse sekkumisega.

(12) Arvutikuritegevuse vastase võitluse huvides peaks iga liikmesriik tagama tõhusa õigusalase koostöö artiklites 2, 3, 4 ja 5 nimetatud tegevustel põhinevate kuritegude osas.

(13) Tegevuste kuritegelikeks tunnistamisel tuleb hoiduda liialdamisest, eelkõige väheoluliste juhtumite puhul, ning samuti tuleb vältida õiguse omajate ja volitatud isikute tegevuste kuritegelikuks tunnistamist.

(14) Liikmesriikidel tuleb sätestada sanktsioonid infosüsteemide vastu suunatud rünnete suhtes. Sätestatavad sanktsioonid peavad olema tõhusad, proportsionaalsed ja hoiatavad.

(15) Asjakohane on sätestada rangemad karistused juhtumiteks, kui infosüsteemi vastu suunatud rünne toimub kuritegelikus ühenduses, nagu on määratletud 21. detsembri 1998. aasta ühismeetmes 98/733/JSK Euroopa Liidu liikmesriikides kuritegelikku ühendusse kuulumise tunnistamise kohta kuriteoks. [1] Samuti on asjakohane sätestada rangemad karistused juhtumiteks, kui selline rünne on põhjustanud olulist kahju või mõjutanud olulisi huve.

(16) Samuti tuleks ette näha meetmed liikmesriikide vahelise koostöö arendamiseks eesmärgiga tagada infosüsteemide vastu suunatud rünnete vastane tõhus tegutsemine. Seega peaks liikmesriigid info vahetamiseks kasutama operatiivsete kontaktpunktide olemasolevat võrgustikku, millele on osutatud nõukogu 25. juuni 2001 soovituses ööpäevaringsete kontaktpunktide kohta kõrgtehnoloogiaga seotud kuritegevuse vastu võitlemisel. [2]

(17) Kuna käesoleva raamotsuse eesmärke – tagada kõikides liikmesriikides infosüsteemide vastu suunatud rünnete sanktsioneerimine tõhusate, proportsionaalsete ja hoiatavate kriminaalkaristuste abil ning õigusalase koostöö arendamine ja soodustamine potentsiaalsete raskuste kõrvaldamise teel – ei suuda liikmesriigid täielikult saavutada, sest eeskirjad peavad olema ühised ja kooskõlas ning on seega paremini saavutatavad liidu tasandil, võib liit vastu võtta meetmeid vastavalt EÜ asutamislepingu artiklis 5 sätestatud subsidiaarsuse põhimõttele. Kõnealuses artiklis sätestatud proportsionaalsuse põhimõtte kohaselt ei lähe käesolev raamotsus nimetatud eesmärkide saavutamiseks vajalikust kaugemale.

(18) Käesolev raamotsus austab põhiõigusi ja järgib põhimõtteid, mida tunnustatakse Euroopa Liidu lepingu artiklis 6 ja mis on kajastatud Euroopa Liidu põhiõiguste hartas, eelkõige selle II ja VI peatükis,

ON VASTU VÕTNUD KÄESOLEVA RAAMOTSUSE:

Artikkel 1

Mõisted

Käesolevas raamotsuses 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 või edastatud arvutiandmed, mis on vajalikud kõnealuse seadme või seadmete rühma toimimiseks, kasutamiseks, kaitseks ja hoolduseks.

b) *Arvutiandmed* – igasugune faktide, teabe või mõistete esitamine infosüsteemis töötlemiseks sobivas vormis, sealhulgas programm, mille abil saab infosüsteemi panna ülesannet täitma.

c) *Juriidiline isik* – üksus, millel on juriidilise isiku staatus vastavalt kehtivatele õigusaktidele, välja arvatud riigid või teised riigivõimu teostavad avalik-õiguslikud organid ja avalik-õiguslikud rahvusvahelised organisatsioonid.

[1] EÜT L 351, 29.12.1998, lk 1.

[2] EÜT C 187, 3.7.2001, lk 5.

d) *Õigusliku aluseta* – süsteemi või selle osa omaniku või selle suhtes muu õiguse omaja loata või siseriiklike õigusaktide kohaselt mitte lubatud sisenemine või sekkumine.

Artikkel 2

Ebaseaduslik sisenemine infosüsteemidesse

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

2. Iga liikmesriik võib otsustada, et lõikes 1 nimetatud tegevus on inkrimineeritav üksnes siis, kui õiguserikkumise toimepanemisel rikutakse mõnda turvameedet.

Artikkel 3

Ebaseaduslik süsteemi sekkumine

Liikmesriigid võtavad vajalikud meetmed tagamaks, et infosüsteemi töö tahtlik takistamine või katkestamine arvutiandmete sisestamise, edastamise, kahjustamise, kustutamise, rikkumise, muutmise, sulustamise või ligipääsmatuks muutmise teel on kriminaalkorras karistatav vähemalt oluliste juhtumite puhul, kui tegu pannakse toime ilma õigusliku aluseta.

Artikkel 4

Ebaseaduslik andmetesse sekkumine

Liikmesriigid võtavad vajalikud meetmed tagamaks, et infosüsteemis asuvate arvutiandmete tahtlik kustutamine, kahjustamine, rikkumine, muutmine, sulustamine või ligipääsmatuks muutmine on kriminaalkorras karistatav vähemalt oluliste juhtumite puhul, kui tegu pannakse toime ilma õigusliku aluseta.

Artikkel 5

Süüteole kallutamine, kaasaaitamine ja süüteokatse

1. Iga liikmesriik tagab, et artiklites 2, 3 ja 4 nimetatud süüteole kallutamine ja kaasaaitamine on kriminaalkorras karistatav.

2. Iga liikmesriik tagab, et artiklites 2, 3 ja 4 nimetatud süütegude katsed on kriminaalkorras karistatavad.

3. Iga liikmesriik võib otsustada artiklis 2 nimetatud süütegude suhtes lõiget 2 mitte kohaldada.

Artikkel 6

Karistused

1. Iga liikmesriik võtab vajalikud meetmed tagamaks, et artiklites 2, 3, 4 ja 5 nimetatud süütegude eest karistatakse tõhusate, proportsionaalsete ja hoiatavate kriminaalkaristustega.

2. Iga liikmesriik võtab vajalikud meetmed tagamaks, et artiklites 3 ja 4 nimetatud süüteod oleksid karistatavad kriminaalkorras, kusjuures maksimaalmääraks on vähemalt ühe- kuni kolmeaastane vangistus.

Artikkel 7

Raskendavad asjaolud

1. Kõik liikmesriigid võtavad vajalikud meetmed tagamaks, et artikli 2 lõikes 2 ning artiklites 3 ja 4 nimetatud süüteod on ühismeetmes 98/733/JSK määratletud kuritegeliku ühenduse raames toime panduna kriminaalkorras karistatavad, kusjuures maksimaalmääraks on vähemalt kahe- kuni viieaastane vangistus sõltumata nimetatud ühismeetmes viidatud sanktsioonimäärast.

2. Liikmesriik võib võtta lõikes 1 nimetatud meetmeid ka siis, kui süütegu on põhjustanud olulist kahju või on mõjutanud olulisi huve.

Artikkel 8

Juriidiliste isikute vastutus

1. Liikmesriigid võtavad vajalikud meetmed tagamaks, et juriidilisi isikuid saab võtta vastutusele artiklites 2, 3, 4 ja 5 nimetatud süütegude eest, mille on nende kasuks toime pannud iseseisvalt või juriidilise isiku organi liikmena tegutsenud isik, kes on juriidilise isiku juures juhtival kohal, järgmistel alustel:

a) õigus esindada juriidilist isikut,

b) õigus teha juriidilise isiku nimel otsuseid või

c) õigus teostada kontrolli juriidilise isiku piires.

2. Lisaks lõikes 1 sätestatud juhtudele tagavad liikmesriigid, et juriidilisi isikuid saab võtta vastutusele, kui lõikes 1 nimetatud isiku puuduliku järelevalve või kontrolli tagajärjel on osutunud võimalikuks, et juriidilise isiku alluvuses olev isik on pannud toime juriidilise isiku kasuks artiklites 2, 3, 4 ja 5 nimetatud süüteo.

3. Juriidilise isiku vastutus vastavalt lõigetele 1 ja 2 ei välista kriminaalmenetlust füüsiliste isikute suhtes, kes on osalenud artiklites 2, 3, 4 ja 5 nimetatud süütegude toimepanemises täideviija, kihutaja või kaasaaitajana.

Artikkel 9

Juriidilistele isikutele kohaldatavad karistused

1. Iga liikmesriik võtab vajalikke meetmeid tagamaks, et artikli 8 lõike 1 kohaselt vastutusele võetud juriidilise isiku suhtes saab kohaldada tõhusaid, proportsionaalseid ja hoiatavaid karistusi, mille hulka kuuluvad kriminaalõiguslikud ja muud trahvid ning võivad kuuluda muud karistused, näiteks:

a) riiklike hüvitiste või abi saamise õigusest ilmajätmine,

b) ajutine või alaline äritegevuse keeld,

c) kohtuliku järelevalve alla võtmine, või

d) sundlõpetamine.

2. Iga liikmesriik võtab vajalikke meetmeid tagamaks, et artikli 8 lõike 2 kohaselt vastutusele võetud juriidilise isiku suhtes saab kohaldada tõhusaid, proportsionaalseid ja hoiatavaid karistusi või meetmeid.

Artikkel 10

Jurisdiktsioon

1. Iga liikmesriik kehtestab oma jurisdiktsiooni artiklites 2, 3, 4 ja 5 nimetatud süütegude suhtes, kui süütegu on pandud toime:

a) täielikult või osaliselt selle liikmesriigi territooriumil, või

b) selle liikmesriigi kodaniku poolt või

c) juriidilise isiku huvides, mille peakontor asub kõnealuse liikmesriigi territooriumil.

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

a) õigusrikkuja viibib süüteo toimepanemise ajal füüsiliselt antud riigi territooriumil, olenemata sellest, kas süütegu on suunatud kõnealuse riigi territooriumil asuva infosüsteemi vastu või mitte, või

b) süütegu on suunatud antud riigi territooriumil asuva infosüsteemi vastu, olenemata sellest, kas õigusrikkuja viibib süüteo toimepanemise ajal füüsiliselt kõnealuse riigi territooriumil või mitte.

3. Liikmesriik, kes vastavalt siseriiklikele õigusaktidele oma kodanikke veel üle või välja ei anna, võtab vajalikud meetmed, et kehtestada oma jurisdiktsioon artiklites 2, 3, 4 ja 5 nimetatud süütegude üle ja vajaduse korral esitada süüdistus, kui selle liikmesriigi kodanik on süüteo toime pannud väljaspool kõnealuse riigi territooriumi.

4. Kui süütegu kuulub mitme liikmesriigi jurisdiktsiooni alla ja kui mis tahes asjaomane riik saab samade faktide alusel esitada nõuetekohase süüdistuse, teevad kõnealused liikmesriigid koostööd otsustamaks milline riik õigusrikkujate vastu süüdistuse esitab, et koondada menetlus võimaluse korral ühte liikmesriiki. Selleks võivad liikmesriigid kasutada Euroopa Liidus loodud mis tahes organit või mehhanismi, et hõlbustada õigusasutuste koostööd ja nende tegevuse koordineerimist. Arvesse võetakse järgmisi tegureid allpool esitatud järjekorras:

— tegemist peab olema selle liikmesriigiga, mille territooriumil süüteod vastavalt lõike 1 punktile a ja lõikele 2 toime pandi,

— tegemist peab olema selle liikmesriigiga, mille kodanik teo täideviija on,

— tegemist peab olema selle liikmesriigiga, mille territooriumil teo täideviija leiti.

5. Liikmesriik võib otsustada mitte kohaldada või kohaldada üksnes erijuhtudel või -asjaoludel lõike 1 punktides b ja c sätestatud jurisdiktsiooni käsitlevaid norme.

6. Kui liikmesriigid otsustavad kohaldada lõiget 5, teatavad nad sellest nõukogu peasekretariaadile ja komisjonile ning viitavad vajaduse korral erijuhtudele või -asjaoludele, mille suhtes otsust kohaldatakse.

Artikkel 11

Teabevahetus

1. Artiklites 2, 3, 4 ja 5 nimetatud süütegudega seotud teabe vahetamisel tagavad liikmesriigid kooskõlas andmekaitse eeskirjadega, et nad kasutavad operatiivsete kontaktpunktide olemasolevat võrgustikku, mis on nende käsutuses ööpäevaringselt seitse päeva nädalas.

2. Iga liikmesriik teatab nõukogu peasekretariaadile ja komisjonile oma määratud kontaktpunkti, et vahetada infosüsteemide vastu suunatud rünnetega seotud süütegude alast teavet. Peasekretariaat edastab selle teabe teistele liikmesriikidele.

Artikkel 12

Rakendamine

1. Liikmesriigid võtavad käesoleva raamotsuse sätete järgimiseks vajalikud meetmed hiljemalt 16. märtsiks 2007.

2. Liikmesriigid edastavad hiljemalt 16. märtsiks 2007 nõukogu peasekretariaadile ja komisjonile nende sätete teksti, millega võetakse siseriiklikku õigusse üle käesolevast raamotsusest tulenevad kohustused. Hiljemalt 16. septembriks 2007 hindab nõukogu selle teabe põhjal koostatud aruande ja komisjoni kirjaliku aruande alusel, mil määral liikmesriigid on järginud käesoleva raamotsuse sätteid.

Artikkel 13

Jõustumine

Käesolev raamotsus jõustub *Euroopa Liidu Teatajas* avaldamise päeval.

Brüssel, 24. veebruar 2005

Nõukogu nimel
eesistuja
N. SCHMIT