



EUROOPAN YHTEISÖJEN KOMISSIO

Bryssel 22.01.2004
KOM(2004) 28 lopullinen

**KOMISSION TIEDONANTO
EUROOPAN PARLAMENTILLE, NEUVOSTOLLE, EUROOPAN TALOUS- JA
SOSIAALIKOMITEALLE JA ALUEIDEN KOMITEALLE**

ei-toivotusta kaupallisesta viestinnästä eli roskapostista ("spam")

SISÄLLYSLUETTELO

Tiivistelmä.....	4
Tausta ja tarkoitus.....	5
1. Roskapostin ongelma	6
1.1. Ongelman laajuus	6
1.2. Miksi roskaposti on ongelma?.....	7
2. Ei-toivottua kaupallista viestintää koskevat säännöt lyhyesti	9
2.1. Suostumukseen perustuva järjestelmä.....	9
2.2. Lainvalvonta.....	10
2.3. Muut roskapostiin sovellettavat säännöt	11
3. Tehokas täytäntöönpano ja lainvalvonta jäsenvaltioiden ja viranomaisten toimesta	12
3.1. Johdanto	13
3.2. Oikeuskeinot ja seuraamukset	15
3.2.1. Tämänhetkinen tilanne	15
3.2.2. Ehdotetut toimet	15
3.3. Valituskeinot	16
3.3.1. Tämänhetkinen tilanne	16
3.3.2. Ehdotetut toimet	17
3.4. Rajatylittävät valitukset ja lainvalvontayhteistyö EU:ssa	17
3.4.1. Tämänhetkinen tilanne	17
3.4.2. Ehdotetut toimet	18
3.5. Yhteistyö EU:n ulkopuolisten maiden kanssa.....	19
3.5.1. Tämänhetkinen tilanne	19
3.5.2. Ehdotetut toimet	19
3.6. Seuranta.....	20
3.6.1. Tämänhetkinen tilanne	20
3.6.2. Ehdotetut toimet	21
4. Yritysten tekniset toimenpiteet ja itsesääntely	21
4.1. Suostumukseen perustuvan järjestelmän soveltaminen	21

4.1.1.	Tämänhetkinen tilanne	21
4.1.2.	Ehdotetut toimet	22
4.2.	Vaihtoehtoiset riidanratkaisumenetelmät	23
4.2.1.	Tämänhetkinen tilanne	23
4.2.2.	Ehdotetut toimet	24
4.3.	Tekniset kysymykset	24
4.3.1.	Tämänhetkinen tilanne	24
4.3.2.	Ehdotetut toimet	25
5.	Tiedotustoimet	26
5.1.	Tämänhetkinen tilanne	26
5.2.	Ehdotetut toimet	28
	Päätelmät	29
	Taulukko: Yhteenveto tiedonannossa esitetyistä toimista	30

**KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE,
NEUVOSTOLLE, EUROOPAN TALOUS- JA SOSIAALIKOMITEALLE JA
ALUEIDEN KOMITEALLE**

ei-toivotusta kaupallisesta viestinnästä eli roskapostista ("spam")

(ETA:n kannalta merkityksellinen teksti)

TIIVISTELMÄ

Ei-toivottu kaupallinen sähköpostiviestintä, jota yleensä kutsutaan roskapostiksi ("spam"), on saavuttanut huolestuttavat mittasuhteet. Jo yli 50 prosenttia maailman sähköpostiliikenteestä arvioidaan olevan roskapostia. Vielä huolestuttavampaa on kasvuvauhti: vuonna 2001 osuus oli vielä "vain" 7 prosenttia.

Roskaposti on ongelma monestakin syystä, joita ovat yksityisyyden suojeleminen, kuluttajien harhaanjohtaminen, alaikäisten ja ihmisarvon suojeleminen, yrityksille aiheutuvat ylimääräiset kustannukset ja tuottavuuden menetys. Yleisemmin ottaen roskaposti vie pohjaa kuluttajaluottamukselta, joka on edellytys sähköisen kaupankäynnin, verkkopalvelujen ja koko tietoyhteiskunnan menestykselle.

EU varautui tähän vaaraan antamalla heinäkuussa 2002 sähköisen viestinnän tietosuojadirektiivin 2002/58/EY, jolla otettiin EU:n laajuudessa käyttöön suostumukseen perustuvan markkinoinnin periaate ("opt-in") sähköpostiviestinnässä (myös teksti- ja multimediaviesteissä) ja lisätoimenpiteitä kuluttajien suojaamiseksi. Sähköisen viestinnän tietosuojadirektiivi oli pantava täytäntöön viimeistään 31. lokakuuta 2003. Rikkomismenettelyjä on käynnistetty niitä jäsenvaltioita vastaan, jotka eivät ole ilmoittaneet komissiolle toimenpiteistä direktiivin saattamiseksi osaksi kansallista lainsäädäntöä.

Tarvittavan lainsäädännön antaminen on ensimmäinen ja välttämätön askel, mutta se on vasta osaratkaisu. Tässä tiedonannossa yksilöidään toimia, joita tarvitaan EU:n sääntöjen täydentämiseksi, jotta "roskapostikielto" voidaan käytännössä toteuttaa.

Roskapostia varten ei kuitenkaan ole patenttiratkaisua. Tässä tiedonannossa kuvatut toimet keskittyvät tehokkaaseen lainvalvontaan, josta vastaavat jäsenvaltiot ja viranomaiset, sekä itsesääntelyratkaisuihin yrityksissä ja kuluttajavalistukseen. Myös kansainväliseen ulottuvuuteen kiinnitetään huomiota, koska suuri osa roskapostista tulee Euroopan unionin ulkopuolelta.

Toimet pohjautuvat vuoden 2003 aikana muotoutuneeseen yhteisymmärrykseen, joka vahvistettiin lokakuussa 2003 järjestetyssä julkisessa työryhmätapaamisessa. Käytännön toteutuksesta on niin ikään päästävä yhteisymmärrykseen. Roskapostin leviämistä voidaan torjua vain, jos kaikki tahot jäsenvaltioista ja viranomaisista aina yrityksiin, kuluttajiin ja Internetin ja sähköisen viestinnän käyttäjiin osallistuvat toimintaan.

Joillakin näistä toimista on selkeä hintansa. Mutta tämä hinta on maksettava, jos sähköposti ja verkkopalvelut halutaan pitää toimivana viestintävälineenä. Tässä

tiedonannossa kuvatuilla toimilla voidaan vähentää tuntuvasti roskapostin määrää tietoyhteiskunnan, Euroopan kansalaisten ja Euroopan talouksien hyväksi.

Tausta ja tarkoitus

Ei-toivottu kaupallinen sähköpostiviestintää¹ eli roskapostia ("spam") pidetään laajalti yhtenä Internetin tämän hetken pahimmista ongelmista. Se on saavuttanut huolestuttavat mittasuhteet. On jo olemassa vaara, että sähköpostin tai tekstiviestien käyttäjät yksinkertaisesti lakkaavat käyttämästä sähköpostia tai matkaviestintäpalveluja tai vähentävät niiden käyttöä tavallisesta. Yleisemmin voidaan todeta, että koska Internetin ja muun sähköisen viestinnän (kuten laajakaista-, matka- ja langattoman viestinnän) katsotaan olevan avainasemassa modernin talouden tuottavuuden kasvun kannalta, roskapostiin liittyvä ongelma vaatii erityistä huomiota.

Yksimielisyys vallitsee siitä, että on ryhdyttävä toimiin ennen kuin roskapostin leviäminen tekee tyhjäksi sähköpostin ja muiden verkkopalvelujen yrityksille ja kansalaisille tuomat edut. Ei ole kuitenkaan itsestään selvää, miten roskapostia olisi parasta torjua. Mitään patenttiratkaisua ei ole. Roskapostin ongelmaan voidaan puuttua tehokkaasti vain, jos kaikki tahot jäsenvaltioista ja viranomaisista aina yrityksiin, kuluttajiin ja Internetin ja sähköisen viestinnän käyttäjiin osallistuvat tahollaan toimintaan.

Tässä tiedonannossa esitellään erilaisia oikeudellisia, teknisiä ja tietoisuuden lisäämiseen tähtääviä toimia direktiivin 2002/58/EY pohjalta. Direktiivillä otettiin käyttöön suostumukseen perustuva järjestelmä, joka tuli 31. lokakuuta 2003 pakolliseksi kaupallisessa viestinnässä jäsenmaissa².

Toimet keskittyvät direktiivin tehokkaaseen täytäntöönpanoon ja toimeenpanon valvontaan jäsenvaltioissa, teknisiin toimenpiteisiin, yritysten itsesääntelyyn, kuluttajavalistukseen ja kansainväliseen yhteistyöhön. Kansainvälinen ulottuvuus on toiminnassa keskeistä, koska suuri osa roskapostista näyttää tulevan Euroopan unionin ulkopuolelta, erityisesti Pohjois-Amerikasta³.

Toimet pohjautuvat vuoden 2003 aikana syntyneeseen yhteisymmärrykseen, joka vahvistettiin lokakuussa 2003 järjestetyssä julkisessa työryhmätapaamisessa⁴. Yhteisymmärrys tässä asiassa on sitäkin tärkeämpää, koska juuri sidosryhmien tehtävänä

¹ Tämä tiedonanto ei koske muulla tavoin kuin sähköisesti toimitettua ei-toivottua viestintää, esim. ei-toivottua kannettua postia.

² Ks. erityisesti sähköisen viestinnän tietosuojadirektiivin 2002/58/EY 13 artikla (ja tämän tiedonannon luku 2).

³ Esimerkiksi Ranskan tietosuojaviranomaisen CNIL:n ja Belgian tietosuojalautakunnan CPVP:n vuonna 2002 järjestämien roskapostilaatikkoaloitteiden tulosten perusteella pääteltiin, että roskaposti tulee ensisijaisesti Yhdysvalloista ja vähemmässä määrin Kanadasta. CPVP:n raportti: http://www.privacy.fgov.be/publications/spam_4-7-03_fr.pdf; CNIL:n raportti: http://www.cnil.fr/thematic/docs/internet/boite_a_spam.pdf. Ks. myös UNCTAD, E-Commerce and Development Report 2003, New York ja Geneve, 2003, s. 27.

⁴ Työryhmätapaamisen osallistujille toimitettiin etukäteen roskapostia käsitellyt keskusteluasiakirja, joka pohjautui aiempiin, viestintäkomiteassa (COCOM) ja direktiivin 95/46/EY 29 artiklalla perustetussa tietosuojatyöryhmässä käytyihin keskusteluihin. Viestintäkomitean ja tietosuojatyöryhmän jäsenet antoivat tietoja kyselylomakkeella. Myös monet toimialajärjestöt ja yksittäiset yritykset vastasivat kyselyyn. Näiden joukossa oli Internet-palveluntarjoajia ja (kiinteiden ja matkaviestinverkkojen) operaattoreita, suoramarkkinoijia ja mainostoimistoja sekä tietokone- ja ohjelmistoyrityksiä.

on, mahdollisuuksien mukaan komission tuella, toteuttaa tässä tiedonannossa esitetyt toimet tietoyhteiskunnan, sen yritysten ja käyttäjien hyväksi.

Asiakirjan rakenne

Tässä tiedonannossa eritellään roskapostiongelmaan liittyviä eri näkökohtia ja ehdotetaan erityisiä toimia, joilla kuhunkin ongelmaan voidaan puuttua. Siinä myös esitellään eräitä hyödylliseksi havaittuja parhaita käytäntöjä.

Toimenpide-ehdotukset esitetään seuraavan jäsenyyksen mukaisesti:

- **Täytäntöönpano- ja lainvalvontatoimet** erityisesti hallituksille ja viranomaisille, muun muassa oikeuskeinot ja seuraamukset, valitusmenettelyt, rajat ylittävät kuluttajavalitukset, yhteistyö EU:n ulkopuolisten maiden kanssa ja seuranta (luku 3).
- **Itsesääntely- ja tekniset toimenpiteet** erityisesti yrityksille, muun muassa sopimusjärjestelyt, käytäntösäännöt, hyväksyttävät markkinointikäytännöt, merkinnät, vaihtoehtoiset riidanratkaisumenetelmät ja tekniset ratkaisut (esim. suodatus, tietoturva) (luku 4).
- **Tiedotustoimet** hallituksille ja viranomaisille, yrityksille, kuluttajajärjestöille ja vastaaville, muun muassa ennaltaehkäisy, kuluttajavalistus ja raportointijärjestelmät (luku 5).

Tämän tiedonannon lopussa olevassa taulukossa esitetään yhteenveto näistä toimista. Toimet liittyvät toisiinsa monin tavoin. Ne pitäisi mahdollisuuksien mukaan toteuttaa rinnakkain ja kokonaisvaltaisella tavalla.

Ennen toimenpiteiden esittelyä seuraavissa kappaleissa tarkastellaan roskapostia ilmiönä (luku 1) ja palautetaan mieleen uudet, 31. lokakuuta 2003 lähtien voimassa olleet säännöt (luku 2).

1. ROSKAPOSTIN ONGELMA

Mitä roskaposti on?

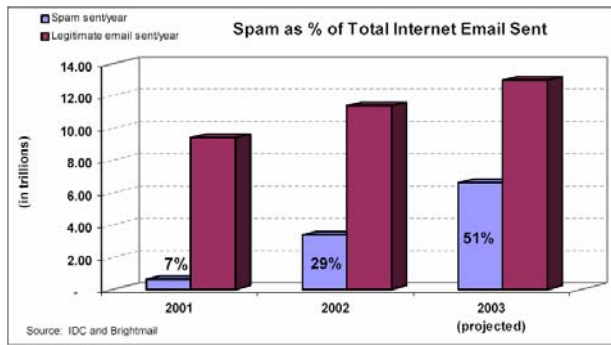
Roskaposti eli ”spam” on usein käytetty mutta harvoin määritelty termi. Tavallisesti sillä tarkoitetaan ei-toivottua, usein massapostituksina lähetettyjä sähköpostiviestejä. Uudessa direktiivissä ei määritellä eikä käytetä kyseistä termiä. Siinä käytetään käsitettä ”ei-toivottu sähköpostiviestintä”, jota harjoitetaan ”suoramarkkinointitarkoituksiin”. Tämä kattaa useimmat roskapostin lajit. Käsitteellä ”roskaposti” viitataan tässä tiedonannossa ei-toivotuun kaupalliseen sähköpostiviestintään.

Huomattakoon, että ”sähköpostiviestintä” itsessään kattaa perinteisten SMTP-sähköpostiviestien lisäksi myös teksti- ja multimediamiestit ja kaiken muun sähköisen viestinnän, joka ei edellytä lähettäjän ja vastaanottajan samanaikaista osallistumista (ks. luku 2 jäljempänä).

1.1. Ongelman laajuus

Ei-toivottu kaupallinen sähköposti eli roskaposti on saavuttavut huolestuttavat mittasuhteet. Tilastot vaihtelevat, mutta yleisenä arviona on, että yli 50 prosenttia koko maailman sähköpostiliikenteestä on roskapostia.

Vielä huolestuttavampaa on kasvuvauhti. Vielä vuonna 2001 arvioitiin, että roskapostin osuus on ”vain” 7 prosenttia maailman sähköpostiliikenteestä. Vuonna 2002 osuuden arvioitiin olevan 29 prosenttia, ja vuotta 2003 koskeva arvio on 51 prosenttia.



Kaavio 1: Roskapostin osuus kaikesta Internet-sähköpostiliikenteestä

Eri käyttäjäryhmien ja eri alueiden välillä voi olla huomattavia eroja. (Esim. Euroopan komissiossa arviolta 30 prosenttia ulkoa tulevasta sähköpostista on roskapostia.) Yleisesti ottaen EU:n luvut ovat kuitenkin yhtä huolestuttavia kuin koko maailman luvut⁵.

Matkaviestintäverkkojen ei-toivottu viestintä tai roskaposti, esim. lyhytsanomapalveluina eli tekstiviesteinä, ei tällä hetkellä näytä olevan vastaavanlaajuinen ongelma, mutta näiden verkkojen kehitys, kuten sähköpostin yleistymisen niissä, voi johtaa roskapostin määrän kasvuun. Maissa, joissa I-mode-palvelut ovat laajassa käytössä, (esim. Japanissa) kokemukset vahvistavat tämän uhan olevan olemassa.

1.2. Miksi roskaposti on ongelma?

Yksittäisten käyttäjien näkökulmasta roskaposti on yksityisyyden loukkaus. Tämä huoli oli lähtökohtana seuraavassa jluvussa kuvatuille ei-toivottua viestintää koskeville uusille säännöille. Lisäksi roskaposti on usein harhaanjohtavaa tai vilpillistä. Suuri osa roskapostista näyttää olevan viestintää, jonka taustalla on halu pettaa kuluttajia harhaanjohtavalla tai vilpillisellä mainonnalla⁶. Valitettavan usein kuluttajat vastaavat tällaisiin harhaanjohtaviin tai vilpillisiin viesteihin⁷. Myös pornografiset viestit voivat olla häiritseviä⁸. Käyttäjälle postilaatikkojen siivoaminen roskapostista merkitsee

Suhtaudutaanko ongelmaan vakavasti?

Valitusten määrä on yksi osoitin käyttäjien ilmaisemista huolista. Ranskan tietosuojaviranomaisen roskapostilaatikkoon toimitettiin kolmessa kuukaudessa 325 000 viestiä. Belgian vastaava aloite tuotti 50 000 valitusta kahdessa ja puolessa kuukaudessa. FTC:n jatkuvasti ylläpitämään roskapostilaatikkoon (UCE Database) toimitettiin vuoden 2003 alkupuolella 130 000 viestiä päivässä¹.

⁵ Syyskuussa 2003 arviolta 49 prosenttia EU:n sähköpostiviestinnästä oli roskapostia, koko maailmassa noin 54 prosenttia (Lähde: Brightmail, 2003).

⁶ Yhdysvaltain kauppakomission FTC:n hiljattain ilmestyneen raportin mukaan 22 prosenttia tutkitusta roskapostista sisälsi väärää tietoa viestin aihekentässä, 42 prosentissa viesteistä oli harhaanjohtava aihekentä, jonka mukaan lähettäjällä oli liike- tai henkilökohtainen suhde vastaanottajaan, 44 prosenttia sisälsi väärää tietoa viestin lähettäjä- tai aihekentässä, yli puolet rahaan liittyvästä roskapostista sisälsi väärää tietoa lähettäjä- tai aihekentässä, 40 prosenttia kaikesta roskapostista sisälsi vilpillisiin tarkoituksiin viittaavia merkkejä itse viestissä, 90 prosenttia viesteissä kuvatuista sijoitus- ja liiketoimintamahdollisuuksista sisälsi todennäköisesti perättömiä väitteitä ja 66 prosenttia roskapostista sisälsi väärää tietoa lähettäjäkentässä, aihekentässä tai viestin tekstissä. (*False Claims in Spam*, FTC:n markkinointikäytännöyksikön raportti, 30. huhtikuuta 2003 <http://www.ftc.gov/reports/spam/030429spamreport.pdf>).

⁷ Pew Internetin mukaan 7 prosenttia sähköpostin käyttäjistä ilmoittaa tilanneensa jotain roskapostiviestin perusteella ja 33 prosenttia sähköpostin käyttäjistä ilmoittaa avanneensa roskapostiviestissä olleen linkin saadakseen lisätietoa. Vaikka huijatuksi joutuvien kuluttajien

ajanmenetystä sekä lisäkuluja tarvittavien suodatus- ja muiden ohjelmistojen hankinnan vuoksi.

Roskaposti aiheuttaa nykyisellään huomattavia kustannuksia myös yrityksille. Välittömiä kustannuksia aiheutuu, kun työntekijät joutuvat siivoamaan roskapostin sähköpostilaatikoistaan. Tämä vähentää tehokkuutta/tuottavuutta työssä. Tietotekniikkaosastot käyttävät aikaa ja rahaa ongelman ratkaisemiseen. Internet- ja sähköpostipalvelun tarjoajien on hankittava lisää siirto- ja tallennuskapasiteettia välittääkseen sähköpostiviestejä, joita asiakas ei edes halua. On myös olemassa vaara, että roskaposti saattaa vastuuseen tahon, joka ottaa sen vastaan (esim. haitallinen sisältö työntekijän PC:llä), tai joka yksinkertaisesti ja pahaa aavistamatta lähettää sen eteenpäin (esim. aiheeton mustalle listalle joutuminen, maineelle aiheutuvat vahingot). Myös välillisiä kustannuksia aiheutuu: jotkut oikeutetut kaupalliset viestit eivät pääse perille roskapostisuodatuksen vuoksi (ns. väärät osumat) tai niitä ei yksinkertaisesti enää lueta, kun ne mielletään roskapostiksi. Roskapostia käytetään yhä enemmän keinona levittää viruksia, jotka voivat koitua kalliiksi yrityksille.

Roskapostin kustannusten määrittäminen on vaikeaa erityisesti yksityishenkilöille, ei vähiten siksi, että aiheutunutta haittaa on osin vaikea mitata rahassa. Arviot ovat kuitenkin yleisesti ottaen huolestuttavia. Esimerkiksi Ferris Research on arvioinut, että vuonna 2002 roskaposti aiheutti Euroopan yrityksille 2,5 miljardin euron kustannukset pelkästään menetetyn tuottavuuden vuoksi⁹. Asiaa pahentaa se edellä mainittu seikka, että roskapostin määrä on kasvanut tuntuvasti vuoden 2002 jälkeen. Ohjelmistotoimittaja MessageLabs Ltd:n kesäkuussa 2003 tekemän arvion mukaan roskaposti aiheuttaa Britannian yrityksille noin 3,2 miljardin punnan kustannukset¹⁰. Roskapostin vaikutus voi vaihdella toimialasta riippuen. Roskapostilla voi olla erityinen vaikutus esimerkiksi lakialaan sen käsittelemän luottamuksellisen ja arkaluonteisen tiedon vuoksi.

Yksi roskapostin huolestuttavimmista seurauksista on se, että se vie pohjaa kuluttajaluottamukselta, joka on edellytys sähköisen kaupankäynnin ja koko tietoyhteiskunnan menestykselle. Sellainen kuluttajien mielle, että jollakin vähittäiskaupan kanavalla toimii huijareita, voi vaikuttaa merkittävästi samaa kanavaa käyttävien rehellisten liikkeenharjoittajien maineeseen. Tuoreet luvut Yhdysvalloista, jolla on EU:ta laajempaa kokemusta roskapostista, vahvistavat sen päätelmän, että monet ihmiset luottavat sähköpostiin vähemmän saadessaan paljon roskapostia¹¹.

osuus on suhteellisen pieni, harhaanjohtavaa tai vilpillistä roskapostia hyödyntävien huijareiden saavuttamat ilmiömäiset mittakaavaedut ovat vieneet kuluttajille suunnatun roskapostin ongelman kokonaan uudelle tasolle. Ks. Deborah Fallows, Spam—How It Is Hurting Email and Degrading Life on the Internet, October 2003, raportin tilaaja Pew Internet & American Life Project, saatavilla osoitteessa http://www.pewinternet.org/reports/pdfs/PIP_Spam_Report.pdf. Huhti-toukokuussa 2003 järjestetyssä FTC Spam Forum –tapahtumassa kuultu roskapostin lähettäjä ilmoitti toiminnan tuovan voittoa, vaikka vastaamisaste olisi alle 0,0001%. (Timothy J. Muris, puheenjohtaja, Federal Trade Commission, Aspen Summit, Cyberspace and the American Dream, The Progress and Freedom Foundation, 19. elokuuta 2003, Aspen, Colorado).

⁸ Roskapostiviestit sisältävät joskus aiheetonta väkivaltaa tai yllyttävät vihaan rodun, sukupuolen, uskonnon tai kansallisuuden perusteella.

⁹ Lähde: Ferris Research, 2003.

¹⁰ Kyseinen luku ja muita arvioita sisältyy selvitykseen *“Spam”; Report of an Inquiry by the All Party Internet Group*, Lontoo, lokakuu 2003, s. 8. Saatavilla osoitteessa <http://www.apig.org.uk>.

¹¹ Edellä mainitun Pew Internetin hiljattaisen selvityksen mukaan 25 prosenttia haastatelluista käytti sähköpostia vähemmän, koska he saivat niin paljon roskapostia.

Yleisemmin Internetin ja muun sähköisen viestinnän – laajakaistaviestinnän, langattoman viestinnän – odotetaan olevan avainasemassa modernin talouden tuottavuuden kasvun kannalta. Tiettyt tällaisten palvelujen houkuttelevat ominaisuudet – ”aina auki” oleva yhteys, langattomuus – ovat kuitenkin seikkoja, jotka voivat lisätä merkittävästi vastaanotetun tai eteenpäin lähetetyn roskapostin määrää, jos käytössä ei ole asianmukaisia turvakeinoja. Kyseisten palvelujen leviäminen voikin ikävä kyllä johtaa roskapostin määrän kasvuun, jos tehokkaita turvakeinoja ei oteta käyttöön pikaisesti.

2. EI-TOIVOTTUA KAUPALLISTA VIESTINTÄÄ KOSKEVAT SÄÄNNÖT LYHYESTI

2.1. Suostumukseen perustuva järjestelmä

Sähköisen viestinnän tietosuojadirektiivissä 2002/58/EY (joka oli saatettava osaksi jäsenvaltioiden lainsäädäntöä viimeistään 31. lokakuuta 2003) edellytetään, että jäsenvaltiot kieltävät ei-toivottujen kaupallisten sähköpostiviestien lähettämisen (kattaa kaikki sähköiset viestinvälitysjärjestelmät, kuten tekstiviestit ja multimediaviestit), ellei näiden sähköisten palvelujen tilaaja ole antanut suostumustaan ennalta (direktiivin 13 artiklan 1 kohta)¹². Kyseessä on niin sanottu *opt in* -järjestelmä, jota on tähän mennessä jo sovellettu fakseihin ja automaattisiin soittojärjestelmiin¹³.

Uuden järjestelmän kolme perussääntöä:

Sääntö nro 1: Sähköpostimarkkinoinnille on saatava ennalta tilaajan suostumus. Poikkeuksena ovat sähköpostiviestit (tai tekstiviestit), jotka sama yritys lähettää vanhoille asiakkailleen mainostaen omia vastaavia palvelujaan tai tuotteitaan. Tätä sääntöä sovelletaan tilaajiin, jotka ovat luonnollisia henkilöitä, mutta jäsenvaltiot voivat halutessaan laajentaa sen koskemaan myös oikeushenkilöitä.

Sääntö nro 2: On kiellettyä peittää tai salata sen lähettäjän henkilöllisyys, jonka puolesta viesti on lähetetty.

Sääntö nro 3: Kaikissa viesteissä on oltava voimassa oleva osoite, johon vastaanottaja voi lähettää pyynnön siitä, että kyseinen viestintä lopetetaan (”opt-out”).

Kaikki ei-toivotut sähköpostiviestit eivät ole kiellettyjä. Säännöstä nro 1 poiketaan tapauksissa, joissa yhteystiedot sähköpostin tai tekstiviestien lähettämiseksi on saatu tuotteen tai palvelun myynnin yhteydessä. Tästä käytetään joskus nimitystä ”soft opt-in”. Tällaisessa jo olemassa olevassa asiakassuhteessa yritys, joka on saanut tiedot asiakkailtaan, saa käyttää niitä sellaisten tuotteiden tai palvelujen markkinoinnissa, jotka vastaavat asiakkaalle jo myytyjä. Poikkeus on yhdenmukaistettu yhteisötasolla, ja jäsenvaltioilla on velvollisuus soveltaa sitä. Sitä on kuitenkin sovellettava tiukasti ja rajatusti, jottei se horjuttaisi suostumukseen perustuvaa järjestelmää. Yrityksen on joka tapauksessa tehtävä asiakkaalle selväksi heti, kun yhteystiedot kerätään ensimmäisen kerran, että niitä voidaan käyttää suoramarkkinointiin (ja tarvittaessa ilmoitettava, että ne voidaan antaa tätä tarkoitusta varten kolmannelle osapuolelle), ja annettava asiakkaalle oikeus kieltää tietojensa käyttö ”maksutta ja helposti”. Lisäksi kussakin markkinointiviestissä asiakkaalle on annettava helppo mahdollisuus lopettaa mainonta maksutta (kieltoon perustuva järjestelmä, ”opt-out”).

¹² Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi) EYVL L 201, 31.7.2002.

¹³ Suoramarkkinointipuhelujen (muiden kuin automaattisten järjestelmien) osalta jäsenvaltiot voivat valita joko suostumukseen tai kieltoon perustuvan järjestelmän.

Suostumukseen perustuva järjestelmä on pakollinen kaikessa suoramarkkinointiin käytettävässä yksityishenkilöille (luonnollisille henkilöille) suunnatussa sähköposti- ja testiviestinnässä. Jäsenvaltiot voivat laajentaa suostumukseen perustuvan järjestelmän koskemaan myös yrityksille (oikeushenkilöille) suunnattua viestintää. Jäsenvaltiot, jotka ovat valinneet yritysten välistä markkinointia varten kieltoon perustuvan järjestelmän (kieltolistoineen), voivat jatkaa kyseisen järjestelmän soveltamista. Erilaisten järjestelmien käyttö sähköpostipalvelun tilaajakategorian mukaan voi olla hankalaa lähettäville, kun oikeushenkilöt on eroteltava luonnollisista henkilöistä.

Kaikissa kategorioissa, olivatpa kyseessä oikeus- tai luonnolliset henkilöt, direktiivi kieltää sellaiset suoramarkkinointiviestit, joissa peitetään tai salataan lähettäjän henkilöllisyys. Lisäksi kaikissa viesteissä on oltava voimassa oleva osoite, johon vastaanottaja voi lähettää pyynnön siitä, että kyseinen viestintä lopetetaan¹⁴.

Direktiivin 95/46/EY 29 artiklalla perustettu tietosuojatyöryhmä, jossa kokoontuvat EU:n tietosuojaviranomaiset ja jonka tehtävänä on neuvoa komissiota, tarkastelee parhaillaan lähemmin joitakin näistä ratkaisuksista. Työryhmä pyrkii tässä työssä edistämään direktiivin 2002/58/EY kansallisten täytäntöönpanosäännösten yhdenmukaista soveltamista¹⁵. Jos näistä seikoista päästään yhteisymmärrykseen, vältetään tulkintaerot, jotka voisivat haitata sisämarkkinoiden toimintaa. Ei-toivotun viestinnän muita näkökohtia käsitellään työryhmän aiemmissa asiakirjoissa¹⁶.

2.2. Lainvalvonta

”Yleisen” tietosuojadirektiivin säännöksiä oikeuskeinoista, vastuista ja sanktioista sovelletaan myös sähköisen viestinnän tietosuojadirektiivissa tarkoitetuissa yhteyksissä, siis myös ei-toivottuun viestintään¹⁷.

¹⁴ Direktiivin 2002/58/EY 13 artiklan 4 kohta.

¹⁵ Direktiivin 2002/58/EY 15 artiklan 3 kohdan ja direktiivin 95/46/EY 30 artiklan mukaisesti.

¹⁶ Ks. esim. 12. heinäkuuta 2000 annettu lausunto 7/2000 Euroopan komission ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla sekä suositus 2/2001 Euroopan unionissa verkossa tapahtuvaan henkilötietojen keruuseen sovellettavista tietyistä vähimmäisvaatimuksista. Tietojen keruuta tarkastellaan 21. marraskuuta 2000 annetussa työasiakirjassa ”Tietosuoja Internetissä - Euroopan unionin yhdenmennyksen lähestymistapa”. Nämä asiakirjat ovat saatavilla seuraavassa osoitteessa:

http://europa.eu.int/comm/internal_market/privacy/workinggroup_en.htm.

¹⁷ Direktiivin 2002/58/EY 15 artiklassa viitataan direktiivin 95/46/EY III lukuun ”Oikeuskeinot, vastuut ja sanktiot”:

22 artikla – Oikeuskeinot

Jäsenvaltioiden on säädettävä siitä, että kenellä tahansa henkilöllä on mahdollisuus käyttää oikeussuojakeinoja, jos kyseessä olevaan käsittelyyn sovellettavien kansallisten säännösten mukaisesti hänelle kuuluvia oikeuksia loukataan, sanotun kuitenkin rajoittamatta sellaisen hallinnollisen keinon soveltamista, johon voidaan turvautua, muun muassa 28 artiklassa tarkoitettua valvontaviranomaisen avulla ennen asian vireillepanoa oikeudessa.

23 – Vastuu

1. Jäsenvaltioiden on säädettävä siitä, että jos kenelle tahansa henkilölle aiheutuu vahinkoa laittomasta käsittelystä tai minkä tahansa toiminnan yhteensopimattomuudesta tämän direktiivin mukaisesti toteutettujen kansallisten toimenpiteiden kanssa, hänellä on oikeus saada rekisterinpitäjältä korvaus aiheutuneesta vahingosta

2. Rekisterinpitäjä voidaan vapauttaa tästä vastuusta osittain tai kokonaan, jos hän osoittaa, ettei hän ole vastuussa vahingon aiheuttaneesta tapahtumasta

24 artikla – Sanktiot

Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet tämän direktiivin säännösten täydellisen

Jäsenvaltioiden on siis varmistettava, että käytössä ovat oikeuskeinot ja seuraamukset siltä varalta, että säännöksiä rikotaan. Jokaisen henkilön on voitava turvautua oikeussuojakeinoon, jos jotain kansallisen lain takaamaa oikeutta rikotaan. Oikeuskeinon käyttö ei rajoita hallinnollisten menetelmien soveltamista (mahdollisesti ennen asian vireillepanoa oikeudessa), mutta tällaisten hallinnollisten keinojen soveltamisesta ei ole säädetty EU:n laajuudessa. Jokaisella henkilöllä on oltava oikeus korvauksiin vahingoista, jotka aiheutuvat laittomasta tietojen käsittelystä tai teosta. Säännösten rikkomistapauksissa on voitava soveltaa seuraamuksia, jotta varmistetaan direktiivin säännösten täysimääräinen täytäntöönpano.

Toisin sanoen: vaikka direktiivi on säädöstyyppeä, joka jättää jäsenvaltioille liikkumavaran kansallisten täytäntöönpanotoimenpiteiden – myös oikeuskeinojen ja seuraamusten – valinnassa, näillä toimenpiteillä on varmistettava ei-toivottua sähköpostimainontaa koskevien säännösten ”täysimääräinen täytäntöönpanotaminen”.

Kuten direktiivien tapauksessa yleensä, säännösten noudattamisen valvonta kuuluu ensisijaisesti jäsenvaltioille eikä komissiolle. Ei esimerkiksi ole komission tehtävä ajaa syytteitä tai määrätä sakkoja niille, jotka rikkovat direktiivissä vahvistettuja oikeuksia ja velvollisuuksia¹⁸.

2.3. Muut roskapostiin sovellettavat säännöt

Roskapostin lähettämiseen usein liittyvä käytäntö on sähköpostiosoitteiden haravointi eli henkilötietojen automaattinen keruu Internetin julkisista osista, kuten WWW:stä ja keskusteluryhmistä. Tällainen toiminta on laitonta ”yleisen” tietosuojadirektiivin 95/46/EY nojalla, tapahtuipa keruu automaattisesti ohjelmistojen avulla tai ei¹⁹.

Vilpillinen ja harhaanjohtava roskaposti voi olla erityisen häiritsevää. Tällaiset markkinointikeinot ovat jo nyt laittomia harhaanjohtavaa mainontaa ja sopimatonta markkinointia koskevien EU-sääntöjen nojalla (esim. harhaanjohtavaa mainontaa koskeva direktiivi 84/450/ETY)²⁰. Myös kansallinen laki määrää yleensä tiukempia (myös rikosoikeudellisia) seuraamuksia vakavammissa tapauksissa.

Tietyt roskapostin lajit voivat olla vielä epämiellyttävämpiä, kuten pornografinen tai tarpeetonta väkivaltaa sisältävä roskaposti, varsinkin jos se joutuu lasten ulottuville²¹. Joissain tapauksissa tällaisten viestien sisältö voi olla haitallista olematta sinänsä laitonta,

soveltamisen varmistamiseksi ja määriteltävä erityisesti sanktiot, joita sovelletaan tämän direktiivin mukaisesti säädettyjen säännösten rikkomistapauksissa.

¹⁸ Tämä poikkeaa esimerkiksi Yhdysvaltojen FTC:n käytännöstä.

¹⁹ Ks. myös direktiivin 95/46/EY 29 artiklalla perustetun tietosuojatyöryhmän työasiakirja ”Tietosuoja Internetissä - Euroopan unionin yhdenmätty lähestymistapa” (asiakirja WP 37, julkaistu 21. marraskuuta 2000).

²⁰ Neuvoston direktiivi 84/450/ETY, annettu 10 päivänä syyskuuta 1984, harhaanjohtavaa mainontaa koskevien jäsenvaltioiden lakien, asetusten ja hallinnollisten määräysten lähentämisestä, EYVL L 250, 19.9.1984, s. 17-20. Komissio on hiljattain antanut ehdotuksen harhaanjohtavaa mainontaa koskevan direktiivin korvaamiseksi ajantasaisemmalla säädöksellä (KOM(2003) 356 lopullinen).

²¹ Neuvosto antoi 24. syyskuuta 1998 suosituksen 98/560/EY Euroopan audiovisuaalisia ja tietopalveluja tuottavien yritysten kilpailukyvyyn parantamisesta edistämällä kansallisia järjestelmiä, joiden tarkoituksena on saattaa alaikäisten ja ihmisarvon suojele vertailukelpoiselle ja tehokkaalle tasolle. Suositus on ensimmäinen audiovisuaalisten ja tietopalvelujen sisältöä koskeva EU:n tason oikeudellinen väline, joka kattaa kaikki tiedonvälityskanavat radio- ja televisiotoiminnasta Internetiin.

mutta niiden valikoimaton lähettäminen sekä aikuisille että lapsille on yleensä vastoin kansallista lakia ja voi johtaa ankariinkin seuraamuksiin. Roskapostiviesteissä voi myös olla laitonta sisältöä, kuten yllytyksiä vihaan rodun, sukupuolen, uskonnon tai kansallisuuden perusteella. Kaikissa tapauksissa pätee se sääntö, että heti kun viesteillä on suoramarkkinointitarkoitus – kuten usein on asianlaita – ne joutuvat ”roskapostikiellon” piiriin kuten muukin ei-toivottu sähköpostiviestintä.

Tietoyhteiskunnan palveluja, erityisesti sähköistä kaupankäyntiä, sisämarkkinoilla koskevista tietyistä oikeudellisista näkökohdista annetussa direktiivissä 2000/31/EY (direktiivi sähköisestä kaupankäynnistä) asetetaan lisäksi se vaatimus, että ”kaupallinen viestintä” on oltava selvästi tunnistettavissa sellaiseksi (direktiivin 6 artiklan a alakohta)²².

Roskapostin lähettämisen yhteydessä harjoitetaan usein myös hakkerointia tai tunnistetietojen anastamista lähetyksien laatimiseksi tai osoitetietokantoihin tai tietokoneisiin murtautumiseksi. Tulossa oleva puitepäättös tietojärjestelmiin kohdistuvien hyökkäyksien torjunnasta kattaa monet tällaiset teot ja siinä säädetään rikosoikeudellisista seuraamuksista. Kyseisestä komission ehdotukseen perustuvasta puitepäätöksestä päästiin poliittiseen yhteisymmärrykseen helmikuussa 2003. Päätös on piakkoin määrä vahvistaa virallisesti²³. Jäsenvaltiot voivat jo nyt nostaa rikosoikeudellisen syytteen palvelimien tai henkilökohtaisten tietokoneiden luvattomasta käytöstä tai väärinkäytöstä.

3. TEHOKAS TÄYTÄNTÖÖNPANO JA LAINVALVONTA JÄSENVALTIOIDEN JA VIRANOMAISTEN TOIMESTA

Tässä luvussa tehokkaasta täytäntöönpanosta ja lainvalvonnasta tarkastellaan erityisesti toimia, joita ehdotetaan hallituksille ja viranomaisille. Näitä ovat oikeuskeinot ja seuraamukset, valitusmenettelyt, rajat ylittävät kuluttajavalitukset, yhteistyö EU:n ulkopuolisten maiden kanssa ja seuranta.

Komissio toteaa aivan aluksi, että osa jäsenvaltioista ei ole vielä siirtänyt kansalliseen lainsäädäntönsä sähköisen viestinnän tietosuojadirektiiviä, joka sisältää säännöksiä ei-toivotusta kaupallisesta sähköpostiviestinnästä. Direktiivi on osa uutta laajempaa sähköisen viestinnän sääntelyjärjestelmää²⁴. Euroopan parlamentti on hiljattain ilmaissut

²² Euroopan parlamentin ja neuvoston direktiivi, annettu 8 päivänä kesäkuuta 2000, EYVL L 178, 17.7.2000. Yleissääntönä on, että ”kaupallisen viestinnän” on oltava niiden sääntöjen mukaista, joita siihen sovelletaan jäsenvaltiossa, johon palvelun tarjoaja on sijoittautunut. Tätä sääntöä ei kuitenkaan sovelleta sähköpostitse tapahtuvan ei-toivotun viestinnän sallittavuuteen (ks. direktiivi sähköisestä kaupankäynnistä, 3 artikla ja liite). Niissä (harvoissa) tapauksissa, joissa direktiivi 2002/58/EY ei suojaisi luonnollisia henkilöitä ei-toivotulta kaupalliselta viestinnältä (ts. luonnollisia henkilöitä, jotka eivät ole tilaajia), jäsenvaltioiden on huolehdittava sähköistä kaupankäyntiä koskevan direktiivin mukaisesti siitä, että ei-toivottua kaupallista viestintää sähköpostitse harjoittavat palveluntarjoajat käyttävät säännöllisesti ja myös noudattavat rekistereitä, joihin luonnolliset henkilöt, jotka eivät halua tällaista kaupallista viestintää, voivat ilmoittautua (ks. sähköistä kaupankäyntiä koskevan direktiivin 7 artikla).

²³ Ehdotus: neuvoston puitepäättös tietojärjestelmiin kohdistuvista hyökkäyksistä, KOM(2002) 173 lopullinen, 19.4.2002.

²⁴ Ks. myös televiestinnän sääntelypaketin täytäntöönpanoa koskeva yhdeksäs raportti osoitteessa http://europa.eu.int/information_society/topics/ecommerce/all_about/implementation_enforcement/annualreports/9threport/index_en.htm.

huolensa tästä viiveestä²⁵. Koska jäsenvaltioilla oli velvollisuus saattaa sähköisen viestinnän tietosuojadirektiivi osaksi kansallista lainsäädäntöä viimeistään 31. lokakuuta 2003, komissio käynnisti marraskuussa 2003 jäsenyysvelvoitteiden rikkomisesta johtuvan menettelyn niitä jäsenvaltioita vastaan, jotka eivät olleet ilmoittaneet komissiolle kansallisista täytäntöönpanotoimenpiteistä²⁶.

3.1. Johdanto

Vaikka pelkkä lainsäädännön olemassaolo toimii pelotteena roskapostittajille, se ei yksinään riitä. Yhtenä prioriteettina on oltava myös se, että suostumukseen perustuvan järjestelmän soveltamista valvotaan tehokkaasti kaikissa jäsenvaltioissa. Tämä edellyttää riittävän henkilöstön ja voimavarojen ohella riittäviä lainvalvontakeinoja, myös valtioiden rajat ylittäviä. Keskeinen merkitys on myös yhteistyöllä EU:n ulkopuolisten maiden kanssa. Myös seuranta on tärkeää jo lainvalvonnan painopisteiden määrittämiseksi.

Useat tekijät näyttävät vaikuttavan lainvalvontakeinojen toimivuuteen:

- Voidaanko lain noudattamista valvoa tehokkaiden sakko- tai muiden rangaistusten tuella. Joillakin sääntelyviranomaisille ei ole tässä suhteessa nähtävästi edelleenkaan (tehokkaita) valtuuksia.
- Millaisia valitus- ja oikeuskeinoja yksityishenkilöiden ja yritysten käytössä on.
- Onko kansallisten viranomaisten keskinäistä toimintakenttää selvennettävä ja koordinoitava johtuen viranomaisten toisinaan päällekkäisistä tehtävistä tällä osa-alueella.
- Miten hyvin käyttäjät ovat selvillä oikeuksistaan ja tavoista valvoa niitä. Käyttäjille on annettava tietoa siitä, minne valitetaan, mitä valitusmenettelyssä tutkitaan ja mitä ei, millaisia toimia valituksesta voi olla tuloksena ja mitä tietoja heidän on annettava viranomaisille tutkimuksen käynnistämiseksi.
- Jäsenvaltioiden keskinen sekä jäsenvaltioiden ja EU:n ulkopuolisten maiden välinen koordinointi ja yhteistyö liittyen oikeuspaikan valintaan yksittäisissä tapauksissa.
- Mitä resursseja on käytössä sellaisten EU:ssa tai sen ulkopuolella toimivien roskapostin lähettäjien jäljittämiseksi, jotka peittävät jälkensä käyttämällä muiden tunnistetietoja, osoitteita tai palvelimia.

Ei-toivottuun viestintään sovellettavat säännökset kuvataan edellä kohdassa 2.2. Tällaiseen ei-toivottuun sähköpostimainontaan liittyvät menettelyt on tähän asti järjestetty melko vaihtelevasti²⁷. Vaikka EU-direktiivi on säädöstyypinä sellainen, että se jättää jäsenvaltioille tietyn liikkumavaran täytäntöönpanossa, säännösten noudattamista on valvottava tehokkaasti, olipa täytäntöönpanokeino mikä hyvänsä.

²⁵ Komissio painottaa sähköisen viestinnän uuden sääntelyjärjestelmän – myös siis kyseisen direktiivin – täydellisenn, tehokkaan ja ripeän täytäntöönpanon tärkeyttä tiedonannossaan ”Sähköinen viestintä: tie osaamistalouteen” (KOM(2003) 65, 11. helmikuuta 2003).

²⁶ Viralliset ilmoitukset lähetettiin 25. marraskuuta 2003 (ks. IP/03/1663).

²⁷ Valitukset koskevat usein myös muita asiaan liittyviä kysymyksiä, kuten henkilötietojen saantioikeutta ja oikeutta kieltää tietojen käsittely.

Käytännöt vaihtelevat

Ei-toivottua kaupallista viestintää koskevien säännösten soveltamisen valvonnasta ei huolehdi sama viranomainen kaikissa jäsenvaltioissa. Useimmissa jäsenvaltioissa tämä valvonta kuuluu ensi kädessä tietosuojaviranomaiselle, mutta joissain siitä huolehtii sähköisen viestinnän sääntelyviranomainen ja joissain pääasiallisesti kuluttajansuojaviranomainen (myös kuluttaja-asiamies). Usein lainvalvontavastuun jakaa useampi kuin yksi viranomainen. Lisäksi roskaposti on monissa tapauksissa myös harhaanjohtavaa tai vilpillistä mainontaa. (Joissain harvoissa jäsenvaltioissa ei ole kuluttajansuojaviranomaista, jolloin valvonta jää kuluttajajärjestöille tai kuluttajille itselleen.) Roskapostin lähettäminen liittyy usein tietosuojarikkomuksiin, kuten osoitteiden haravointiin, ja jopa tietoverkkorikollisuuteen, kuten luvattomaan murtautumiseen tietokoneisiin tai palvelimiin. Saattaa olla, että kulloistenkin säännösten soveltamisen valvonnasta eivät vastaa samat viranomaiset edes jäsenvaltion sisällä, saati jäsenvaltioiden välillä.

Valitukset johtavat yleensä tutkintaan vain joissain jäsenvaltioissa. Toisinaan ennen varsinaista selvitysprosessia asianomaisiin otetaan yhteyttä muun muassa antamalla ohjeita ja suuntaviivoja yrityksille, osittain hyvin tuloksin. Joskus näistä esitoimista huolehtii kuluttaja, joka ottaa yhteyttä yritykseen ennen valituksen jättämistä. Muutamissa maissa (esim. Britanniassa) sovelletaan itsesääntelyä tässä ensimmäisessä vaiheessa. Joissain jäsenvaltioissa yritykset soveltavat itsesääntelyä omien valitusmenettelyjen muodossa. Myös viranomaiset toimivat usein omasta aloitteestaan. Asian kuuluminen hallintoviranomaisen toimivaltaan ei tavallisesti estä turvautumista suoraan oikeusviranomaisiin.

Kaikilla tietosuojaviranomaisilla ei ole valtuuksia käynnistää toimia oikeushenkilöitä vastaan. Kaikilla tietosuojaviranomaisilla ei liioin ole (ainakaan vielä) mahdollisuutta määrätä seuraamuksia. Näiden viranomaisten on siksi hoidettava asia oikeusteitse. Ranskassa roskapostilaatikkoaloitteesta saatu kokemus on johtanut käytäntöön, jossa tietosuojaviranomainen valikoi tietyt erityistapaukset ja siirtää niiden käsittelyn oikeusviranomaisille, tosin ilman mainittavaa menestystä. Belgiassa vastaava aloite on johtanut yhteydenottoihin epäiltyjen lähettäjien kanssa ja rajatylittävissä tapauksissa asian käsittelyn siirtämiseen EU:n tason viranomaiselle tai Yhdysvaltojen FTC:lle.

Toimivimpana tapana huolehtia suostumukseen perustuvan järjestelmän valvonnasta pidetään usein käytäntöä, joka sisältää oikeassa suhteessa sekä lainsäädäntöä, lainvalvontaa että itsesääntelyä. Jäsenvaltioita pyydetäänkin arvioimaan lainvalvontakeinojensa tehokkuus erityisesti jäljempänä kohdissa 3.2–3.6 ehdotettujen eri toimien kannalta.

Jäsenvaltioita pyydetään myös laatimaan erityiset kansalliset strategiat, jotta voidaan varmistaa tietosuojaviranomaisten, kuluttajansuojaviranomaisten ja sähköisen viestinnän kansallisten sääntelyviranomaisten välinen yhteistyö ja välttää päällekkäisyydet eri viranomaisten välillä.

Lainvalvontaan liittyvän tiedonvaihdon ja parhaiden toimintatapojen (esim. valitukset, oikeuskeinot, seuraamukset ja kansainvälinen yhteistyö) edistämiseksi ja koordinoimiseksi komission yksiköt ovat jäsenvaltioiden ja tietosuojaviranomaisten tuella perustaneet **ei-toivottua sähköpostiviestintää käsittelevän epävirallisen online-työryhmän**. Työryhmä helpottaa ja koordinoi myös muihin tässä tiedonannossa esitettyihin toimiin (tiedotus, tekniset ratkaisut) liittyvää työtä.

Työryhmän keskustelujen perusteella laaditut asiakirjat toimitetaan yleensä viestintäkomitealle (COCOM), joka on perustettu osana sähköisen viestinnän verkkojen ja palvelujen sääntelyjärjestelmää, ja/tai direktiivin 95/46/EY 29 artiklalla perustetulle tietosuojatyöryhmälle, jotka ryhtyvät tarvittaviin toimiin. Online-työryhmä voi muun muassa laatia vertailuindikaattoreita ehdotettaville eri toimenpiteille.

Tässä online-työryhmässä kokoontuvat toimivaltaiset kansalliset viranomaiset (mm. tietosuojaviranomaiset) ja komission yksiköiden edustajat. Online-työryhmä määrittää, miten muiden sidosryhmien osallistuminen järjestetään.

3.2. Oikeuskeinot ja seuraamukset

3.2.1. Tämänhetkinen tilanne

Tällä hetkellä oikeuskeinoin kuuluvat sakot ja luvattoman tietojen käsittelyn lopettamismääräys, johon liittyy joskus pääsyn estäminen kyseisille verkkosivuille. Joissain jäsenvaltioissa lopettamismääräys edeltää sakkoja (jotka määrätään sen noudattamatta jättämisestä) tai se määrätään sakkojen kera. Kaikilla viranomaisilla ei ole kuitenkaan lainkäyttövaltaa kaikissa roskapostiin liittyvissä rikkomuksissa eikä samoja keinoja käytettävissään. Lisäksi tapausten käsittely siirretään usein oikeusviranomaisille. Kaikissa jäsenvaltioissa ei ole oikeudellisia sanktioita rikkomistapausten varalta.

Kaikissa jäsenvaltioissa ei ole käytössä hallinto- eikä rikosoikeudellisia oikeuskeinoja tai sakkoja/seuraamuksia. Rikosoikeudelliset sanktiot vaihtelevat. Joissain jäsenvaltioissa niihin kuuluu vankeusrangaistuksia. Lisäksi kuluttajilla on yleensä mahdollisuus hakea vahingonkorvausta siviilioikeuden nojalla.

”Lievien” ja ”vakavien” rikkeiden (esim. massapostitukset, harhaanjohtava tai vilpillinen mainonta ja kauppa) välillä tehdään usein ero, mutta itse seuraamukset vaihtelevat suuresti jäsenvaltioittain.

Useissa tapauksissa roskapostin lähettäminen voi johtaa seuraamuksiin myös yleisen tietosuojalainsäädännön nojalla (esim. rikottaessa ilmoittamisvelvoitetta, käyttöoikeutta, velvoitetta nimetä edustaja EU:n jäsenmaassa) tai erityislainsäädännön nojalla (esim. harhaanjohtava mainonta, vilpillinen markkinointi). Erityisesti ennen suostumukseen perustuvan järjestelmän käyttöönottoa roskapostin eri näkökohtiin (esim. massapostitukset, henkilötietojen luvaton käyttö, verkkohäiriöt, sähköpostiosoitteiden väärinkäyttö, petokset ja sopimusten väärintulkinta) puututtiin eri oikeusperustoista käsin.

Yleisesti ottaen pelkkää mahdollisuutta turvautua tuomioistuinkäsittelyyn ei pidetä riittävänä lainvalvonnan kannalta. Tietosuojaviranomaiset, kuluttajansuojaviranomaiset ja/tai kansalliset sääntelyviranomaiset voivat yleensä määrätä hallinnollisia sakkoja, joiden suuruus vaihtelee. Useimmat jäsenvaltioista, joissa tätä mahdollisuutta ei vielä ole, harkitsevat sen käyttöönottoa. Verrattuna tuomioistuinkäsittelyyn hallinnolliset sanktiot voivat olla erityisen sopiva keino tällaiselle dynaamiselle alalle. Tietosuojaviranomaiset, kuluttajansuojaviranomaiset ja kansalliset sääntelyviranomaiset käyttävät lainvalvonnessa usein lisäkeinoja. Hallinnolliset menettelyt voivat olla huokea ja nopea vaihtoehto (esim. Italian tietosuojaviranomaiset ilmoittavat menettelyn kestävän enintään 50 päivää).

3.2.2. Ehdotetut toimet

Ensimmäisenä edellytyksenä on, että ne jäsenvaltiot, jotka eivät ole vielä saattaneet direktiiviä ja erityisesti ei-toivottua viestintää koskevia säännöksiä osaksi kansallista lainsäädäntöään, tekevät niin viipymättä. Komission yksiköt ovat valmiita tarvittaessa auttamaan jäsenvaltioita.

Jäsenvaltioita pyydetään arvioimaan käyttämiensä oikeuskeinojen ja seuraamusten toimivuus ja luomaan rikkomusten uhreille riittävät mahdollisuudet hakea korvausta.

Jäsenvaltioiden ja toimivaltaisten viranomaisten, joilla ei ole käytössään hallinto-oikeudellisia keinoja, tulisi harkita niiden käyttöönottoa roskapostia vastaan, sillä ne ovat nopea, huokea ja tehokas keino valvoa suostumukseen perustuvan järjestelmän soveltamista.

Komissio aikoo varmistua siitä, että direktiivin kansalliset täytäntöönpanotoimenpiteet sisältävät todellisia sanktioita (tarvittaessa taloudellisia ja rikosoikeudellisia seuraamuksia) siltä varalta, että vaatimuksia ei noudateta.

Tässä yhteydessä komissio aikoo myös tutkia, missä määrin toimivaltaisilla viranomaisilla on tarvittavat tutkinta- ja täytäntöönpanovaltuudet.

3.3. Valituskeinot

3.3.1. Tämänhetkinen tilanne

Tehokas lainvalvonta edellyttää riittäviä valituskeinoja. Eräät tietosuojaviranomaiset ovat luoneet erityisiä sähköpostilaatikkoja, joihin käyttäjät voivat toimittaa saamansa ei-toivotut sähköpostiviestit, ja ovat sitoutuneet ryhtymään toimiin kohdennetuissa tapauksissa. Eräät jäsenvaltiot näyttävät asettavan etusijalle normaalit hallinnolliset keinot ja/tai yhteydenpidon Internet-palveluntarjoajiin, tai tietotekniikan kriisiryhmät (Computer Emergency Response Teams (CERT)) verkkohäiriöiden tapauksessa. Toiset jäsenvaltiot suosivat perinteisiä menettelyjä (siviilioikeudellisia vahingonkorvausmenettelyjä tai hallintomenettelyjä). Yhteissääntelyä tai itsesääntelyä pidetään joskus parempana vaihtoehtona kuin suoria lainvalvontatoimenpiteitä.

Parhaat toimintatavat

Ranska ja Belgia ottivat loppuvuodesta 2002 käyttöön erityiset sähköpostilaatikat, joihin käyttäjät voivat lähettää valituksia roskapostista. Saadut tulokset ovat kiinnostavia. Tulokset ovat julkisesti saatavilla raporteissa²⁸. Odotettavissa on, että Ranska ottaa roskapostilaatikon käyttöön pysyvästi osana uusia toimenpiteitä, joilla sähköisen viestinnän tietosuojadirektiivi saatetaan osaksi kansallista lainsäädäntöä. Yhdysvaltojen FTC ylläpitää vastaavaa roskapostilaatikkoa, johon toimitettua ainestoa käytetään nostettaessa syytteitä sopimatonta ja harhaanjohtavaa markkinointia vastaan²⁹.

Tällaisten sähköpostilaatikkojen etuihin kuuluu, että ne näyttävät rohkaisevan kuluttajia raportoimaan rikkomuksista ja sitä kautta tehostavan lainvalvontaa. Lisäksi ne voivat tarjota olennaisia tilastoja ongelman laajuudesta ja luonteesta tietyssä maassa tai tietyllä alueella ja sitä kautta selkeän yleiskuvan, joka puolestaan on viranomaisille arvokas väline lainvalvonnan painopisteiden asettamisessa tai mukauttamisessa. Lisäksi näin saadun tietämyksen perusteella voidaan suunnitella ennaltaehkäiseviä toimia. Esimerkkinä mainittakoon, että Ranskan tietosuojaviranomainen CNIL on käyttänyt

²⁸ Ranskan tietosuojaviranomaisen CNIL:n 24. lokakuuta 2002 julkaisema raportti: http://www.cnil.fr/frame.htm?http://www.cnil.fr/thematic/internet/spam/spam_sommaire.htm
Belgian tietosuojalautakunnan CPVP:n heinäkuussa julkaisema raportti:

http://www.privacy.fgov.be/publications/spam_4-7-03_fr.pdf

²⁹ Ks. esim. <http://www.ftc.gov/bcp/online/pubs/online/inbox.pdf> Ei-toivotut tai harhaanjohtavat viestit voi lähettää seuraavaan osoitteeseen uce@ftc.gov.

roskapostilaatikon avulla kerättyjä tietoja hyväkseen laatiakseen käyttäjille ja markkinoijille suunnattuja tietopaketteja tavoitteena puuttua roskapostin ongelmaan ennakolta.

Se, miten hyödyllinen tällainen sähköpostilaatikko on roskapostiongelman seuraamisessa ja sen laajuuden määrittämisessä, riippuu valmiuksista tutkia tehdyt valitukset hyödyllisesti ja nopeasti.

Vaikka jäsenvaltioilla on yleensä kiinnostusta oppia kokemuksista, joita tällaisista hankkeista on saatu muissa jäsenvaltioissa, vain muutamat jäsenvaltiot näyttävät suunnittelevan tai harkitsevan omaa roskapostilaatikkoo. Perusteina mainitaan yleensä, että käytössä on jo mahdollisuus valittaa sähköpostitse (tyypillisesti viranomaisen verkkosivulla), että erityinen roskapostilaatikko edellyttäisi omaa henkilöstöä ja välineistöä tai että voimassa olevia oikeudellisia menettelyjä olisi muutettava.

3.3.2. Ehdotetut toimet

Jäsenvaltioiden ja toimivaltaisten viranomaisten pitäisi arvioida, miten tehokkaasti niiden oikeusjärjestelmä kykenee käsittelemään käyttäjien valitukset, ja hahmotella tarvittaessa muutoksia.

Jäsenvaltioita ja viranomaisia pyydetään käynnistämään oma roskapostilaatikkohanke ja tukemaan sitä tiedotuskampanjoin.

Nämä postilaatikat tulisi suunnitella siten, että ne mahdollistavat yksinkertaisen haun ja analyysin. Tarkoituksena on saada ongelmasta parempi käsitys, jolloin voidaan asettaa painopisteet lainvalvonnassa.

Komission yksiköt tukevat tiedonvaihtoa kokemuksista, joita postilaatikkohankkeista saadaan.

3.4. Rajatylittävät valitukset ja lainvalvontayhteistyö EU:ssa

3.4.1. Tämänhetkinen tilanne

Myös rajatylittävät valitukset on voitava käsitellä tehokkaasti, jotta kuluttajansuoja toteutuisi tällä osa-alueella. On tärkeää taata, että kansalliset valitusjärjestelmät voidaan niiden toimintatavoista riippumatta verkottaa keskenään siten, että tietystä jäsenvaltiosta tulevat kuluttajavalitukset, jotka koskevat toisesta jäsenvaltiosta tulevia viestejä, voidaan nekin käsitellä tehokkaasti (ks. kohta 3.5 ”Yhteistyö EU:n ulkopuolisten maiden kanssa”).

Kaikilla jäsenvaltioilla ei ole tätä nykyä virallista menettelyä rajat ylittävien valitusten käsittelemiseksi. Asia ratkaistaan tällä hetkellä ottamalla yhteyttä toisen jäsenvaltion vastaavaan viranomaiseen tai mahdollisesti siirtämällä valitus sen valtion viranomaisen käsiteltäväksi, josta viestit ovat lähtöisin.

Tietosuojaviranomaiset vaihtavat Euroopan tasolla (myös ETA- ja ehdokasmaat) tietoa rajatylittävistä valituksista erityisen valitusten käsittelyä tarkastelevan työryhmän kautta. Työryhmä perustettiin Euroopan tietosuojavaaltuutettujen konferenssin yhteyteen (European Conference of Data Protection Commissioners). Työryhmää on mahdollista käyttää roskapostia koskeviin rajatylittävien valitusten käsittelyyn, muun muassa

määritettäessä oikeuspaikkaa yksittäisissä tapauksissa. Samalla on kuitenkin todettava, että kaikki tietosuojaviranomaiset eivät valvo ei-toivottua sähköpostiviestintää koskevien säännösten soveltamista.

Kuluttajansuojan alalla komissio on hiljattain ehdottanut asetusta kuluttajansuoja-alan yhteistyöstä. Asetuksella luotaisiin kuluttajansuojaviranomaisten verkko, joka käsittelee rajatylittäviä valituksia³⁰. Sillä otettaisiin käyttöön keskinäiset avunantomenettelyt ja luotaisiin tiivis käytännön yhteistyö kansallisten viranomaisten välille. Harhaanjohtava tai vilpillinen tai kuluttajansuojasäännöksiä muuten rikkova roskaposti kuuluisi asetuksen soveltamisalaan, vaikkakaan ei kaikki sähköisen viestinnän tietosuojadirektiivissä kielletty roskaposti. Asetusehdotus on parhaillaan neuvoston ja parlamentin käsittelyssä.

3.4.2. Ehdotetut toimet

Jäsenvaltioita ja toimivaltaisia viranomaisia pyydetään arvioimaan, miten tehokkaasti rajatylittävät valitukset voidaan käsitellä nykymenettelyillä (esim. sopimukset keskinäisestä avunannosta).

Kansallisia viranomaisia pyydetään tehostamaan keskinäistä koordinoitua. Kyse on koordinoinnista ja tiedonvaihdosta niiden viranomaisten kesken, jotka vastaavat uusien säännösten täytäntöönpanosta, sekä näiden viranomaisten ja sellaisten muiden viranomaisten välillä, joilla on vastuullaan roskapostin eri muotoja (esim. vilpillinen roskaposti ("scams"), pornografinen roskaposti, terveystuotteiden laittomaan jakeluun liittyvät viestit).

Vilpillisen ja harhaanjohtavan roskapostin osalta neuvostoa ja Euroopan parlamenttia pyydetään sopimaan komission ehdottamasta kuluttajansuoja-alan yhteistyötä koskevasta asetuksesta mahdollisimman pian, jotta EU:n kuluttajansuojaviranomaisille saataisiin täydet edellytykset puuttua harhaanjohtavaan ja vilpilliseen roskapostiin. Niitä pyydetään myös harkitsemaan asetuksen soveltamisalan laajentamista kattamaan sähköisen viestinnän tietosuojadirektiivi. Jäsenvaltioita pyydetään tutkimaan keinoja poistaa esteitä tiedonvaihdon ja yhteistyön tieltä sekä avun pyytämiseltä muiden jäsenvaltioiden vastaavilta viranomaisilta. Käytännössä voisi olla hyödyllistä ottaa käyttöön erityinen yhteydenpitojärjestelmä (vrt. edellä mainittu tietosuojaviranomaisten aloite), jonka kautta kansalliset sääntelyviranomaiset voisivat toimia yhteistyössä rajatylittävän lainvalvonnan tiimoilta. Yhteistyötä tukevan verkon luomisessa voitaisiin hyödyntää jo meneillään olevia komission ohjelmia, kuten IDA-ohjelmaa³¹.

Komissio aikoo helpottaa ja edistää tällaista kansallisten viranomaisten välistä koordinoitua ja hyödyntää tässä erityisesti epävirallista online-työryhmää, joka asetettiin hiljattain käsittelemään ei-toivottua sähköpostiviestintää. Komission yksiköt ovat yhdessä jäsenvaltioiden ja kansallisten lainvalvontaviranomaisten kanssa alkaneet tutkia, mitä konkreettisia toimia tarvitaan rajatylittävien valitusten käsittelyn parantamiseksi. Kansallisten viranomaisten kanssa jatketaan keskusteluja vuoden 2004 aikana.

³⁰ KOM(2003) 443 lopullinen.

³¹ Tietoa IDA-ohjelmasta: <http://europa.eu.int/comm/enterprise/ida/index.htm>.

3.5. Yhteistyö EU:n ulkopuolisten maiden kanssa

3.5.1. Tämänhetkinen tilanne

Uusia sääntöjä sovelletaan henkilötietojen käsittelyyn, joka liittyy yleisesti saatavilla olevien sähköisen viestinnän palvelujen tarjoamiseen yleisissä viestintäverkoissa EU:ssa (ja ETA:ssa). Niinpä direktiivin 2002/58/EY 13 artiklaa, jossa suostumukseen perustuva järjestelmä vahvistetaan, sovelletaan kaikkeen ei-toivottuun kaupalliseen viestintään, joka vastaanotetaan ja lähetetään verkkojen välityksellä EU:ssa (ja ETA:ssa). Tämä tarkoittaa, että tällaisten viestien on oltava EU:n säännösten mukaisia myös silloin, kun ne ovat lähtöisin EU:n ulkopuolelta. Sama pätee viesteihin, jotka lähetetään EU:sta sen ulkopuolelle.

Säännön soveltamisen valvonta on selvästi vaikeampaa niissä tapauksissa, joissa viestit ovat lähtöisin EU:n ulkopuolelta. Se on kuitenkin tärkeää, koska suuri osa roskapostista tulee EU:n ulkopuolelta.

Ongelmaan on puututtava eri tavoilla, joita ovat ennaltaehkäisy, suodatustekniikat, itsesääntely, sopimukset sekä kansainvälinen yhteistyö, johon keskitytään tässä luvussa. Kansainvälisen yhteistyön ensimmäisenä tavoitteena on edistää sitä, että EU:n ulkopuolisissa maissa otetaan käyttöön tehokas lainsäädäntö tällä osa-alueella. Toisena tavoitteena on harjoittaa yhteistyötä EU:n ulkopuolisten maiden kanssa, jotta voidaan varmistaa sääntöjen soveltamisen tehokas valvonta.

Nykyisten suostumus- tai kielto­sääntöjen soveltamisen valvonnasta ei ole paljonkaan kokemusta tapauksissa, joissa viestit tulevat EU:n ulkopuolelta. Sen lisäksi, että roskaposti sinänsä on suhteellisen uusi ilmiö, esteinä mainitaan usein, että tällaisen roskapostin lähettäjiä on vaikea jäljittää tai että tämä vaatii paljon työtä, että käytössä ei ole (sopivia) kansainvälisiä yhteistyökeinoja ja että joillakin viranomaisilla ei ole toimivaltaa kansainvälisissä asioissa.

Mitä tulee vilpilliseen ja harhaanjohtavaan roskapostiin, kuluttajansuoja-alan yhteistyötä koskevassa komission asetusehdotuksessa säädetään myös lainvalvontaan liittyvästä yhteistyöstä EU:n ulkopuolisten maiden kanssa. Taloudellisen yhteistyön ja kehityksen järjestö OECD antoi vuonna 2003 suosituksen, jonka tavoitteena on suojella kuluttajia rajatylittäviltä vilpillisiltä ja harhaanjohtavilta kaupallisilta menettelyiltä³².

3.5.2. Ehdotetut toimet

Monenvälisellä tasolla osa jäsenvaltioista osallistuu jo aktiivisesti toimintaan esimerkiksi OECD:n puitteissa ja muualla, missä roskapostin ongelmaa on alettu käsitellä. Aktiivinen osallistuminen tähän työhön on toivottavaa, varsinkin jotta ongelmaan voitaisiin löytää kansainvälisesti toimivia ratkaisuja.

Komissio järjestää helmikuussa 2004 roskapostia käsittelevän OECD-tapaamisen, jossa on tarkoitus parantaa käsitystä roskapostiongelmosta ja edistää kansainvälisiä ratkaisuja. Tapaamisen tulokset tarjoavat perustaa konkreettisille jatkotoimille OECD:n tasolla. Komission yksiköt keskustelevat jäsenvaltioiden kanssa näistä jatkotoimista, joihin kuuluvat OECD:n toimet, joilla tuetaan tehokkaan lainsäädännön aikaansaamista

³² OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders, OECD, 2003.

kansainvälisesti, sekä tiedotus, tekniset ratkaisut, itsesääntely ja lainvalvontaan liittyvä kansainvälinen yhteistyö.

YK:n tasolla järjestetyn tietoyhteiskuntahuippukokouksen (Geneve 10.-12. joulukuuta 2003) julistusluonnoksessa ja siihen liittyvässä toimintasuunnitelmassa painotetaan, että roskapostiongelmaan on puututtava asianmukaisella kansallisella ja kansainvälisellä tasolla. Komissio aikoo tarkastella, mihin toimiin huippukokouksen tulosten pohjalta pitäisi ryhtyä EU:ssa, ottaen huomioon, että Tunisian huippukokous järjestetään vuonna 2005.

Jäsenvaltioita ja viranomaisia pyydetään tehostamaan tai panemaan alulle myös kahdenvälistä yhteistyötä EU:n ulkopuolisten maiden kanssa. Tavoitteena on edistää tehokkaan lainsäädännön aikaansaamista ja myös harjoittaa yhteistyötä (tarvittaessa poliisi- ja oikeusyhteistyötä) sen soveltamisen valvonnassa.

Myös viranomaisten ja yksityisen sektorin, erityisesti Internet- ja sähköpostipalvelun tarjoajien välistä yhteistyötä rohkaistaan. Tavoitteena on jäljittää roskapostin lähettäjät rajoittamatta asianmukaista oikeusturvaa.

Komission yksiköt aikovat edelleen toimia aktiivisesti kansainvälisillä foorumeilla, kuten OECD:n puitteissa ja tapaamisessa, jonka komissio järjestää Brysselissä helmikuussa 2004. Komissio aikoo myös järjestää kahdenvälisiä kokouksia ja keskusteluja EU:n ulkopuolisten maiden kanssa muun muassa rohkaistakseen niitä ryhtymään tehokkaisiin toimiin roskapostia (erityisesti sen haitallisimpia muotoja) vastaan ja ajaakseen yhteistyötä lainvalvonnassa.

Komission yksiköt ovat alkaneet tutkia yhdessä jäsenvaltioiden ja kansallisten lainvalvontaviranomaisten kanssa, miten kansainvälinen yhteistyö voitaisiin parhaiten järjestää – erityisesti jotta taattaisiin, että EU:n ulkopuolelta tulevaa roskapostia koskevat valitukset voidaan käsitellä. Työtä jatketaan kansallisten viranomaisten kanssa vuoden 2004 aikana.

3.6. Seuranta

3.6.1. Tämänhetkinen tilanne

Jotta suostumukseen (”opt-in”) perustuvan järjestelmän toimintaa voitaisiin arvioida käytännössä ja puuttua yksittäisiin ongelmiin sopivin keinoin, jäsenvaltiot tarvitsevat puolueetonta ja ajantasaista tietoa roskapostin, käyttäjien valitusten ja palveluntarjoajien kohtaamien ongelmien kehityssuuntauksista. Tietoa tarvitaan ei-toivotun kaupallisen sähköpostiviestinnän luonteen, alkuperän ja volyymin kehityssuuntauksista, jolloin tiedot saadaan suodatusohjelmistojen tarjoajilta, palveluntarjoajilta ja kansallisilta viranomaisilta. Lisäksi tarvitaan valituspostilaatikkojen käyttöön liittyviä tilastotietoja, kun tällaisia on käytettävissä.

OECD aloitti vuonna 2003 ei-toivottujen sähköpostiviestien määrällisen arvioinnin kansainvälisellä tasolla ja jatkaa tätä työtä vuonna 2004.

Sähköisen viestinnän tietosuojadirektiivin 18 artiklan mukaan komissio julkaisee vuonna 2006 kertomuksen direktiivin soveltamisesta ja sen vaikutuksista taloudellisiin toimijoihin ja kuluttajiin, erityisesti mitä tulee ei-toivottua viestintää koskeviin

säännöksiin. Kertomusta laatiessaan komissio tarvitsee tietoa jäsenvaltiolta, muun muassa tarvittavat tilastot.

3.6.2. Ehdotetut toimet

Jäsenvaltioiden tulisi varmistaa, että niillä on lainvalvonnan edellyttämät tiedot ja tilastot. Tässä tulisi tarvittaessa toimia yhteistyössä yritysten kanssa ja ottaa huomioon, että OECD:ssä on meneillään ei-toivotun sähköpostiviestinnän määrällinen arviointi.

Komissio käyttää epävirallista online-ryhmää, joka perustettiin hiljattain käsittelemään ei-toivottua sähköpostiviestintää ja helpottamaan ja koordinoimaan roskapostitrendeihin, parhaisiin toimintatapoihin ja roskapostitilastoihin liittyvää tiedonvaihtoa.

4. YRITYSTEN TEKNISET TOIMENPITEET JA ITSESÄÄNTELY

Tässä luvussa käsitellään erityisesti yrityksille ehdotettavia toimenpiteitä, joita ovat sopimusjärjestelyt, käytäntösäännöt, hyväksyttävät markkinointikäytännöt, merkinnät ja vaihtoehtoiset riidanratkaisumenetelmät. Niihin kuuluvat myös eräät tekniset ratkaisut, kuten suodatus ja palvelinten turvatoiminnot.

4.1. Suostumukseen perustuvan järjestelmän soveltaminen

4.1.1. Tämänhetkinen tilanne

Roskapostin torjunta on kaikkien sidosryhmien tehtävä. Yrityksillä voi olla tässä erityinen rooli, koska ne voivat tehdä suostumukseen perustuvasta järjestelmästä jokapäiväisen liiketoimintakäytäntönsä. Tällainen käytäntö kattaa loppukäyttäjille tarjottavien ehtojen lisäksi myös asiainnity yrityskumppanien kanssa.

Monissa tapauksissa on tarpeen, että koordinoitua tehostetaan toimialajärjestöjen kautta ja että mukana on alakohtaisia itsesääntelyelimiä ja kuluttaja- tai käyttäjäjärjestöjä sekä myös tietosuojaviranomaisia tai muita toimivaltaisia kansallisia viranomaisia.

Parhaat käytännöt

Esimerkiksi Alankomaissa vuonna 2002 toimintansa aloittanut sähköisen kaupan foorumi ECP on käynnistänyt hankkeen ”sähköpostimainonnan käytäntösääntöjen” (*Code Verspreiding Reclame via E-mail*) laatimiseksi. Hankkeeseen osallistuu suoramarkkinointia harjoittavia yrityksiä, Internet-palveluntarjoajia ja Alankomaiden kuluttajajärjestö. Tavoitteena on kehittää suostumukseen perustuvan järjestelmän käytännön soveltamista. Käytännön toteutusta testataan tietosuojaviranomaisen kanssa³³.

Sopimukset voivat auttaa roskapostin torjunnassa, kunhan yksilöiden oikeudet turvataan. Monet Internet- ja sähköpostipalveluntarjoajat sisällyttävät jo asiakassopimuksiinsa velvoitteita, joilla ne kieltävät palvelintensa käytön roskapostin lähettämiseen. Nämä palveluntarjoajat estävät jo ei-toivottujen sähköpostiviestien ja massapostitusten lähettämisen hallinnoimistaan sähköpostiosoitteista³⁴.

³³ see <http://www.ecp.nl/projecten.php#32>.

³⁴ Nämä lausekkeet perustuvat joskus tarpeeseen ryhtyä kaikkiin toimenpiteisiin palvelinten väärinkäytön estämiseksi. Toisinaan sopimuksissa viitataan jo käytössä oleviin käytäntösääntöihin massapostituksista taikka itsesääntelyperiaatteisiin (esim. nettietiketti).

Aiemmissa Internet-palveluntarjoajien ja asiakkaiden välisissä sopimuksissa sovelletut periaatteet todennäköisesti poikkeavat uuden direktiivin ja siihen perustuvan kansallisen lain periaatteista.

Asiakaspalvelua ajatellen tarvitaan myös aktiivisempi toimintaperiaate suodattamiseen: tilaajille pitäisi tarjota tietoa roskapostisuodattimista sekä suodatuspalveluja tai -toimintoja valinnaisena palveluna.

Sama pätee myös aina, kun Internet-palveluntarjoajat tai matkaviestinoperaattorit tekevät sopimuksia kolmansien osapuolten ja erityisesti suoramarkkinoijien kanssa. Tässä ei ole kyse vain suorista suhteista lisäarvopalveluja tarjoaviin yrityksiin, vaan se käsittää myös operaattorit, joiden kanssa yksittäisellä palveluntarjoajalla on yhteenliittämissopimus, kuten on laita matkaviestintäpalveluissa.

Uudella suostumukseen perustuvalla järjestelmällä on vaikutuksia myös moniin suoramarkkinointitoimintoihin:

- sähköpostiosoitteiden ja sähköisten yhteystietojen keruumenetelmiin tullaan soveltamaan uutta järjestelmää (kuten edellä todetaan, sähköpostiosoitteiden ”haravointi” on yhteisön oikeuden vastaista)
- olemassa olevien luettelojen mukauttaminen
- kiellot käyttää tietoja ilman suostumusta ja myydä luvattomia luetteloja.

4.1.2. Ehdotetut toimet

Yritysten osallistumista ja itsesääntelyä sekä myös yhteissääntelyä pitäisi edistää erityisesti osa-alueilla, joilla lainsäädäntö ja sen soveltamisen valvonta viranomaisten toimesta ei välttämättä ole riittävää. Kaikkien sidosryhmien, myös kuluttaja- ja/tai käyttäjäjärjestöjen, pitäisi osallistua tähän toimintaan.

Palveluntarjoajien sopimuskäytännöt tilaajien ja yrityskumppanien suhteen

Ensiksikin yritysten on arvioitava, missä määrin niiden nykyiset sopimukset vastaavat uusia sääntöjä, ja mukauttaa sopimuksia tarvittaessa.

Tämä koskee tilaajasopimusehtojen ja Internet- ja sähköpostipalvelun tarjoajien lisäksi myös matkaviestintäpalvelujen tarjoajia. Lisäksi asiakkaille voitaisiin tarjota tietoa suodattimista ja suodatusohjelmistoista tai suodatuspalveluista lisäpalveluina (ks. myös kohta 4.3 jäljempänä). Myös yrityskumppanien kanssa tehtävissä sopimuksissa (esim. yhteenliittäminen matkaviestintäpalveluissa, lisäarvopalvelut) tulisi ottaa huomioon, että markkinointikäytäntöjen on oltava suostumussäännön mukaisia, ja määrätä riittävistä seuraamuksista rikkomistapausten varalta.

Suoramarkkinoijien omat käytännöt

Toiseksi voidaan joutua mukauttamaan suoramarkkinoijien käytäntöjä, jotta ne olisivat sopusoinnussa suostumussäännön kanssa. Suoramarkkinoijat voisivat etenkin sopia erityisistä uusien sääntöjen mukaisista keinoista, joita käytetään henkilötietojen keräämiseen (esim. ”toistettu” tai ”vahvistettu” suostumus).

Käytännösäännöt

Kolmanneksi toimialajärjestöt ovat jo ilmoittaneet eri aloitteista, kuten käytännesääntöjen mukauttamisesta tai käyttöönnotosta ja hyvien markkinointikäytäntöjen levittämisestä³⁵. Komissio tukee suoramarkkinoijille tarkoitettuja verkkotoiminnan käytännesäännöstöjä, joita sovellettaisiin koko Euroopan laajuudessa. Käytännesääntöjen ja muiden itsesääntelyaloitteiden sekä sopimusten on oltava suostumussäännön mukaisia. Toimivaltaisen sääntelyviranomaisen mukanaolosta voisi tässä olla apua. Tässä yhteydessä on hyvä muistaa, että direktiivin 95/46/EY 29 artiklalla perustettu tietosuojatyöryhmä voisi hyväksyä EU:n laajuiset käytännesäännöt (ks. ”yleisen” tietosuojadirektiivin 95/46/EY 30 artikla).

Kuten on usein asianlaita, itsesääntelyratkaisujen tehokas soveltaminen riippuu siitä, millä keinoin sovittujen sääntöjen noudattamista valvotaan, muun muassa mistä seuraamuksista on säädetty.

Merkinnät

Neljänneksi, jotta lisättäisiin tietoisuutta käyttäjien keskuudessa, voitaisiin käyttää merkintöjä (esim. luotettavuusmerkintöjä tai ”verkkosinettejä”) erityisesti silloin, kun luotetut kolmannet osapuolet valvovat ja varmentavat, että markkinatoimijat noudattavat käytännesääntöjä.

Näkyvät merkinnät voivat auttaa käyttäjiä tunnistamaan ne Internet- ja sähköpostipalveluntarjoajat ja muut markkinatoimijat, jotka noudattavat EU:n sääntöjä ja/tai tunnustettuja käytännesääntöjä, joilla EU:n säännöt pannaan täytäntöön. Ne voivat myös osaltaan tehostaa suodatusjärjestelmiä.

Myös suostumussäännön mukaiset käyttäjätietokannat on mahdollista varustaa merkinnöin, kuten myös suostumussäännön mukaiset sähköpostiviestit (esim. aihekentässä oleva merkintä ”ADV”, joka kertoo viestin sisältävän mainontaa).

Merkintöjen ansiosta vastaanottajat voisivat myös tunnistaa helposti kaupallisen viestinnän sähköistä kaupankäyntiä koskevan direktiivin mukaisesti (ks. direktiivin 2000/31/EY 6 artiklan a alakohta; ks. myös luku 2 edellä).

4.2. Vaihtoehtoiset riidanratkaisumenetelmät

4.2.1. Tämänhetkinen tilanne

Kun on kyse yksityisyyden loukkauksista, kuten ei-toivotun sähköpostin lähettämisestä, tuomioistuimen ulkopuolinen riidanratkaisu voi edistää uusien sääntöjen noudattamista. Kansallisella ja EU:n tasolla on käynnistetty useita aloitteita, joilla pyritään ottamaan käyttöön vaihtoehtoisia menetelmiä verkkoasiointiin ja –viestintään liittyvien riitojen ratkaisemiseksi. Komissio on antanut vuosina 1998 ja 2001 suositukset vaihtoehtoisista riidanratkaisumenetelmistä ja määrittänyt niiden periaatteet. Parhaillaan on käynnissä hankkeita (esim. EEJ-NET), jotka liittyvät kuluttajansuoja-alan vaihtoehtoiisiin riidanratkaisumalleihin³⁶. Myös sähköistä kaupankäyntiä koskevan direktiivin 17 artiklassa tuetaan tällaisten riidanratkaisumallien kehittämistä.

³⁵ Euroopan suoramarkkinointiliitto FEDMA on ilmoittanut julkaisevansa verkossa erityisen suoramarkkinoijille tarkoitetun käytännesäännöston.

³⁶ Lisätietoa: http://europa.eu.int/comm/consumers/redress/out_of_court/index_en.htm.

Tuomioistuinten ulkopuolisia riidanratkaisumenetelmiä – joissain tapauksissa lakisäätteisiä – on käytössä eräissä maissa. Ne voivat kuitenkin vaihdella monessa suhteessa, kuten soveltamisalan (toimintokohtainen, esim. suoramarkkinointi tai sähköpostimarkkinointi), lainkäyttövallan, toimivallan ja sanktioiden (esim. vahingonkorvausvaatimukset) tai vastuuviranomaisen suhteen (esim. tietosuojaviranomaiset, mainonnan normeista vastaavat viranomaiset).

Jotta vaihtoehtoiset riidanratkaisumallit olisivat riittävän toimivia, tiettyjen edellytysten on täyttyttävä liittyen esimerkiksi organisaatioon ja tiedottamiseen sekä päätösten täytäntöönpanoon. Tällaiset riidanratkaisumallit edellyttävät myös viranomaisten ja yritysten välistä yhteistyötä.

4.2.2. Ehdotetut toimet

Olisi pyrittävä luomaan ja ottamaan käyttöön toimivia itsesääntelyyn perustuvia valituskeinoja ja vaihtoehtoisia riidanratkaisumalleja. Niiden pitäisi mahdollisuuksien mukaan rakentua jo meneillään olevien hankkeiden pohjalle (esim. EEJ-NET). Tällaiset vaihtoehdot voivat olla erityisen hyödyllisiä tapauksissa, joissa kansainvälinen yhteistyö olisi vaikeampi toteuttaa.

4.3. Tekniset kysymykset

4.3.1. Tämänhetkinen tilanne

Roskapostin torjuntaan käytetään teknisellä rintamalla erilaisia ratkaisuja. Myös Internet-yhteisö (esim. RIPE, IETF) on tarttunut vakavasti roskapostiongelmaan³⁷. Pitemmän tähtäimen aloitteet, kuten sähköpostin uudet tekniset standardit, eivät kuulu tämän tiedonannon alaan. Internet- ja sähköpostipalveluntarjoajat estävät usein tulevan postin palvelimilta, joita käytetään roskapostin lähettämiseen (mustat listat), kunnes roskapostin lähde on saatu selville ja sitä estetään käyttämästä sähköpostipalvelinta. Lisäksi yksittäiset käyttäjät voivat käyttää suodatusohjelmistoja omissa päätelaitteissaan. Niitä voivat käyttää myös sähköisten viestintäpalvelujen tarjoajat omilla palvelimillaan.

Kaikki suodatusratkaisut ja –tekniikat eivät kuitenkaan tarjoa käyttäjälle yhtä hyviä sääntömahdollisuuksia. Ne eivät liioin tarjoa samoja takeita tietosuojasta ja yksityisyydestä, kuten viestinnän luottamuksellisuudesta. Ne eivät ehkä myöskään vielä sovellu uuteen suostumussääntöön, jota EU-maat soveltavat markkinointiviestintään (ennakkosuostumus saatava, liittyy markkinointiin, koskee sekä massapostituksia että muita viestejä). Mainittakoon myös, että tarkempi erottelu luvallisen (esim. suostumussäännön mukaisen) markkinoinnin ja ei-toivotun kaupallisen viestinnän välillä voi mahdollistaa tehokkaampien suodatusohjelmistojen kehittämisen.

Vaikka ei-toivottua kaupallista sähköpostiviestintää koskevat uudet säännökset tarjoavat lisätakeita käyttäjälle ja suuremman varmuuden palveluntarjoajille, kun ne ryhtyvät pyynnöstä toimiin roskapostin lähettäjiä vastaan, suodatus voi toisinaan estää luvallisten viestien perillepääsyn (”väärät osumat”) tai päästää läpi roskapostia (”väärät läpäisy”).

³⁷

Esim. roskapostiongelmaa käsittelevä RIPE:n (Réseaux IP Européens) työryhmä on ollut toiminnassa vuodesta 1998 (ks. asiakirja “Good Practice for combating Unsolicited Bulk Email”, saatavilla RIPE:n sivustolla (<http://www.ripe.net>). Sitten IRTF (Internet Research Task Force) on perustanut roskapostin torjuntaan keskittyvän tutkimustyöryhmän (<http://www.irtf.org/charters/asrg.html>). Tutkimustyöryhmä voi kehittää tekniikoita, jotka voivat tarjota lähtökohdan standardointitoimille IETF:ssä (Internet Engineering Task Force).

Joissain tapauksissa tämä voi johtaa riskiin, että joko lähettäjä tai aiottu vastaanottaja ryhtyy oikeustoimiin Internet- tai sähköpostipalvelun tarjoajaa vastaan. Siksi jotkut Internet- ja sähköpostipalvelujen tarjoajat tarjoavat käyttäjilleen suodatusta valinnaisena palveluna ja edellyttävät käyttäjän lupaa sen aktivoimiseksi.

Suodatustekniikoiden käyttö roskapostin torjumiseen nostaa esille myös muita kysymyksiä, joihin kuuluvat suodatus suhteessa sananvapauteen ja suodatus suhteessa Internet-/sähköpostipalvelun tarjoajan veloitteeseen toimittaa sähköpostiviestit tilaajiensa asiakkaille. Nämä kysymykset eivät kuitenkaan kuulu tämän tiedonannon alaan.

Matkaviestintäpalvelujen liiketoimintaympäristö poikkeaa kiinteän verkon Internet-palveluista, mikä voi olla peruste erilaisille suodatusratkaisuille. Erityisenä perusteena on se, että matkaviestintäpalveluista veloitetaan normaalisti viestikohtaisesti, mikä tekee roskapostin lähettämisestä kalliimpaa. Joissakin uusissa palveluissa veloitetaan kuitenkin viestin hausta omalle päätelaitteelle, mikä merkitsee kuluja vastaanottajalle. Lisäksi sähköpostia voidaan tätä nykyä toimittaa matkaviestimiin. Tilaajille voitaisiin tarjota suodattimia ja esikatselutoimintoja matkaviestinnän roskapostin hallitsemiseksi.

Huomiota kiinnitetään myös avoimiin kauttakulkupalvelimiin. Avoimet kauttakulkupalvelimet ovat SMTP-palvelimia, joiden kautta kulkevat muiden kuin palvelimen paikallisten käyttäjien viestit. Aiemmin useimmat palvelimet olivat avoimia. Avoimia palvelimia on kuitenkin helppo käyttää ei-toivotun viestinnän lähettämiseen. Yksinkertaiset estotoimet vähentäisivät mahdollisuuksia tällaiseen väärinkäyttöön. Sama pätee avoimiin proxy-palvelimiin, joilla toimivat ohjelmat mahdollistavat Internetin suoran käytön.

4.3.2. Ehdotetut toimet

Jäsenvaltioita ja viranomaisia pyydetään selkeyttämään maansa oikeudellisia olosuhteita (mm. yksityisyysvaatimukset), joissa erityyppisiä suodatusohjelmistoja voidaan käyttää.

Suodatusohjelmistojen tarjoajien on varmistettava, että niiden suodatusjärjestelmät ovat sellaisia kuin edellytetään suostumussäännössä ja muissa (mm. viestinnän luottamuksellisuuteen liittyvissä) EU-lain vaatimuksissa.

Käyttäjille tulisi antaa mahdollisuus hallita saamansa roskapostin käsittelyä omien yksilöllisten tarpeidensa mukaisesti. Suodatusohjelmistojen tarjoajien on otettava huomioon seuraukset, joita käyttäjille aiheutuu "vääristä osumista" ja "vääristä läpäisyistä" ja tietyn tyyppisestä sisältöön perustuvasta suodatuksesta, sekä asiaan mahdollisesti liittyvät vastuukysymykset.

Suodatuspalveluja tarjoavien yritysten tulisi yhdessä sidosryhmien kanssa kehittää tekniikoita (mm. verkkosinetit, merkinnät), joiden avulla voidaan tunnistaa EU:n hyväksyttävien markkinointikäytäntöjen mukaiset kaupalliset sähköpostiviestit

Sähköpostipalvelun (ja tarvittaessa matkaviestintäpalvelujen) tarjoajien pitäisi tarjota asiakkailleen suodatustoimintoja tai -palveluja valinnaisena palveluna, jota asiakas voi halutessaan pyytää, sekä tietoa loppukäyttäjien saatavilla olevista kolmansien osapuolten suodatuspalveluista ja -tuotteista.

Palvelinten ylläpitäjien tulisi varmistaa, että niiden palvelimet ovat kunnolla suojattuja eivätkä toimi avoimina palvelimina (ellei se ole perusteltua). Sama pätee avoimiin proxy-palvelimiin.

5. TIEDOTUSTOIMET

Tämän luvun toimenpide-ehdotukset liittyvät ennaltaehkäisyyn, kuluttajatiedotukseen ja raportointiin.

5.1. Tämänhetkinen tilanne

EU:n jäsenvaltioiden oli määrä sattaa uusi suostumukseen perustuva järjestelmä osaksi kansallista lainsäädäntöään viimeistään 31. lokakuuta 2003. Tämä uusi toimintamalli on saanut kohtalaisesti julkisuutta osakseen tiedotusvälineissä, mutta yritysten ja kansalaisten keskuudessa voi olla vielä epätietoisuutta siitä, mitä ”suostumukseen perustuva” tosiasiaa merkitsee käytännössä³⁸.

Uuden toimintamallin lähtökohtana on se periaate, että käyttäjä saa itse valita, haluaako hän ottaa vastaan kaupallisia viestejä vai ei. Jotta tämä toimisi käytännössä, käyttäjien on oltava selvillä perussäännöistä, joita ei-toivottuun viestintään sovelletaan, ja siitä, minne ongelmista raportoidaan.

³⁸

Taustatietoa ei-toivottuun viestintään sovellettavista direktiivin 2002/58/EY säännöistä: http://europa.eu.int/information_society/topics/ecommerce/all_about/todays_framework/privacy_protection/index_en.htm#unsolicited.

Parhaat käytännöt

Britannian tietosuojaviranomainen (Information Commissioner) julkaisi pari viikkoa ennen direktiivin kansallisten täytäntöönpanosäännösten voimaantuloa oppaan, jossa selitetään kansallisen lain uudet säännökset. Oppaassa on erillinen sähköistä markkinointia koskeva osa. Britannian tietosuojaviranomainen on myös ilmoittanut, että valituslomakkeet saa verkosta ja tietosuojaviranomaisen toimistoista tarvittavine tietoineen, kun säännökset astuvat voimaan³⁹.

Käyttäjien tulisi myös ymmärtää riskit, joita liittyy henkilötietojen antamiseen Internetissä (esim. vierailuilla Internet-sivuilla, keskusteluryhmissä), ja muuttaa käyttäytymistään vastaavasti.

Lisäksi heidän on tiedettävä, mitä suodatusohjelmistoja on markkinoilla ja mitä palvelujen ja ohjelmistojen tarjoajat (esim. Internet- ja sähköpostipalvelun tarjoajat) voivat tehdä heidän hyväkseen.

Parhaat käytännöt

Ranskan tietosuojaviranomainen CNIL (Commission National Informatique et Libertés) on julkaissut verkkosivuillaan laajan tietopaketin roskapostin eri näkökohdista. Tietopaketissa on muun muassa tulokset CNIL:n roskapostilaatikkaloitteesta ja oikeusviranomaisille siirretyistä asioista (ks. jäljempänä), perustietoa roskapostin torjumisesta ja roskapostista raportoisesta ja asiaa ajavien käyttäjäjärjestöjen yhteystiedot.

Useimmissa jäsenvaltioissa on meneillään tai suunnitteilla uuteen järjestelmään liittyviä tiedotustoimia, mutta ne vaihtelevat suuresti ajoituksen, tarjotun informaation luonteen, kohdeyleisön ja osallistujien suhteen. Osa jäsenvaltioista on puolestaan päättänyt odottaa, kunnes niiden omat lait ovat tulleet voimaan. Julkinen kuuleminen direktiivin 2002/58/EY täytäntöönpanosta on lisännyt tietoisuutta kaikissa tapauksissa, joissa sellainen on järjestetty.

Näistä toimista saattavat vastata eri viranomaiset (esim. tietosuojaviranomaiset, kansalliset sääntelyviranomaiset, kuluttajansuojaviranomaiset, kuluttaja-asiamiehet) riippuen niiden valtuuksista jäsenvaltiossa. Eri toimivaltaisten viranomaisten välillä ei (vielä) ole koordinoitua kaikissa jäsenvaltioissa. Eräissä jäsenvaltioissa ministeriöt näyttävät osallistuvan toimintaan, kuten myös useat toimialajärjestöt. Joskus myös kuluttaja- tai käyttäjäjärjestöt ovat mukana ko. toimissa.

Myös yritykset ovat ryhtyneet vaihtelevasti tiedotustoimiin kansallisesti, EU:n tasolla tai maailmanlaajuisesti. Näitä toimia ovat esimerkiksi:

- suoramarkkinoijille suunnatut käytännöt oppaat ja viestintäsektorille suunnatut kampanjat
- yleinen kuluttajavalistus käytäntesäännöistä, valituskeinoista ja suodatuksista
- kaupallisen viestinnän parhaita toimintatapoja kehittävät työryhmät.

39

http://www.dti.gov.uk/industries/ecomunications/directive_on_privacy_electronic_communications_200258ec.html#guidance

5.2. Ehdotetut toimet

Jotta päästäisiin hyvään selvyyteen siitä, miten kaupallisen sähköpostiviestin suhteen kannattaa menetellä ja miten ei, kaikissa jäsenvaltioissa on jo lyhyen ajan sisällä ryhdyttävä kattaviin ja pitkäjänteisiin toimiin, jotka liittyvät sekä ennaltaehkäisyyn että lainvalvontaan. Käyttäjille on tarjottava käytännön tietoa roskapostin ennaltatorjunnasta, hyväksyttävistä markkinointikäytännöistä ja käytettävissä olevista teknisistä ratkaisuista ja oikeuskeinoista.

Kaikkia sidosryhmiä - jäsenvaltioita ja viranomaisia sekä yrityksiä ja kuluttaja- ja käyttäjäjärjestöjä - pyydetään osallistumaan tiedotustoimiin. Niitä jäsenvaltioita ja viranomaisia, jotka eivät ole vielä ryhtyneet tällaisiin toimiin, pyydetään käynnistämään kampanjoita tai antamaan niille tukensa vuoden 2004 alussa.

Yrityksille ja/tai kuluttajille suunnatuissa tiedotustoimissa tulisi tarjota seuraavaa tietoa:

- tietoa, jolla varmistetaan, että uudet perussäännöt ja niihin mukanaan tuomat oikeudet ymmärretään laajalti
- käytännön tiedot suostumukseen perustuvan järjestelmän mukaisista hyväksyttävistä markkinointikäytännöistä, muun muassa siitä, mikä henkilötietojen keruu on luvallista
- käytännön tiedot kuluttajille tavoista, joilla roskapostia voi torjua (esim. henkilötietojen käyttöön liittyen)
- käytännön tiedot kuluttajille tuotteista ja palveluista, joita on saatavilla roskapostin torjumiseksi (esim. suodatus, tietoturvatoinnot)
- tietoa käytännön toimista roskapostin varalle, muun muassa valituskeinoista ja vaihtoehtoisista riidanratkaisumenetelmistä, kun tällaisia on.

Safer Internet -ohjelma ja roskaposti

Euroopan komissio on julkaissut Internetin käyttöturvallisuutta koskevassa *Safer Internet* -ohjelmassa ehdotuspyynnön, jolla haetaan erityyppisiä hankkeita (esim. tiedotus), joilla roskapostia voidaan torjua. Ensimmäisellä arviointikierroksella valitut hankkeet voivat aloittaa toukokuussa 2004.

Komissio laatii parhaillaan ehdotusta jatko-ohjelmaksi *Safer Internet Plus*. Siinä tuettaisiin lisää hankkeita, joilla torjutaan laitonta ja haitallista sekä tilaamatonta sisältöä, kuten roskapostia.

http://www.europa.eu.int/information_society/programmes/iap/call/index_en.htm

Tiedotustoimet tulisi suunnata seuraaville kohderyhmille:

- a) suoramarkkinointia harjoittavat tai hyödyntävät yritykset
- b) sähköpostipalvelujen, myös tekstiviestipalvelujen, tilaajat (kuluttajat)
- c) sähköpostipalvelujen, myös matkaviestintäpalvelujen, tarjoajat.

Tiedotus tulisi toteuttaa eri kanavien kautta (ei pelkästään verkossa) siten, että eri kohdeyleisöt saavutetaan tehokkaasti. Tämän kannalta on tärkeää, että mukana on toimiala- ja kuluttajajärjestöjä. Mahdollisten eri aloitteiden välillä on varmistettava koordinointi.

Tiedotuksen sisällössä pitäisi viitata käytössä oleviin yritysten käytännesääntöihin, valituskanaviin, merkintöihin (esim. luotettavuusmerkinnät) ja sertifiointijärjestelmiin, kun tällaisia on.

Komission yksiköt tarjoavat jo nyt EUROPA-sivustolla perustietoa suostumukseen perustuvasta järjestelmästä⁴⁰. Komissio aikoo linkittää nämä sivut kansallista täytäntöönpanoa koskeviin tietoihin sekä roskapostia ja sen kehityssuuntauksia koskeviin perustilastoihin (sikäli kuin käytettävissä). Komission yksiköt levittävät lisäksi tietoa uusista säännöistä euroneuvontakeskusten kautta.

PÄÄTELMÄT

Roskaposti on yksi Internetin tämän hetken merkittävimmistä haasteista. Roskapostiongelmiaan puuttuminen vaatii toimia eri rintamilla: tehokkaan lainvalvonnan ja kansainvälisen yhteistyön lisäksi tarvitaan itsesääntelyratkaisuja ja teknisiä ratkaisuja yrityksille sekä kuluttajavalistusta. Tässä tiedonannossa kuvatut toimet esitetään yhteenvedonomaaisesti taulukossa jäljempänä.

Komissio tukee toimia niin pitkälle kuin mahdollista, mutta toiminnasta vastaavat ensi kädessä EU:n jäsenvaltiot ja viranomaiset, yritykset, kuluttajat ja Internetin ja sähköisten viestintäpalvelujen käyttäjät kansallisesti ja kansainvälisesti.

Tässä tiedonannossa esitettyjen toimien – joilla on sidosryhmien laaja tuki – kokonaisvaltainen ja rinnakkainen toteutus voi vähentää merkittävästi roskapostia, joka uhkaa nykyisellään jo vähentää sähköpostin ja muun sähköisen viestinnän yhteiskunnalle ja taloudelle tuomia hyötyjä.

Komissio seuraa toteutusta vuoden 2004 aikana muun muassa ei-toivottua sähköpostiviestintää käsittelevän epävirallisen työryhmän kautta. Komissio arvioi viimeistään vuoden 2004 lopulla, tarvitaanko lisätoimia tai onko toimintaa tarkistettava.

40

http://europa.eu.int/information_society/topics/ecommerce/highlights/current_spotlights/spam/index_en.htm

TAULUKKO: YHTEENVETO TIEDONANNOSSA ESITETYISTÄ TOIMISTA

Seuraavassa taulukossa tehdään yhteenveto tiedonannossa kuvatuista toimista. Taulukossa mainitaan komission / komission yksiköiden toimet erikseen. Kuten edellä mainitaan, toimet liittyvät toisiinsa monin tavoin ja ne pitäisi toteuttaa mahdollisuuksien mukaan rinnakkain ja kokonaisvaltaisella tavalla.

I - Täytäntöönpano ja lainvalvonta jäsenvaltioiden ja viranomaisten toimesta

Ensimmäisenä edellytyksenä on, että jäsenvaltiot saattavat sähköisen viestinnän tietosuojadirektiivin ja erityisesti säännökset ei-toivotusta sähköpostiviestinnästä viipymättä osaksi kansallista lainsäädäntöään.

Jäsenvaltioiden ja viranomaisten pitäisi arvioida, miten tehokkaita niiden lainvalvontakeinot ovat. Näihin kuuluvat oikeuskeinot ja seuraamukset, valituskeinot, EU:n sisäinen yhteistyö, yhteistyö EU:n ulkopuolisten maiden kanssa ja seuranta. Jäsenvaltioiden pitäisi myös kehittää kansallisia strategioita, jotta voidaan taata yhteistyö tietosuojaviranomaisten, kuluttajansuojaviranomaisten ja kansallisten sääntelyviranomaisten välillä ja välttää turhaa päällekkäisyyttä.

Jäsenvaltioiden ja viranomaisten tulisi huolehtia erityisesti seuraavista:

a) Oikeuskeinot ja seuraamukset

- Olisi luotava riittävät mahdollisuudet hakea korvauksia ja otettava käyttöön todelliset sanktiot, tarvittaessa sakko- ja rikosoikeudelliset rangaistukset.
- Jäsenvaltioissa, joissa ei ole vielä käytössä hallinnollisia sanktioita, pitäisi harkita niiden käyttöönottoa keinona valvoa uusien sääntöjen soveltamista.
- Toimivaltaisille viranomaisille on annettava tarvittavat tutkinta- ja lainvalvontavaltuudet.

b) Valituskeinot

- Pitäisi ottaa käyttöön riittävät valituskeinot, muun muassa erityiset sähköpostilaatikat, joihin käyttäjät voivat osoittaa valitukset.
- Eri toimivaltaisten kansallisten viranomaisten välille on luotava koordinointi.

c) Rajatylittävät valitukset ja lainvalvontayhteistyö EU:ssa

– Tulisi hyödyntää olemassa olevaa yhteistyömekanismia (tai tarvittaessa luotava sellainen), jonka kautta kansalliset viranomaiset voivat harjoittaa yhteistyötä rajatylittävässä lainvalvonnassa EU:ssa (tiedonvaihto, keskinäinen avunanto). Tässä yhteydessä ja erityisesti vilpillistä ja harhaanjohtavaa roskapostia ajatellen neuvostoa ja Euroopan parlamenttia pyydetään sopimaan mahdollisimman pian kuluttajansuoja-alan yhteistyötä koskevasta asetusehdotuksesta sekä tutkimaan, missä määrin sähköisen viestinnän tietosuojadirektiivin kattamat kysymykset voitaisiin sisällyttää sen soveltamisalaan.

d) Yhteistyö EU:n ulkopuolisten maiden kanssa

- Monenvälisiin foorumeihin (esim. OECD) olisi osallistuttava aktiivisesti ratkaisujen löytämiseksi kansainvälisellä tasolla.
- EU:n ulkopuolisten maiden kanssa harjoitettavaa kahdenvälistä yhteistyötä olisi tehostettava tai tällainen yhteistyö olisi pantava alulle.
- Komission kanssa pitäisi tutkia, millä erityisillä toimilla se voisi helpottaa kansainvälistä yhteistyötä.
- Yksityisen sektorin kanssa pitäisi toimia yhteistyössä roskapostittajien jäljittämiseksi, kuitenkin rajoittamatta oikeusturvaa.

e) Seuranta

– Jäsenvaltioiden pitäisi varmistaa, että niillä on lainvalvonnan edellyttämät tiedot ja tilastot. Tässä tulisi tarvittaessa toimia yhteistyössä yritysten kanssa ja ottaa huomioon, että OECD:ssä on meneillään ei-toivotun sähköpostiviestinnän määrällinen arviointi.

II – Yritysten itsesääntely ja tekniset toimenpiteet

Yritysten (esim. Internet- ja sähköpostipalvelun tarjoajien, matkaviestintäoperaattorien, ohjelmistoyritysten, suoramarkkinoijien) tulisi pyrkiä tekemään ennakkosuostumusjärjestelmästä jokapäiväinen liiketoimintakäytäntö, tarvittaessa yhteistyössä kuluttaja- ja käyttäjäjärjestöjen ja viranomaisten kanssa. Erityisesti on kyse seuraavista:

a) Itsesääntely

– Palveluntarjoajien (Internet, sähköposti, matkaviestintä) tilaajilleen ja yrityskumppaneilleen tarjoamia sopimusehtoja pitäisi arvioida ja tarvittaessa muuttaa. Palveluntarjoajien pitäisi tarjota tietoa suodattuksesta sekä mahdollisesti suodatusohjelmistoja tai –palveluja valinnaisena asiakaspalveluna.

– Suoramarkkinointikäytäntöjä pitäisi muuttaa ennakkosuostumusjärjestelmän mukaisiksi ja mahdollisesti sopia erityisistä lainmukaisista menetelmistä, joita voidaan käyttää henkilötietojen keruussa (esim. ”toistettu” tai ”vahvistettu” suostumus).

– Pitäisi kehittää ja levittää ennakkosuostumussäännön mukaisia käytäntöjä (esim. FEDMA:n aloite) yhdessä direktiivin 95/46/EY 29 artiklalla perustetun tietosuojatyöryhmän tai toimivaltaisen kansallisen viranomaisen kanssa, tarpeen mukaan.

– Pitäisi harkita sellaisten merkintöjen käyttöä, jotka auttavat käyttäjiä (ja suodattimia) tunnistamaan ennakkosuostumussäännön mukaiset sähköpostiviestit ja tietokannat sähköistä kaupankäyntiä koskevan direktiivin mukaisesti.

– Toimivia itsesääntelyyn perustuvia valituskeinoja ja vaihtoehtoisia riidanratkaisumalleja olisi pyrittävä käyttämään tai tarvittaessa luomaan. Mahdollisuuksien mukaan pitäisi tukeutua jo meneillään oleviin hankkeisiin (esim. EEJ-NET).

d) Tekniset toimenpiteet

– Suodatusohjelmistojen tarjoajien on varmistettava, että niiden suodatusjärjestelmät ovat sellaisia kuin edellytetään suostumussäännössä ja muissa (mm. viestinnän luottamuksellisuuteen liittyvissä) EU-lain vaatimuksissa. Jäsenvaltioita ja viranomaisia pyydetään selkeyttämään maansa oikeudellisia olosuhteita (mm. yksityisyysvaatimukset), joissa erityyppisiä suodatusohjelmistoja voidaan käyttää.

– Suodatusohjelmistojen tarjoajien olisi otettava huomioon seuraukset, joita käyttäjille aiheutuu ”vääristä osumista” ja ”vääristä läpäisyistä” ja tietyn tyyppisestä sisältöön perustuvasta suodattuksesta, ja asiaan mahdollisesti liittyvät vastuukysymykset. Käyttäjille tulisi antaa mahdollisuus hallita saamansa roskapostin käsittelyä omien yksilöllisten tarpeidensa mukaisesti.

– Suodatuspalveluja tarjoavien yritysten pitäisi yhdessä sidosryhmien kanssa kehittää tekniikoita (mm. merkinnät), joiden avulla voidaan tunnistaa luvalliset (esim. EU:n hyväksyttävien markkinointikäytäntöjen mukaiset) kaupalliset sähköpostiviestit.

– Sähköpostipalvelun ja tarvittaessa matkaviestintäpalvelujen tarjoajien pitäisi tarjota asiakkailleen suodatustoimintoja tai –palveluja valinnaisena palveluna, jota asiakas voi halutessaan pyytää, sekä tietoa loppukäyttäjien saatavilla olevista kolmansien osapuolten suodatuspalveluista ja -tuotteista.

Palvelinten ylläpitäjien tulisi varmistaa, että niiden palvelimet ovat kunnolla suojattuja eivätkä toimi avoimina palvelimina (ellei se ole perusteltua). Sama pätee avoimiin proxy-palvelimiin.

III – Jäsenvaltioiden, yritysten ja kuluttaja- ja käyttäjäjärjestöjen tiedotustoimet

Niitä jäsenvaltioita ja viranomaisia, jotka eivät ole vielä ryhtyneet tiedotustoimiin, pyydetään käynnistämään kampanjoita tai antamaan niille tukensa vuoden 2004 alussa.

Kyse on käytännön tiedotuskampanjoista, joiden aiheina ovat roskapostin ennaltaehkäisy, hyväksyttävät markkinakäytännöt ja käyttäjien käytettävissä olevat tekniset ratkaisut ja oikeuskeinot. Niihin pyydetään osallistumaan kaikkia sidosryhmiä jäsenvaltioista ja viranomaisista aina yrityksiin ja kuluttaja- ja käyttäjäjärjestöihin. Tavoitteena on:

– suunnata kampanjat a) suoramarkkinointia harjoittaville tai hyödyntäville yrityksille, b) sähköpostipalvelujen, myös tekstiviestipalvelujen, tilaajille (kuluttajille) ja c) sähköpostipalvelujen, myös matkaviestintäpalvelujen, tarjoajille

– tarjota yrityksille ja/tai kuluttajille:

- tietoa, jolla varmistetaan, että uudet perussäännöt ja niiden mukanaan tuomat oikeudet ymmärretään laajalti

- käytännön tiedot suostumukseen perustuvan järjestelmän mukaisista hyväksyttävistä markkinointikäytännöistä, muun muassa siitä, mikä henkilötietojen keruu on luallista

- käytännön tiedot kuluttajille tavoista, joilla roskapostia voi torjua (esim. henkilötietojen käyttöön liittyen)

- käytännön tiedot kuluttajille tuotteista ja palveluista, joita on saatavilla roskapostin torjumiseksi (esim. suodatus, tietoturvatoinnot)

- informaatiota käytännön toimista roskapostin varalle, muun muassa valituskeinoista ja vaihtoehtoista riidanratkaisumenetelmistä, kun tällaisia on.

– viitata tiedotuksen sisällössä käytössä oleviin yritysten käytäntöihin, valituskanaviin, merkintöihin (esim. luotettavuusmerkinnät) ja sertifiointijärjestelmiin, kun tällaisia on

– toteuttaa nämä tiedotustoimet eri kanavien kautta (ei pelkästään verkossa) siten, että eri kohdeyleisöt saavutetaan tehokkaasti.

Tavoitteiden kannalta on tärkeää, että mukana on toimiala- ja kuluttajajärjestöjä. Mahdollisten eri aloitteiden välillä on varmistettava koordinointi.

IV – Komission / komission yksiköiden toimet

Komissio seuraa toteutusta vuoden 2004 aikana muun muassa ei-toivottua sähköpostiviestintää käsittelevän epävirallisen työryhmän kautta. Komissio arvioi viimeistään vuoden 2004 lopulla, tarvitaanko lisätoimia tai onko toimintaa tarkistettava.

Komissio seuraa direktiivin täytäntöönpanoa tiiviisti. Komissio aikoo erityisesti varmistua siitä, että direktiivin kansalliset täytäntöönpanotoimenpiteet sisältävät todellisia sanktioita (tarvittaessa sakko- ja rikosoikeudellisia seuraamuksia) siltä varalta, että vaatimuksia rikotaan. (Komissio käynnisti marraskuussa 2003 jäsenyysselvointeiden rikkomisesta johtuvan menettelyn niitä jäsenvaltioita vastaan, jotka eivät olleet ilmoittaneet komissiolle kansallisista täytäntöönpanotoimenpiteistä.) Komission yksiköt ovat tarvittaessa valmiita auttamaan jäsenvaltioita.

Komission yksiköt ovat jäsenvaltioiden ja tietosuojaviranomaisten tuella perustaneet ei-toivottua sähköpostiviestintää käsittelevän epävirallisen online-työryhmän. Työryhmän tehtävänä on helpottaa lainvalvontaa (esim. valitukset, oikeuskeinot, seuraamukset ja kansainvälinen yhteistyö) ja muuta tässä tiedonannossa esitettyihin toimiin liittyvää työtä.

Komission yksiköt pyytävät direktiivin 95/46/EY 29 artiklalla perustettua tietosuojatyöryhmää antamaan mahdollisimman pian lausunnon tietyistä sähköisen viestinnän tietosuojadirektiivissä käytetyistä ratkaisuista. Tavoitteena on edistää direktiivin kansallisten täytäntöönpanosäännösten yhdenmukaista soveltamista.

Komission yksiköt ovat alkaneet tutkia yhdessä jäsenvaltioiden ja kansallisten lainvalvontaviranomaisten kanssa, miten valtioiden rajat ylittävä lainvalvonta voitaisiin parhaiten järjestää EU:n sisällä ja EU:n ulkopuolisten maiden kanssa. Työtä jatketaan kansallisten viranomaisten kanssa kuluvan vuoden loppuun.

Komissio tukee suoramarkkinoijille tarkoitettuja verkkotoiminnan käytäntösäännöstöjä, joita sovelletaan koko Euroopan laajuudessa. Direktiivin 95/46/EY 29 artiklalla perustettua tietosuojatyöryhmä voisi tarpeen tullen toimia tahona, joka hyväksyy tällaiset säännöstyöt.

Komissio järjestää helmikuussa 2004 roskapostia käsittelevän OECD-tapaamisen ja aikoo keskustella jatkotoimista jäsenvaltioiden kanssa. Näihin kuuluvat OECD:n toimet, joilla edistetään tehokasta lainsäädäntöä kansainvälisesti, sekä tiedotus, tekniset ratkaisut, itsesääntely ja kansainvälinen lainvalvontayhteistyö.

Komissio aikoo myös tarkastella, mihin toimiin vuonna 2003 järjestetyn YK:n tietoyhteiskuntahuippukokouksen tulosten pohjalta pitäisi ryhtyä EU:ssa, ottaen huomioon, että Tunisian huippukokous järjestetään vuonna 2005.

Komissio on julkaissut Internetin käyttöturvallisuutta koskevassa *Safer Internet* -ohjelmassa ehdotuspyynnön, jolla haetaan roskapostin torjumiseen tähtääviä erityyppisiä hankkeita. Komissio laatii parhaillaan ehdotusta jatko-ohjelmaksi *Safer Internet Plus*. Siinä on määrä myöntää lisää rahoitusta muun muassa roskapostiongelman liittyville hankkeille.

Komission yksiköt tarjoavat myös jatkossa perustietoa suostukseen perustuvasta järjestelmästä EUROPA-sivustolla. Komissio aikoo linkittää nämä sivut kansallista täytäntöönpanoa koskeviin tietoihin sekä roskapostia ja sen kehityssuuntauksia koskeviin perustilastoihin (sikäli kuin käytettävissä). Komissio aikoo levittää lisäksi tietoa uusista säännöistä euroneuvontakeskusten kautta.