Max W. Mosing[1]

THE UPS AND DOWNS IN THE HISTORY OF EU-SPAM-REGULATIONS AND THEIR PRACTICAL IMPACT

> "*Two years from now, spam will be solved. I promise a spam-free world by 2006*"
> (Bill Gates; January 2004)

Table of content:

1. (Legal) History of Spam 1
1.1. „Monty Python"and „Canter and Seigel" 2
1.2. Definition of Spam from a Legal Perspective 2
1.3. Harm of Spam and– if the Internet community wants to ban spam – why is spam so successful? 3
1.4. Legal Framework and legal background of spam 4
2. "Spam-Regulations" in EU-Directives 6
2.1. Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector – ISDN-Directive and National Laws 7
2.1.1. Austria (opt-in-system) 7
2.2. Directive 97/7/EC on the protection of consumers in respect of distance contracts – Distance-Selling-Directive 7
2.3. Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') – E-Commerce-Directive 8
2.4. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) – E-Communication-Directive 9
2.5. Directive 2002/65/EC concerning the distance marketing of consumer financial services – Distance Selling Directive for Financial Services 11
2.6. Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market - 'Unfair Commercial Practices Directive' 12
3. Additional "Spam-Initiatives" of the EU 13
4. (Fighting) Spam in Legal Practice 22
4.1. Possibilities and Obstacles for Victims – in Austria 23
4.2. Spamming and Unfair Practices 25
4.2.1. Spamming, UWG and the Impact of the Procedural Law 26
4.3. Spam and Criminal Offence 29
5. Forecast 30
5.1. "Code and Other Laws of Spam" 30
5.2. The Limits of Code 31
5.3. International eMarketing Society – "Anti-Spam Inc." 31
6. Appendix ..... **Fehler! Textmarke nicht definiert.**

1. (Legal) History of Spam

> "*Hegel was right when he said that we learn from history that man can never learn anything from history.*" (George Bernard Shaw)

Unsolicited or Junk Electronic Mail – "[…] *spam* […] *THAT evil*"[2] on the Internet is a very good example for difficulties from learning from the past. Wherever there is evil

---

[1] Dr. iur, LLM (Vienna), LLM (Strathclyde, UK); Austrian Attorney at Law in the firm GASSAUER FLEISSNER RECHTSANWÄLTE GMBH, Vienna; member of the Austrian society for Information Technology Law - IT-LAW.AT; CV: http://www.gassauer.at/en/pdetail/650/.

there are media, politicians and lawyers trying to ban it – so there have been constant efforts to ban spamming. On the other hand, where evil is, there is a huge amount of money (to make) and (therefore) power involved and "money" and "power" are not totally unfamiliar terms to media, politicians and lawyers.

History shows that the run for "money" and "power" is the main issue for nearly every conflict – so also regarding spam, although everything started "rather funny":

1.1. „Monty Python"and „Canter and Seigel"

"SPAM" is a trademark for a canned meat product from Hormel Foods.[3] In a sketch of *Monty Python's Flying Circus*, a British comedy TV-show, the word "spam" is repeated to the point of absurdity in a restaurant menu. It is said that this sketch inspired a user from the MUD/MUSH[4]-community to assign a keyboard macro to the line, "SPAM SPAM SPAM …" and to send it to the MUD once every couple of seconds – and "spamming" was born.[5] A less moving interpretation is that spam could stand for "send phenomenal amounts of mail".

In any case, the first commercial spam was sent – funny enough – by a US husband-and-wife firm of lawyers, *Lawrence Canter* and *Martha Siegel*, on April 12, 1994:[6] they posted identical "green card"-advertisements to every newsgroup they could locate. The Internet community fought back: hackers tried to knock down their server and angry newsgroup-members attacked their e-mail-server with hundreds of senseless e-mails,[7] a measure called "flaming".[8] However, to many people, this spam, coming not long after the National Science Foundation lifted its unofficial ban on commercial speech on the Internet, marks the end of the Net's early period, when the original Netiquette could still be enforced.

Soon the Internet-community shouted for laws against spam - – or were the media, the politicians or even the lawyers shouting?!

But what is spam?

1.2. Definition of Spam from a Legal Perspective

Spamming is the abuse of electronic messaging systems to send unsolicited bulk messages, which are generally undesired.[9] While the most widely recognized form of spam is email spam, the term is applied to similar abuses in other media: instant messaging

---

[2] Commentator on slashdot.org, cited in *Michael Jacobs / David Naylor / Megan Auchincloss / David Melaugh*, "Spam Wars", IT Law Today (ITLT) 2002, 10.4 (19).
[3] Http://www.spam.com/ (05/2007).
[4] See for further information http://en.wikipedia.org/wiki/MUSH (05/2007).
[5] *W.K. Khong*, "Spam Law for the Internet", http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_3/khong/ (05/2007).
[6] http://en.wikipedia.org/wiki/Canter_&_Siegel (05/2007).
[7] *W.K. Khong*, "Spam Law for the Internet", http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_3/khong/ (05/2007).
[8] *Lilian Edwards*, "Canning the Spam: Is There a Case for Legal Control of Junk Electronic Mail?", http://www.law.ed.ac.uk/script/newscript/spam.htm (05/2007).
[9] Comp http://en.wikipedia.org/wiki/Spam_%28electronic%29 (05/2007).

spam, Usenet newsgroup spam, web search engine spam, spam in blogs, mobile phone messaging spam, internet forum spam and junk fax transmissions.

Therefore, "spam" is the umbrella term for[10]

- unsolicited commercial electronic material (UCEM) and
- unsolicited bulk electronic material (UBEM).

The difference of the terms makes no big difference in the annoyance of the recipient and the traffic on the Internet but could have an effect on the legal evaluation (see – also to the legal definitions – below).

One important dimension of spam has to be stressed at this point: spam refers to the method of sending unsolicited material with the help of communication networks and does **not** refer to the (legal or illegal) content of the material; although the content can lead to legal consequences – however irrespectively if this content was sent by electronic mail or normal mail: comp scam, fraud, racism, and other illegal matters). This distinction between method and content follows the communication theory dividing a communication system into three distinct layers:[11] At the bottom the "physical layer" (wires and hardware); in the middle the "logical/code layer" which makes the hardware run (here named as "method"); and on the top the "content layer", the actual content that is transmitted. Spamming is an issue of the "logical/code layer" and only secondarily an issue of the "content layer".

1.3. Harm of Spam and– if the Internet community wants to ban spam – why is spam so successful?

As mentioned above, spamming is not only an issue of e-mails; nevertheless, at the moment spam-e-mails cause the biggest costs and annoyance. The reason for these issues has its origin in the technology used for e-mails: the Simple Mail Transfer Protocol (SMTP), the standard protocol on the Internet for sending e-mails, enables that one e-mail can be sent to an infinite number of recipients and the protocol does not require a valid address to authenticate the sender – why this is the case cannot be answered by a lawyer; however, Spammers could argue that they are just using an infrastructure which technically enables their behaviour, or with other words: if you do not like it – change it.

The history of the Internet is stamped by self-regulation.[12] So it could be argued that (at least) the Internet-community could regulate spamming with technological measures (e.g. no anonymous e-mail; not more than 5 recipients per e-mail and so on). But these measures would limit the usability of the whole e-mail-system because of "some spammers": "A belief that, to date, technology, self-regulatory efforts and case-by-case

---

[10] *Lilian Edwards*, "Canning the Spam: Is There a Case for Legal Control of Junk Electronic Mail?", http://www.law.ed.ac.uk/script/newscript/spam.htm (05/2007).
[11] Comp *Lessig Lawrence*, The Future of Ideas (2002) 23 et sqq.
[12] Comp Request for Comments. The document series, begun in 1969, which describes the Internet suite of protocols and related experiments. Not all (in fact very few) RFCs describe Internet standards, but all Internet standards are written up as RFCs.

legal action have had a limited impact on unsolicited commercial email."[13] Furthermore, one argument convinces why spamming cannot be a case of self-regulation: it is a political decision if spamming shall be forbidden but nearly all self-regulatory-systems handle (only) technological issues and the competent organisation for such a decision would be unclear.[14]

Spamming is economically viable, because advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high. The costs, such as lost productivity and fraud, are borne by the public and by Internet service providers, which have been forced to add extra capacity to cope with the deluge. As the reader knows, a high percentage of the daily e-mail-traffic is caused by spam and the consequences are costs and annoyance on different levels:

- The recipient has to face download-costs, storage-costs and the risk of being unreachable because of full storage-space on his account, and the loss of time because of reading and deleting the spam-message;
- the ISP of the recipient has to bear the costs of storage (until the message is deleted on the server) and traffic of the message and has to spend time to handle customer's complaints and could even lose annoyed subscribers;
- ISPs who have to transport the messages through the network(s) have to bear these costs; and
- the community of users is annoyed and even has to face damages, because the efficiency and speed of the Internet is threatened.

However, there are also pro-spam-arguments: electronic direct marketing causes no pollution – in contrast to direct marketing by mail or leaflet; and it offers the possibility for new companies to enter the market with less market forces and costs, so that the benefit of the (national) economy prevails the damages that are caused. Finally, spammers could bring forward that regulations against spamming would be anyway senseless measures, because it is not possible to enforce them globally and therefore, they would just change their place of business and carry on.

1.4. Legal Framework and legal background of spam

Spammers often refer to their freedom of expression – this is in the author's opinion a legal "bubble": although even advertisement is protected by the freedom of expression,[15] in the case of spamming the freedom of expression (Art 10 European Convention on Human Rights' (ECHR)) is in conflict with the right to respect for private and family life (Art 8 ECHR) and the property of the recipient. Although there are relevant ques-

---

[13] Report to the Federal Trade Commission of the Ad-Hoc Working Group on Unsolicited Commercial Email, www.cdt.org/spam (5/2007).
[14] Comp the competence of the ICANN: www.icann.org (5/2007).
[15] Comp Europ Court of Human Rights, Markt Intern and Beermann v. Germany (1989), http://www.echr.coe.int/ (5/2007).

tions in connection with eg political and religious (spam)messages, there is no good argument, why purely commercial spam shall not be regulated or even banned.

Before the EU-Regulations on spamming are investigated in detail, it is necessary to reflect on what kind of rules and prohibitions are generally possible:

- Total prohibition: Spamming is illegal (as long as there is no ground of justification).
- "Explicit opt-in-system": Spamming is prohibited as long as there is no explicit consent of the recipient before the first spam is sent (the spammer has even to check if the consent is really given from the recipient; called "double-opt-in").
- "Opt-in-system": Spamming is illegal as long as there is no (implicit) consent.
- "first-free-system": The spammer can ask for the consent by sending the recipient a message and only if the consent is given spamming is allowed.
- "Implicit first-free-system": The spammer can ask for the consent by sending the recipient a message and if the recipient does not object, spamming is allowed.
- "register opt-out-system": Spamming is allowed as long as the recipient has not put his name on an (official) opt-out-register.
- "opt-out-system": Spamming is allowed as long as the recipient has not objected to the individually sender.
- Spamming is totally legal.

Regarding the "legal framework" respectively "legal background" the Recitals of the Directives are often providing a closer look on the thoughts of the lawmakers:

Recital 30 of the **E-Commerce-Directive** states: The sending of unsolicited commercial communications by electronic mail may be undesirable for consumers and information society service providers and may disrupt the smooth functioning of interactive networks; in Member States which authorise unsolicited commercial communications by electronic mail, the setting up of appropriate industry filtering initiatives should be encouraged and facilitated; in addition it is necessary that in any event unsolicited commercial communities are clearly identifiable as such in order to improve transparency and to facilitate the functioning of such industry initiatives; unsolicited commercial communications by electronic mail should not result in additional communication costs for the recipient.

Recital 40 of the **E-Communications-Directive** reads as follows: Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient. Moreover, in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment. For such forms of unsolicited communications for direct marketing, it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them. The single market requires a har-

monised approach to ensure simple, Community-wide rules for businesses and users. (41) Within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details for the offering of similar products or services, but only by the same company that has obtained the electronic contact details. When electronic contact details are obtained, the customer should be informed about their further use for direct marketing in a clear and distinct manner, and be given the opportunity to refuse such usage. This opportunity should continue to be offered with each subsequent direct marketing message, free of charge, except for any costs for the transmission of this refusal. (42) Other forms of direct marketing that are more costly for the sender and impose no financial costs on subscribers and users, such as person-to-person voice telephony calls, may justify the maintenance of a system giving subscribers or users the possibility to indicate that they do not want to receive such calls. Nevertheless, in order not to decrease existing levels of privacy protection, Member States should be entitled to uphold national systems, only allowing such calls to subscribers and users who have given their prior consent.

(43) To facilitate effective enforcement of Community rules on unsolicited messages for direct marketing, it is necessary to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes.

(44) Certain electronic mail systems allow subscribers to view the sender and subject line of an electronic mail, and also to delete the message, without having to download the rest of the electronic mail's content or any attachments, thereby reducing costs which could arise from downloading unsolicited electronic mails or attachments. These arrangements may continue to be useful in certain cases as an additional tool to the general obligations established in this Directive.

2. "Spam-Regulations" in EU-Directives

The EU – bearing the above (more or less) in mind – has dealt in not less than six Directives with the issue of direct marketing by the use of (tele)communication infrastructure (comp the above-named layer-model). Because the notion "consent" is so important in the above-listed possibilities of regulation, it is necessary to define it: Art 2 lit h Data Protection Directive[16] stipulates:

> *"the 'data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."*

This definition has to be borne in mind also for all technical solutions "allowing" spam – especially when "double-opt-in" is needed.

---

[16] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal 1995 L 281, 31.

2.1. Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector – ISDN-Directive and National Laws

The ISDN[17]-Directive (or Telecommunications Privacy Directive)[18] provides in its Art 12 that

> *"1. The use of automated calling systems without human intervention (automatic calling machine) or facsimile machines (fax) for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent. […]"*

Although the definition of spam and electronic mail is quite wide, only the spamming-method with facsimile machines (fax) for the purpose of direct marketing can be subsumed under Art 12 ISDN-Directive. Thus, the Directive regulates a method of the first case of the umbrella term spamming: using the fax for the purpose of sending unsolicited commercial material (UCM). E-mail-spamming cannot be subsumed under this Article as the aim is to regulate "standard telecommunication" by voice or fax.[19]

So the Directive determines an "opt-in-system" for fax-spamming. For the interpretation of the consent the definition of the (older) Data Protection Directive must be consulted; an explicit consent is not necessary (an implicit is enough) but it has to be an informed consent.

The Directive determines only a minimum standard for the protection of the subscriber (not the user). Some states have thus enacted national laws which have a wider protection than the Directive (and the following Directives). Here are some examples of laws influenced by the ISDN-Directive; please note that they are not in force anymore:

2.1.1. Austria (opt-in-system)

Sec 101 Telecommunications Law stipulated:

> *"[...] Sending of email in bulk or for advertising purposes requires the prior - revocable at any time - consent of the recipient."*

2.2. Directive 97/7/EC on the protection of consumers in respect of distance contracts – Distance-Selling-Directive

Art 10 of the Distance Selling Directive[20] nearly repeats the wording of the ISDN-Directive:

> *"Restrictions on the use of certain means of distance communication:*

---

[17] ISDN = Integrated Services Digital Network.

[18] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector Official Journal 1998 L 24, 1.

[19] Of another opinion: *W.K. Khong*, "Spam Law for the Internet", http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_3/khong/ (05/2007).

[20] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance, Official Journal 1997 L 144, 19.

1. Use by a supplier of the following means requires the prior consent of the consumer:

- automated calling system without human intervention (automatic calling machine),

- facsimile machine (fax).

2. Member States shall ensure that means of distance communication, other than those referred to in paragraph 1, which allow individual communications may be used only where there is no clear objection from the consumer."

The Directive affirms the opt-in-system for fax-spamming – for other spamming-methods the Directive determines at least an opt-out-system ("clear objection"). Although only consumers are in the scope of protection of the Directive, it is again a minimum standard; so Member-States can pass acts with wider protection (Art 14 of the Directive).

2.3. Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') – E-Commerce-Directive

Article 7 of the E-Commerce Directive leaded to big confusion in connection with the spam-regulations and the aims of the EU-legislator:

"Unsolicited commercial communication

1. In addition to other requirements established by Community law, Member States which permit unsolicited commercial communication by electronic mail shall ensure that such commercial communication by a service provider established in their territory shall be identifiable clearly and unambiguously as such as soon as it is received by the recipient.

2. Without prejudice to Directive 97/7/EC and Directive 97/66/EC, Member States shall take measures to ensure that service providers undertaking unsolicited commercial communications by electronic mail consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves."

One of the most important parts is "*Member States which permit unsolicited commercial communication by electronic mail"*, because of this wording the Member States are still free to choose their own system handling spamming as long as they fulfil the minimum standard, namely a "register opt-out-system" for natural persons. The notion "unsolicited commercial communication" implies that only spam has to be labelled but not electronic mails that are sent with the consent of the recipient.

Again the Directive determines a minimum standard but *prima facie* the "country of origin principle" (Art 3, 2 of the Directive) seems to start a race to the bottom for regulations, because spammers could go to an EU-Member-State with no spam-laws and send the electronic mails from there. But as the Annex of the Directive determines,

Art 3 does not apply to "*the permissibility of unsolicited commercial communications by electronic mail*". Consequently, every spammer has to mind – depending on the wording of the individual national law[21] - the laws of the state, where he sends his mails to **and** (maybe) of the state of his domicile.

The "register opt-out-system" – so-called "Robinson-list" – was subject to a lot of criticisms:[22] It was especially unclear who has to bear the costs and when and how often spammers have to check the register. Furthermore, it was argued that the register with the e-mail-addresses could be used by spammers who do not care about any laws to collect new e-mail-addresses.

Although an obligatory labelling could help filter-system to handle spam, the imprecise terms of the Directive lead to no solution: How does the label have to look like? Has it to be in the subject line of e-mails (what about text messages to mobile phones?)? A more functional wording has e.g. the California Business & Professions Code §17538.4[23] which determines that

> *"[…] the subject line of each and every message shall include "ADV:" as the first four characters […]".*

In some national law systems the obligation to label follows already from the unfair competition law and its' principle of transparency (e.g. Sec 1 of the German and Sec 1 of the Austrian Unfair Competition Act).

2.4. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) – E-Communication-Directive

The E-Communication Directive[24] defined "electronic mail" in its Art 2 as follows:

> *"'electronic mail' means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient."*

The E-Communication Directive determined in its Art 13 under the title "*Unsolicited communications*" for the first time an opt-in-system (with exceptions) for all spam for the purpose of direct marketing:

> *"1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.*

---

[21] Depends if it is forbidden to send spam or to reach sb with spam.
[22] Cp Khong, http://warwick.ac.uk/jilt/01-3/khong.html.
[23] Http://www.spambrigade.com/word/California1.doc (1/10/2003).
[24] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 2002/201, 37.

2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

3. Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.

4. In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.

5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected."

The biggest achievement of the Directive was without any question the EU-wide uniformity of spam-regulation and the technical neutral wording (comp the above-named definitions), which made the regulation applicable to many upcoming spam-methods (e.g. UMTS[25], MMS[26]).

This Directive seemed to be the EU-wide solution for spam – the good seemed to have won over the evil; but the Directive raised some (new) legal issues and changed very few in the practice of spam:

- The Directive applies "only" on "electronic mail for the purposes of direct marketing" and not on unsolicited non-commercial bulk material (UNBM). Although the practical relevance of this kind of spam is not immense, some states prohibit it (e.g. Austria). So there is no uniform regulation for UNBM across the EU-Member-States.

- Article 13 para 2 of the Directive determines that in the context of the sale of a product or a service spamming is allowed for own similar products or services if the customer has been given clearly and distinctly the opportunity to object when the (address-)data are collected and on the occasion of each message. It seems that

[25] Universal Mobile Telecommunications System: The third generation (3G) of mobile phones.
[26] Multimedia Messaging Service (MMS).

this leads to an opt-out-system if there is a contract between the spammer and the recipient. But in the author's point of view it is just an "unfortunate wording": As mentioned above the use of address-data for spamming needs in most cases the consent of the recipient (according to the Data Protection Directive). The definition of "consent" in the same Directive needs no explicit declaration of intention, but the freely given specific and informed indication of the wishes. Recital 41 of the E-Communication Directive states that "[when] electronic contact details are obtained, the customer should be informed about their further use for direct marketing in a clear and distinct manner, and be given the opportunity to refuse such usage." So the customer has to be informed and has the free possibility to object (as a freely given indication of his wishes): So he gives his (implicit) consent by ignoring the opportunity to refuse – para 1 can be applied. In the author's point of view para 2 is only needed if there are Member-States where an implicit declaration of intention is legally not possible.

- Even if there are cases where para 2 can be applied, it is unclear what similar "products or services" are: Is a book from amazon about IT-law similar to a tourist guide? A mobile phone similar to a computer?

- And finally, the Directive does not provide uniform enforcement measures.

2.5. Directive 2002/65/EC concerning the distance marketing of consumer financial services – Distance Selling Directive for Financial Services

A Directive dealing with the Distance Selling Directive for Financial Services[27] includes also regulations on spam; this because the Financial Services are excluded from the above cited "normal" Distance Selling Directive.

Art 10 of the Directive reads as follows:

> *"Unsolicited communications*
>
> *1. The use by a supplier of the following distance communication techniques shall require the consumer's prior consent:*
>
> *(a) automated calling systems without human intervention (automatic calling machines);*
>
> *(b) fax machines.*
>
> *2. Member States shall ensure that means of distance communication other than those referred to in paragraph 1, when they allow individual communications:*
>
> *(a) shall not be authorised unless the consent of the consumers concerned has been obtained, or*

[27] Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC, Official Journal L 2002/271, 16.

(b) may only be used if the consumer has not expressed his manifest objection.

3. The measures referred to in paragraphs 1 and 2 shall not entail costs for consumers."

It seems that the lobby of the financial service providers was strong enough to change the E-Communication Directive in the sector of financial services: according to the Directive it is up to the Member-States to determine an opt-in or an opt-out-system for spamming (UCM) with the exception of fax-spamming where an opt-in-system is obligatory. This raises some (new) issues:

- Can this Directive change the general regulation of the E-Communication Directive which is also applicable on financial services?

- The scope of the Directive is consumer-protection; what about businesses – can they be spammed by suppliers? In the author's point of view they cannot be – comp Recital 26 of the Directive:

  "Member States should take appropriate measures to protect effectively consumers who do not wish to be contacted through certain means of communication or at certain times. This Directive should be without prejudice to the particular safeguards available to consumers under Community legislation concerning the protection of personal data and privacy".

2.6. Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market - 'Unfair Commercial Practices Directive'

Pursuant to Art 5 para 5 of the Unfair Commercial Practice Directive[28] Annex I of the Directive contains the list of those commercial practices which shall in all circumstances be regarded as unfair and therefore forbidden; the same single list shall apply in all Member States and may only be modified by revision of this Directive.

Annex I No 26 reads as follows:

"26. Making persistent and unwanted solicitations by telephone, fax, e-mail or other remote media except in circumstances and to the extent justified under national law to enforce a contractual obligation. This is without prejudice to Article 10 of Directive 97/7/EC and Directives 95/46/EC [2] and 2002/58/EC."

Pursuant to Art 19 of the Directive Member States shall adopt and publish the laws, regulations and administrative provisions necessary to comply with this Directive by 12 June 2007.

---

[28] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (Text with EEA relevance), Official Journal L 2005/149, 22.

3. Additional "Spam-Initiatives" of the EU

The EU-Commission published in 2004 a communication on unsolicited commercial communications or 'spam',[29] reading as follows:

- Unsolicited commercial communications by e-mail, otherwise known as 'spam' have reached worrying proportions. More than 50 percent of global e-mail traffic is now estimated to be spam. What is even more worrying is the rate of growth: in 2001 the figure was 'only' 7 percent.

- There is however no 'silver bullet' for addressing spam.

- Spam has reached a point where it also creates considerable cost for businesses. In terms of direct costs, employees also have to clean up inboxes, thereby undermining efficiency/productivity at work. IT departments spend time and money trying to address the problem. Internet Service Providers (ISPs) and e-mail service providers (ESPs) have to buy more bandwidth and more storage capacity for e-mails that are unwanted. There is also a risk that spam prompts liability for the entity receiving it (e.g., harmful content on employee's PCs) or simply - and unwittingly - relaying it (e.g., wrong blacklisting, damage to reputation). There are also indirect costs: some legitimate commercial or business emails are not delivered due to current anti-spam filtering techniques (so-called 'false positives'), or simply not read anymore due to their association with spam. Spam is increasingly used as a vehicle for spreading viruses, which can prove very costly to businesses.

- In short, Member States must ensure that penalties and remedies are in place for infringements. An individual right to a judicial remedy must be provided for any breach of the rights provided under national law. While this judicial remedy is without prejudice to any (possibly prior) administrative procedures, there is no harmonised requirement to provide for such administrative procedures. There must be an individual right to a compensation for any damage suffered as a result of any unlawful processing or act. There must be sanctions to be imposed in case of infringements, which ensure full implementation of the Directive.

- Not all Member States have judicial sanctions in place for infringements. Not all Member States provide for remedies and fines/penalties under administrative law, or under criminal law. Criminal sanctions vary, including terms of imprisonment in certain Member States. In addition, there is generally the possibility to claim damages under civil law.

- Compared to judicial remedies, administrative sanctions seem to be particularly adequate for such a dynamic sector.

---

[29] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on unsolicited commercial communications or 'spam' (Text with EEA relevance) COM/2004/0028 final.

- As a consequence, Article 13 of Directive 2002/58/EC establishing the opt-in rule is applicable to all unsolicited commercial communications received on and sent from networks in the EU (and EEA). This implies that such messages originating in third countries must also comply with EU rules, as must messages originating in the EU and sent to addressees in third countries.

- The first objective of international co-operation is to promote the adoption of effective legislation in third countries. The second objective is to cooperate with third countries to ensure effective enforcement of the applicable rules. There is not much experience on enforcement of existing opt-in or opt-out rules for communications originating outside the EU. Besides the fact that spam is a relatively new phenomenon, obstacles often singled out include the difficulty of identifying the senders of such spam or the amount of effort required to do so; the lack of (appropriate) international co-operation mechanisms; and the lack of jurisdiction of some authorities on international matters.

- Contracts can help in the fight against spam, subject to safeguards with respect to individual rights. Many internet service providers (ISPs) and e-mail service providers (ESPs) already include obligations in contracts with their customers prohibiting the use of their services for sending spam. Such ISPs and ESPs already prohibit the sending of unsolicited e-mail, or bulk e-mail, from their e-mail accounts. Such clauses are sometimes based on the need to take all measures to prevent inappropriate usage of their services. Other refer to existing codes of conduct regarding bulk e-mails or, indeed, to self-regulatory principles (e.g. 'netiquette'). The concepts as used in previous contracts between ISPs and their customers are likely to be different from those used in the new Directive and subsequent national transposition law.

- In terms of customer service, there is also a need for a more pro-active filtering policy by providing information on anti-spam filters, and by providing filtering services or facilities to subscribers as an option. The same is valid whenever ISPs or mobile operators enter into contracts with third parties and in particular with direct marketeers.

- Various initiatives have already been announced by industry associations such as the adaptation or adoption of codes of conduct and the dissemination of good marketing practices. Europe-wide online codes of conduct for direct marketing will be supported by the Commission. Codes of conduct and other self-regulatory initiatives, and contracts must conform to the opt-in rules. Involvement of the competent regulatory authority could be helpful in this regard. It should be recalled in that context that the Article 29 Data Protection Working Party can approve EU-wide codes of conduct (see Article 30 of the 'general' Data Protection Directive 95/46/EC). The European Federation of Direct Marketing (FEDMA) has announced a specific online code of conduct for direct marketeers. As is often the case, effective application of self-regulatory solutions will depend on the structure put in place to oversee respect for the agreed rules, including effective sanctions.

- However not all filtering practices and techniques offer the same level of user control. Nor do they offer the same guarantees for data protection and privacy, such as respect for the confidentiality of communications. While the new legal provisions on unsolicited commercial e-mail provide additional safeguards for the user and greater security for service providers to undertake action on request against 'spammers', filtering may occasionally block legitimate e-mail ('false positive') or allow spam to get through ('false negatives'). In some cases, this can create a risk that either a sender or an intended addressee undertakes legal action against an ISP/ESP. Although it is beyond the scope of this Communication to address them, other issues, such as filtering versus freedom of expression and filtering versus the contractual obligation of ISPs/ESPs to transmit email messages to their clients' customers, are also presented by the use of filtering techniques to combat spam. Filtering companies should cooperate with interested parties to develop techniques recognising marketing e-mails corresponding to accepted marketing practices under Community law, including webseals, labels, etc.

- Out-of court redress mechanisms exist in some countries, sometimes established by legislation, though they vary in many respects, such as origin (branch-specific e.g., direct marketing, e-mail marketing), 'jurisdiction', powers and sanctions (e.g., damage claims), involvement of specific authorities (e.g., DPAs, advertising standards bodies) etc.

The Committee of the Regions commented on the Communication from the Commission[30] that it regrets that the Commission does not recognise the ability of regional and local authorities to interface with their communities and the public at large and urges the Commission to take proper account of how much assistance regional and local authorities can give in combating unsolicited mail; and proposes that efforts should be made to secure a greater commitment on the part of the main world software manufacturers to undertake research on network and information safety and its immediate practical application. Security should be a priority issue among the telecommunications service and access providers operating in Europe, and more links to activities and organisations outside the EU should also be developed.

However, the Commission had to publish in November 2006 another Communication on fighting spam, spyware and malicious software, reading as follows:[31]

- Society is becoming more and more aware of how essential modern electronic communications networks and services are for everyday life, in business or at home. A wide take-up of services depends on trustworthy, secure and reliable technologies.

---

[30] Opinion of the Committee of the Regions on the 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on unsolicited commercial communications or "spam"' Official Journal C 2004/318, 24.

[31] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on fighting spam, spyware and malicious software, COM/2006/0688 final.

- Spam has grown significantly over the last 5 years. Industry sources report that spam now accounts for 50-80% of messages addressed to end-users. Although the biggest portion of spam originates from outside the EU, European countries now account for 25% of relayed spam messages. The worldwide cost of spam has been estimated at € 39 billion in 2005. Spam costs to major European economies have been estimated to be around respectively € 3,5 billion – Germany, € 1,9 billion – United Kingdom and € 1,4 billion - France. Spamming is considered a 'business' of its own. Spammers rent or sell lists of harvested e-mail addresses to companies for marketing purposes. Spam over the internet is especially lucrative. This has to do with the reach of the medium and the low costs involved in sending massive amounts of messages. At the same time moderate investments to fight spam can also deliver significant results. As an example, in the Netherlands an 85% reduction in Dutch spam was achieved by investing € 570,000 in equipment to fight spam.

- The UN World Summit on the Information Society recognised that spam should be dealt with at appropriate national and international levels. WSIS thematic conferences have been held by the ITU in 2004 and 2005. The WSIS Tunis Agenda adopted in November 2005 calls to deal effectively with the significant and growing problem posed by spam.

- Spam is a cross-border issue, and several cooperation initiatives and cross-border enforcement mechanisms have been put in place. The Commission has set up a Contact Network of Spam Authorities (CNSA), which meets regularly, exchanges best practices and cooperates on enforcement across borders. The CNSA has drawn up a cooperation procedure to facilitate cross-border handling of spam complaints. The Commission services support and participate as observers in the London Action Plan, which gathers enforcement authorities from 20 countries and has also adopted a cross border cooperation procedure. A joint EU CNSA – LAP workshop was held in November 2005. The OECD adopted a Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam which was adopted in April 2006, urging enforcement authorities to share information and work together.

- The Commission is further promoting international cooperation initiatives. The US and the EU have agreed 'to cooperate to tackle spam through joint enforcement initiatives, and explore ways to fight against illegal "spyware" and "malware". The Commission also takes part in the Canadian International Collaboration working group on Spam. Discussions are taking place with major international partners e.g., China, Japan. Concerning Asia the Commission initiated a Joint Statement on International Anti-spam Cooperation which was adopted at the ASEM conference on eCommerce in February 2005.

- The Tunis Agenda, adopted by the World Summit of Information Society in November 2005, stresses that internet security is an area where a better international cooperation is needed and that this issue will need to be addressed in the framework of the enhanced cooperation model for internet governance that will be implemented as a follow-up of the Summit.

- The Commission welcomes industry's pro-active role in relation to spam. Service providers in general have taken technical measures to tackle spam, including better spam filters. ISPs have set up help desk support and provide users with software against spam, spyware and malware. Many ISPs have contractual clauses in place that forbid on-line malpractices. In a recent civil UK court case a € 68,800 fine was imposed on a spammer for breach of contract. Industry groups have adopted best practices to prevent on-line phishing and to improve filtering methods.

- Mobile operators have acted Industry codes of conduct foresee taking action against unsolicited messages. The GMSA has published a Code of practice on Mobile spam in 2006. Currently the Commission co-funds the Spotspam initiative – a partnership between private and public bodies which aims to build a database to facilitate the cross border investigation and enforcement of spam cases.

- It is clear that taking up the fight against spam delivers results. Filtering measures imposed in Finland reduced the proportion of spam in the transmitted e-mail from 80 % to about 30 %. A large number of authorities have undertaken enforcement efforts to stop spammers.

- There are however significant differences between Member States in the actual number of prosecuted cases. Some authorities have launched a hundred or more investigations that have led to successfully ending and penalising spam activities. In other Member States the number of cases investigated has not been more than a handful or in some cases zero. Most actions have been targeted at 'traditional' forms of spam; other noted threats have hardly been prosecuted even though they create major risks.

- To date, the increasingly entwined criminal and administrative aspects of spam and other threats have not been reflected in a corresponding growth of cooperation procedures in Member States that brings together the technical and investigative skills of different agencies. Cooperation protocols are needed to cover such areas as exchange of information and intelligence, contact details, assistance, and transfer of cases.

- Close cooperation between enforcement authorities, network operators and ISPs at national level is also beneficial for exchange of information, technical expertise and the pursuit of on-line malpractices. Authorities from Norway and the Netherlands have reported on the usefulness of such public-private partnerships.

- The Commission Communication on the regulatory framework for electronic communications proposes to strengthen the rules in the area of privacy and security. Under the proposal, network operators and service provider would be obliged to: (i) notify the competent authority in a Member State of any breach of security that led to the loss of personal data and/or to interruptions in the continuity of service supply; (ii) notify their customers of any breach of security leading to the loss, modification, access or destruction of personal customer data.

Council Resolution of 22 March 2007 on a Strategy for a Secure Information Society in Europe summarised the important initiatives (also regarding spam):[32]

- The 10 March 2004 Regulation (EC) No 460/2004 of the European Parliament and of the Council establishing the European Network and Information Security Agency (ENISA);

- The Tunis Agenda and the Tunis Commitment of the World Summit on the Information Society (WSIS) highlighting the need to continue the fight against cyber-crime and spam while ensuring the protection of privacy and freedom of expression, and to further promote, develop and implement, in cooperation with all stakeholders, a global cyber-security culture;

- The Presidency Conclusions of the Annual European Information Society Conference (27- 28 September 2006) "i2010 — Towards a Ubiquitous European Information Society", in Espoo, Finland;

and welcomes the intention of the Commission to

- continue to play its role so as to achieve greater awareness about the need for general political commitment to fight spam, spyware and malware; reinforce the dialogue and cooperation with third countries, in particular through agreements with third countries including the issue of the fight against spam, spyware and malware;

and calls upon

- stakeholders to cooperate and to launch experimental environments for testing and piloting new technologies and services in a secure manner; stakeholders to adopt in a timely manner the new secure technologies and services after they have been launched commercially;

- all stakeholders to engage in further efforts to combat spam and other on-line malpractices and to actively cooperate with competent authorities at national and international level;

In the Communication from the Commission on "i2010 - Annual Information Society Report 2007" the Commission stressed the future of the "knowledge-based economy":[33]

- Six years after the burst of the Internet bubble, the information society is on a steady growth path. A decade of investment in ICT is bearing fruit, fuelling innovation in ICT areas and transforming the EU into a knowledge-based economy.

---

[32] Council Resolution of 22 March 2007 on a Strategy for a Secure Information Society in Europe, Official Journal 2007 C 068, 1.

[33] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - i2010 - Annual Information Society Report 2007, COM/2007/0146 final.

The Opinion of the European Economic and Social Committee on the Communication from the Commission on the Review of the EU Regulatory Framework for electronic communications networks and services, published on April 28, 2007, states:[34]

- As a general principle of regulation, the public interest — the "public good "— should have primacy over private and business interests. The Committee also believes that the market alone cannot properly regulate itself for the benefit of the public good. Therefore, a strong regulatory framework is needed to promote the interests of the greater number of citizens, as intended by the Lisbon strategy.

- Consideration should also be given to mechanisms which would facilitate a fast-track, EU-wide "right of action "by consumers (an individual or collective action) against individual perpetrators.

- Beyond the scope of the Regulatory Framework, the Committee urges the Commission to systematically investigate security offences — such as spam, phishing and hacking — perpetrated by wrongdoers outside of the EU, and to pursue remedies at inter-government level.

- Strong penalties are needed across the EU to prevent this type of crime from undermining consumer confidence and retarding the development of the Information society.

- In addition to security problems caused by persons inside the EU, the security of European networks and citizen's are subject to daily attack from outside the Union. Every step should be taken to pursue the perpetrators of these attacks, including holding the states from which the attacks occur accountable for the damage they do.

However, there are also "political and legal limits"; eg the Working Party 29 referred in its statement on privacy issues related to the provision of email screening services to the following issues:[35]

- With the expansion of the ecommunication services, concerns about the protection of the privacy of the communications have arisen, in particular because of existing practices to inspect communications in order to eliminate spam and viruses as well as to detect any predetermined content.

- However the Working Party 29 considers that, in some cases, using such filtering tools may not be in compliance with the existing data protection legislation de-

---

[34] Opinion of the European Economic and Social Committee on the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on the Review of the EU Regulatory Framework for electronic communications networks and services, Official Journal 2007 C 97, 27.

[35] Working Party 29 Opinion 2/2006 on privacy issues related to the provision of email screening services, adopted on 21 February 2006, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp118_en.pdf.

scribed below. This may be due, among others, to the fact that the application of the legislation to these new types of services is not always clear.

- Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR") and the constitutions of the Member States. Article 8 of the ECHR provides everyone with the right to respect for his private life and his correspondence and lays down the conditions under which restrictions of this right could be acceptable. The European Court of Human Rights ("the Court") has applied Article 8 to regular mail communication on various occasions. Interception, opening, reading, delaying reception of letters or putting up barriers to the sending of letters have all been considered to be interfering with Article 8 of the ECHR. From the case law of Commission and the Court of Human Rights, it may be concluded that email communications almost certainly will be covered by Article 8 ECHR, by combining both the notions of "private life" and "correspondence". Communication partners that use emails may reasonably expect that their communications will not be inspected by third public or private parties. The right to respect for "correspondence" not only includes confidentiality but also the right to send and receive such correspondence. Thus, it may be concluded that a general prohibition of sending or receiving email will conflict with Article 8 of the ECHR.

- Such interceptions are unacceptable unless they fulfil three fundamental criteria, in accordance with Article 8 (2) of the ECHR and the ECHR's interpretation of this provision: *"… a legal basis, the need for such a measure in a democratic society, and conformity with one of the legitimate aims listed in the Convention…"*

- Article 6 (2) of the Treaty on European Union states clearly that the Union shall respect fundamental rights, as guaranteed by the ECHR and as they result from the constitutional traditions common to the Member States, as general principles of Community law. According to Article 52 (3) of the EU Charter, the meaning and scope of rights contained in the Charter shall be the same as those laid down by the ECHR. This provision shall not prevent the Union law from providing more extensive protection.

- According to recital 47 of the Data Protection Directive, the person from whom an email message that contains personal data originates must be considered to be the controller of that personal data, whereas the email service provider will normally be considered controller in respect of the processing of the additional personal data necessary for the operation of the service.

- Article 5 of the E-Communication Directive reads as follows: *"…Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other then users, without the consent of the users concerned, except when legally authorised to do so…"* Moreover, Article 4 provides that *"The provider of*

a publicly available telecommunications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public telecommunications network with respect to network security".

- One of them consists of using the so-called blacklisting by which IP addresses of certain servers and dynamic IP ranges allocated to certain ISPs are blacklisted.

- The Working Party 29 considers that Article 4 of the e-Privacy Directive requiring email providers to take appropriate technical and organisational measures to safeguard security of their services, is concerned about the security of the ESP and network services per se but also about the general performance of the email and network services. Security of the ESP is a problem insofar as it affects the ESP service. For this reason, the Working Party 29 considers that Article 4 might also apply to this situation. In other words, threats to the general performance of email and network services can justify ISPs and ESPs to engage in filtering for anti-spam purposes. If one takes into account the effects that spam produces, even in those cases where the spam sender distributes only few information via emails per day, but those information are sent to a very huge number of recipients, it reinforces the argument in favour of the application of Article 4 of the e-Privacy Directive because even in these cases, the sending of such limited number of emails might block the internet traffic and seriously harm the reliability, the security and the efficiency of email services in general. Furthermore, for the same reasons, the Working Party 29 also considers that such filtering could be legitimized on the basis of Article 7 (b) of the Data Protection Directive, on the basis that filtering for spam is necessary for the email provider to be able to perform properly the service contract to which the data subject, i.e. recipient is a party.

- On the other hand, the Working Party 29 is concerned by the fact that filtering results sometimes in "false positives", i.e. legitimate "wanted" messages are not delivered because they are deemed to be spam. The Working Party 29 considers that the action of filtering and withholding received mail supposedly unwanted may entail not only an invasion to the freedom of speech but also, a violation of Article 10 of the ECHR and constitute an interference of private communications.

- In light of the above, notwithstanding the application of Article 4 of the E-Communication-Directive, and in order to safeguard the principle of freedom of communications, as recognised by Article 10 of the ECHR as well as the confidentiality of the communications provided in Article 5 of the e-Privacy Directive and recognised by Article 8 of the ECHR, the Working Party 29 strongly recommends email providers to take into account the following recommendations, which mainly aim at giving recipients of emails control on the communications that are in principle addressed to them:

  (a) the Working Party 29 encourages the practice consisting of giving subscribers the possibility to opt out of scanning their emails for spam purposes, the possibility to check emails deemed as spam in order to ascertain whether they were indeed spam and the possibility to decide what "kind" of spam should

be filtered out. Furthermore, the Working Party 29 also welcomes the activity of some of ESPs that offer subscribers an easy way of opting back into the scanning of their emails for the purposes of filtering spam;

(b) the Working Party 29 also encourages the development of filtering tools that end users can install or configure either in the terminal equipment or in third party servers or in the provider's email server and which enable them to control what they want to receive and what they do not want to receive, also in order to reduce the costs inherent in downloading unsolicited electronic mail as recalled in Recital 44 to Directive 2002/58. The Working Party 29 also welcomes the research of other tools to fight spam that may be less privacy intrusive.

- In addition to the above, the Working Party 29 reminds email service providers engaged in screening emails for spam purposes of their duties, under Article 10 of the Data Protection Directive, to inform subscribers of their policy as far as spam is concerned in a clear and unambiguous way, as further described under section IV of this Opinion. The email provider must also ensure the confidentiality of the filtered emails that should not be used for any other purpose.

- As far as filtering for the purposes of screening virus and spam is concerned, the Working Party 29 considers appropriate the ESPs practice consisting of informing subscribers as part of the contractual conditions of the service.

- In addition to the above, ESPs must also comply with Article 4 of the E-Communication-Directive which requires providers of a publicly available electronic communication service to inform subscribers of particular risks of breaches of the security of the network. Where the security lies outside the scope of possible remedies by the service provider, the service providers should inform their users and subscribers of measures they can take to protect the security of their communications.

4. (Fighting) Spam in Legal Practice

Although the EU has shown all these initiatives and set in force all these directives, spam is a fact and the fact has to be evaluated based on the circumstances in reality and this reality is the world and in Europe is that there are (still) independent states with (more or less) independent legal systems. Because the 2nd EU Symposium is hold in Vienna, Austria, and Austria was one of the first states implementing a spam-regulation, and – last but not least – the author is an Austrian attorney-at-law, the following part tries to show the possibilities and obstacle for "spammers" and "victims" in Austria.

It shall not be forgotten that eMarketing is an important and growing part of the economy. Six to seven years after the burst of the Internet bubble, the information society is on a steady growth path and the (EU-)economy is moving into a knowledge-based economy.

However, whenever we refer to spam, we refer to "illegal spam", which shall/has to be fought in practice:

4.1. Possibilities and Obstacles for Victims – in Austria

Sec 101 Telecommunications Law 1997 (TKG 1997) stipulated from August 20, 1999 until August 19, 2003:

> *"[...] Sending of email in bulk or for advertising purposes requires the prior - revocable at any time - consent of the recipient."*

This clear regulation was changed twice and today Sec 107 Telecommunications Law 2003 (TKG) stipulates the following:

> *"(2) The sending of electronic mail – including SMS messages – without the recipient's prior consent shall not be permitted if*
> *(i) the sending takes place for purposes of direct marketing or*
> *(ii) is addressed to more than 50 recipients."*

Please note the definition in Sec 92 para 3 No 10 TKG:

> *"'electronic mail' means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient."*

Sec 107 para 3 TKG states exceptions from the above named prerequisite of a "prior consent" regarding electronic mail for purposes of direct marketing:

> *"(3) Prior consent to electronic mail pursuant to para (2) shall not be required if*
> *(i) the sender has received the contact details for the communication in the context of a sale or a service to his customers and*
> *(ii) the communication is transmitted for the purpose of direct marketing of his own similar products or services and*
> *(iii) the recipient clearly and distinctly has been given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use and*
> *(iv) the recipient has not generally refused to receive such mail in the first place, especially by registering in the list named in Sec 7 para 2 ECG."* [comp "Robinson-list" below].

Furthermore, Sec 107 para 5 TKG states a general clause when electronic mail is prohibited – irrespective of the exception in para 3:

> *"(5) The sending of electronic communications for purposes of direct marketing shall be prohibited in any case if the identity of the sender on whose behalf the communication is transmitted is disguised or concealed or if there is no valid address to which the recipient may send a request that such communications cease."*

Sec 107 para 6 TKG makes clear that the prohibition cannot be circumvented by sending the electronic mail from abroad:

> *"(6) If administrative offences pursuant to para (1), (2) or (5) have not been committed in Austria, they shall be considered as having been committed in the place where the unsolicited message reaches the subscriber's line."*

Following the EU-E-Commerce-Directive Sec 7 (Austrian) E-Commerce-Act (ECG) states *inter alia* the keeping of a "Robinson-list"(in para (2)):

> *"(1) A service provider which sends a commercial communication admissibly by electronic mail without prior approval of the recipient must ensure that the commercial communication shall be identifiable clearly and unambiguously as such when received by the user.*
>
> *(2) Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH) must keep a list in which those persons and companies not desiring to receive commercial communications by electronic mail can be entered free of charge. The service providers mentioned in para 1 must comply with such list.*
>
> *(3) No legal provisions on the admissibility or inadmissibility of the transmission of commercial communications by way of electronic mail shall be prejudiced hereby."*

Compare the regarding Website of the RTR-GmbH, which is (part of) the Austrian Telecommunication and Broadcasting Regulatory Authority: http://www.rtr.at/web.nsf/englisch/Telekommunikation_Konsumentenservice_E-Commerce-Gesetz (unfortunately only in German).

Unfortunately, there are ongoing discussions in the doctrine (compare (German) publications on the topic of "Spam" and "Spamming" under http://www.gassauer.at/en/publication/#p650) and no clear case law regarding the question, what impact the above exceptions have in practice and therefore, it is only possible to evaluate the exceptions of the prohibition case-by-case.

In any case, Sec 107 TKG states a prohibition to use electronic mail for the purposes of direct marketing, unless the prior consent of the recipient was obtained or the above named exception applies. Please note that the regarding consent is defined (in the Austrian Data Protection Act 2000) as:

> *"the valid declaration of intention, given without constraint, that he agrees to the use of the data in a given case, after having been informed about the prevalent circumstances."*

Pursuant to the administrative penal regulations in Sec 109 TKG any person who contrary to § 107 TKG sends electronic communications for the purposes of direct marketing shall be guilty of an administrative offence and shall be punished by a fine of up to EUR 37,000.--. Please note that the practical impact of the administrative penal regulations is rather low, because not the police but the "Telecommunications Office" is entrusted with the enforcement of this administrative penalty. The competences of this Office is however normally not to "hunt down and smoke out" criminals or spammers but the administration and licensing of frequencies and radio systems.

Thus, the "private enforcement" is in Austria of more importance:

4.2. Spamming and Unfair Practices

Sec 1 Austrian Federal Act Against Unfair Competition of 1984 (Bundesgesetz gegen den unlauteren Wettbewerb 1984 – UWG) reads as follows:

> "*Any party who in the course of business resorts to competitive practices which are contrary to public policy (bonos mores) may be sued for a cease-and-desist order and payment of damages.*"

Sec 1 UWG generally prohibits actions in business dealings for competition purposes that violate "*bonos mores*" (comp "*good faith*"). Of course, the concept of *bonos mores* requires concrete definition; the determination of an action to be contra *bonos mores* must be made in each individual case and should be based on the views of the public and the average competitor. Case law and doctrine try to make up for the vagaries of the indeterminate legal concept by creating typical case groups in order to improve the practicability of the general clause.

One of the most important case groups under § 1 UWG is "breach of law": it is considered an action in violation of bonos mores

a. to knowingly disregard a law,

b. for the purpose of obtaining a competitive advantage over competitors that obey the law.

A merely unintentional violation of laws and infringement of rules owing to incorrect but defensible interpretation of the law does not correspond to the elements of an offence.

The UWG knows in the context of Sec 1 UWG claims to cease and desist (Sec 14), removal (Sec 15), damages (Sec 16) and publication of judgement (Sec 25).

- **Claim to cease and desist**

Against a party violating the provisions of the UWG a claim to cease and desist can be filed. It is a substantive prerequisite for such claim that the risk of repetition exists, as the cease and desist claim should prevent future anti-competitive actions. A risk of repetition exists if there is serious concern that the defendant will take further interfering actions; this is refutably presumed even upon only one infringement of fair competition – especially whenever spam is involved. It is of particular practical importance that the offer by the defendant to undertake to cease and desist from the relevant action by concluding an enforceable settlement is as a rule considered to preclude the risk of repetition, however, such offer must include everything the plaintiff might be awarded if he succeeded in a lawsuit; this applies to the claim to reimbursement of costs only to a limited extent.

The right to sue is basically with the party concerned, or, in certain cases, only every entrepreneur that produces or puts on the market goods or services of the same or a

similar kind (competitor). In addition, certain associations and chambers also have the right to sue.

The parties against which a lawsuit can be filed are the direct offender, accessories and the owner of the business, who is liable for damages only if he was aware or should have been aware of the unfair practice. However, there are exceptions regarding the ISPs based on the E-Commerce-Act (comp the E-Commerce-Directive).

Basically, cease and desist claims come under the statute of limitation six months after obtaining knowledge of the action and the offender (Sec 20 para. 1 UWG).

- **Claim to removal**

The claim to cease and desist also comprises the right to request the removal of the condition that conflicts with the legal requirements. It does not depend on the risk of repetition but merely on the continuance of the unlawful condition.

In the context of spam this means that the spammer has to stop automatically the sending of spam.

- **Damages**

Where an unfair practice committed due to fault caused a loss to a third party, the infringed party has a claim to damages. Pursuant to Sec 16 para. 1 UWG the damages to be awarded in this case in a case of fault shall also include lost profits; under Sec 16 para. 2, basically also intangible losses can be suitable for triggering damages.

- **Publication of judgement**

Sec 25 para. 3 UWG stipulates that in case of a claim to cease and desist, the court upon application has to award the successful party, if it has a justified interest, the right to have the judgement published within a certain deadline at the opposing party's expense; the publication shall serve the purpose of correcting the incorrect opinion of the market participants concerned that was created by the competitive action and of informing the public. The publication includes the judgement, plus the cost of the decision and the decision on compensation claims.

4.2.1. Spamming, UWG and the Impact of the Procedural Law

The course of unfair competition proceedings can cursorily be described as follows:

- **Statement of Claim / Action and Petition for Preliminary Injunction**

The statement of claim that is filed against a spammer usually also includes a petition for the issuance of an injunction. Upon receipt of a petition the court may – but is not obliged to – forward it to the opponent for filing a reply. The period stipulated by the court for filing a reply is usually between 7 and 14 days. This period can basically be extended upon application by the opponent. In the rare cases where the court does not instruct the opponent to file a reply and the requested preliminary injunction is issued, the opponent is entitled not only to file an appeal as the 'regular' legal remedy but also

to file a protest within 14 days from being served the decision. In the protest proceedings the original court shall conduct an oral hearing to examine whether the issuance of the injunction is admissible and shall then decide whether the injunction shall be upheld or the petition shall be dismissed on the basis of the *prima facie* evidence submitted by the opponent.

Following the court's decision in injunction proceedings the unsuccessful party has the right to file an appeal within 14 days of the service of the decision. It should be noted in this context that an appeal filed against a preliminary injunction does not have a suspensive effect on its enforceability; where reasons of particular relevance exist, however, such suspensive effect may be petitioned for.

Preliminary injunctions are usually issued for the entire duration of the main proceedings. They may be lifted under certain circumstances, however. Whichever grounds may be invoked for such dissolution of a preliminary injunction, they are admissible only if they have become applicable after the injunction has been issued. If the issuing of the injunction was erroneous, such claim must be raised in an appeal or protest. A dissolution is possible *inter alia* in the following cases: (i) dissolution due to subsequent change of circumstances: the preliminary injunction is to be dissolved if following its issuance the circumstances on the basis of which it was granted change to such an extent that the injunction is no longer necessary for securing the party upon whose petition it was granted (here esp change of laws respectively new decision of ECoJ); (ii) dissolution upon extinguishment of the claim: the injunction is to be dissolved if the claim of the party at risk has been settled or finally denied or if the extinguishing of such claim has been finally determined by the courts.

Documents, affidavits and private expert opinions are the most important factor in preliminary proceedings; as provided by the regulations of the Austrian Act on Legal Enforcement (EO), there will be no oral hearings and if (very rarely) witnesses are interrogated, then there is no formal hearing and no possibility for cross-examination, as the parties´ representatives are not admitted to the interrogation sessions in preliminary proceedings.

The suspension of a preliminary injunction upon the provision of security by the opponent, which may also be effected for a limited period, is subject to the filing of a petition setting out the grounds for suspension in sufficient detail. In accordance with prevailing judicial practice the value of the claim to be secured is to be used as a basis for the determination of the discharge amount; the plaintiff is deemed to be sufficiently secured if the amount enables the reestablishment of the former state in case the plaintiff should be successful in the proceedings. The discharge amount should not be too low as this might tempt the opponent to pay the amount and nevertheless continue its unlawful conduct. The suspension order by the court does not dissolve the preliminary injunction itself but only stops its enforcement; therefore the right to exercise legal remedies against the injunction is not affected. It is also possible to challenge the suspension order by an independent appeal; since the injunction itself is not dissolved it will again become enforceable if the appeal is granted.

- **Main Proceeding respectively Proceeding for Compensation**

  After a valid and enforceable decision in the injunction proceedings, many unfair competition proceedings are not continued but terminated by a settlement.

  Even though the instrument of a preliminary injunction is the most effective means of legal protection against further infringements it nevertheless involves a considerable risk that should only be assumed if it appears certain that the petitioner will win the main proceedings. This is due to the provisions of Sec 394 EO pursuant to which the opponent is entitled to claim damages if it is found that the issuance of the preliminary injunction was not justified. Sec 394 EO reads as follows:

  > *"If the party at risk is finally denied the alleged claim in respect of which the preliminary injunction had been granted, if such party's petition is otherwise found to be unjustified, or if such party fails to comply with the delay for filing a complaint or instituting enforcement proceedings, the party upon whose petition the preliminary injunction had been granted shall be liable to pay damages to its opponent in respect of any and all property loss incurred by such opponent as a result of the preliminary injunction. The amount of damages shall be determined by the court in its discretion upon a relevant petition (Sec 273 ZPO) by way of a decision. If such decision has become final it shall be enforced against the property of the party that petitioned for the preliminary injunction."*

- **Enforcement**

  Claims to cease and desist – irrespective of whether included in a final order or in a preliminary injunction – are enforced in accordance with Sec 355 EO, whereby a petition shall be filed with the court of enforcement in respect of each act of non-compliance following the enforceability of the claim (ie in case of an preliminary injunction its service) and the court shall then impose a fine on the liable party without prior warning. For each further act of non-compliance the court shall impose a further fine or a custodial sentence up to a total duration of one year. The party at risk may also request that the court order the provision of security in respect of the damage incurred by further non-compliance. In accordance with Sec 359 EO the fine imposed must not exceed EUR 100,000 for each individual petition. The petition for enforcement must include a concrete and conclusive allegation of the act of non-compliance with the preliminary injunction; it is not required to submit *prima facie* evidence for the allegation, and no examination of its content is carried out; the so-called 'enforcement permission' based on which the bailiff will enforce the claim is granted solely on the basis of the petitioner's allegation. The liable party in enforcement proceedings can (essentially) choose one of two counterstrategies: On the one hand, an appeal can be filed against incorrect enforcement permission, eg if it is not in accordance with the petitioner's allegations or if the alleged infringements were committed prior to the service of the preliminary injunction. Objections to the claim itself or to the enforcement permission, on the other hand, must be raised not by way of an appeal but by way of a separate 'opposition' or 'impugnation' action pursuant to SSec 35 and 36 EO. In such cases, separate proceedings before the court of enforcement will be instituted in which the plaintiff (being the defendant in the patent infringement proceedings) is liable to

prove that it is not guilty of any non-compliance with the enforcement order (other than alleged in the enforcement petition).

Payment claims (which include the claim to payment of the costs in connection with the publication of the judgement by plaintiff in accordance with the court's decision) are collectible in various ways (enforcement against movables, enforcement against personal property and salary, etc).

- **Appeal Procedure**

Any first instance decision – be it in main or in preliminary proceedings – can be appealed before the Court of Appeals. If the question at stake is of general importance and interest, there is the possibility of filing a third instance appeal to the Supreme Court.

The appeal deadlines generally are four weeks in main proceedings and 14 days in preliminary proceedings; within the same periods of time the opponent to the appeal may file counter-statements. Oral proceedings in the appeal stage are very rare.

- **Litigation Costs**

The actual costs will naturally depend on the complexity of the case and the value in litigation. Traditionally, a cease and desist claim based on UWG against a spammer is rated at EUR 36,000 and the court fees amount to approximately 0.2% of the value in litigation. The actual lawyers fees depends on the time spent and the respective fee arrangements.

However, a refund of a part of the lawyer's fees by the losing party is available, which refund is calculated on the basis of the minimum fees defined by the Austrian Act on Legal Ethics (RAO). With standard values in litigation, a refund would normally range between € 7,500–15.000 in preliminary proceedings and € 15,000–30,000 in main proceedings.

Based on the above the following question arises: Who wants / can afford these costs against a single spammer?

4.3. Spam and Criminal Offence

Not all Member States have judicial sanctions in place for spam. Not all Member States provide for remedies and fines/penalties under administrative law, or under criminal law. Criminal sanctions vary, including terms of imprisonment in certain Member States. In addition, there is generally the possibility to claim damages under civil law.

The Commission is of the opinion that to date, the increasingly entwined criminal and administrative aspects of spam and other threats have not been reflected in a corresponding growth of cooperation procedures in Member States that brings together the technical and investigative skills of different agencies. Cooperation protocols are needed to cover such areas as exchange of information and intelligence, contact details, assistance, and transfer of cases.

However, spam is not murder, fraud or theft – as the legal practice shows, the harder the penalties are in comparison to the actual seen damage the less law enforcement agencies are willing to enforce the law. Furthermore, especially in criminal cases the international aspects often lead to a "neverending file".

Therefore, the author is of the opinion that criminal law does not mean the end of spam.

5. Forecast

5.1. "Code and Other Laws of Spam"

We saw the limits of the legal handling of spam. *Lawrence Lessig* is suggesting that technical solutions rather than legal solutions are anyway more appropriate to the Internet context:[36]

> *"Just as we should worry about the bad regulations of law, so too should we worry about the bad regulations of code.*
>
> *Y2K* [but could also stand for spam] *is the product of a certain kind of libertarianism. It is the product of not thinking through the regulation of code, and of law not properly holding coders responsible for their code. Now, years after the first bad code was compiled, we are faced with a kind of environmental disaster: we are surrounded by code that in critical and unpredictable ways will misfire – at a minimum causing the economy millions of dollars, and under some doomsday scenarios causing much worse damage.*
>
> *Were the tort system better at holding producers responsible for the harms they create, code writers and their employers would have been more concerned with the harm their code would create. Were contract law not so eager to allow liability in economic transactions to be waived, the licenses that absolved the code writers of any potential liability from bad code would not have induced an even greater laxity in what these code writers were producing.*
>
> *Code may be only a difference in degree, but a difference in degree at some point becomes a difference in kind. The unintended consequence of private coding behavior is a time-bomb set to explode over the next year or so. The Y2K problem should awaken us to other time-bombs in our lives – that is, to the general effect that code will have on our lives.*
>
> *We live life in real space, subject to the effects of code. We live ordinary lives, subject to the effects of code. We live social and political lives, subject to the effects of code. Code regulates all these aspects of our lives, more pervasively over time than any other regulator in our life. Should we remain passive about this regulator? Should we let it affect us without doing anything in return?*

---

[36] *Lessig*, Code and Other Laws of Cyperspace (1999).

We will treat code-based environmental disasters – like Y2K, like the loss of privacy, like the censorship of filters, like the disappearance of an intellectual commons – as if they were produced by gods, not by Man. We will in many domains of our social life come to see the Net as the product of something alien – something we cannot direct because we cannot direct anything. Something instead that we must simply accept, as it invades and transforms our lives.

Some say this is an exciting time. But it is the excitement of a teenager playing chicken, his car barreling down the highway, hands held far from the steering wheel. There are choices we could make, but we pretend that there is nothing we can do. We choose to pretend; we shut our eyes. We build this nature, then are constrained by this nature we have built.

It is the age of the ostrich. We are excited by what we cannot know. We are proud to leave things to the invisible hand. We make the hand invisible simply by looking the other way."

5.2. The Limits of Code

Therefore, also code is not the "silver bullet" for addressing spam – as long as it does not follow certain rules:

Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR") and the constitutions of the Member States. Article 8 of the ECHR provides everyone with the right to respect for his private life and his correspondence and lays down the conditions under which restrictions of this right could be acceptable. Interceptions are unacceptable unless they fulfil three fundamental criteria, in accordance with Article 8 (2) of the ECHR and the ECHR's interpretation of this provision: "*… a legal basis, the need for such a measure in a democratic society, and conformity with one of the legitimate aims listed in the Convention…*".

Furthermore, filter systems could violate the existing regulations on Telecommunications Laws.

5.3. International eMarketing Society – "Anti-Spam Inc."

The author suggests the following solution to the problem of spam and the fact that eMarketing is a growing part of the economy:

- **What is the issue – at the same time the base to built on:**
  - Spam has reached a point where it also creates considerable costs for businesses.
  - The Internet (spam) requires a harmonised approach to ensure simple, world/community-wide rules on spam for businesses and users.
  - Obligatory labelling could help filter-system to handle spam; but there have to be clear enforceable guidelines.

- As is often the case, effective application of self-regulatory solutions will depend on the structure put in place to oversee respect for the agreed rules, including effective sanctions.

- Furthermore, filtering may occasionally block legitimate e-mail ('false positive') or allow spam to get through ('false negatives'). In some cases, this can create a risk that either a sender or an intended addressee undertakes legal action against an ISP/ESP.

- Enforcement of rules on unsolicited messages for direct marketing has to be balanced with the right to privacy – however, there is no reason not to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes and enforce this prohibition.

- Obstacles in fighting spam include the difficulty of identifying the senders of such spam or the amount of effort required to do so and the costs of the proceedings, the lack of (appropriate) international co-operation mechanisms, and the lack of jurisdiction of some authorities on international matters.

- The EU-regulation is applicable to all unsolicited commercial communications received on and sent from networks in the EU (and EEA). This implies that such messages originating in third countries must also comply with EU rules, as must messages originating in the EU and sent to addressees in third countries.

- There is a need to promote the adoption of effective legislation in third countries and to ensure effective enforcement of the applicable rules. Although the Commission has set up a Contact Network of Spam Authorities (CNSA), the over-impression is that they are only seeing "bad guys" and are acting slow and not with all (legal) possibilities. The same seems to apply to most public-private partnerships, like "Spotspam" – a partnership between private and public bodies which aims to build a database to facilitate the cross border investigation and enforcement of spam cases – however, they do no offer the "full program".

- **What we need is somebody, who**

  - has the possibility to change the "code on e-Mails";

  - does lobbying for clear legal frameworks for legitimate eMarketing and for illegal spamming;

  - supports companies / consumers in their fight against spammers;

  - supports companies / consumers in their right to communicate and in their right to privacy;

- convinces governments to use technical measures against spam – and that these measures shall not be stopped by "data protection";
- does lobbying for legitimate eMarketing ("seal of approval" etc);
- fights spammers with all possible measures: PR, actions, laws, economical pressure;
- is not a state authority but fast acting.

- **Who can do that?**

  We need an international, objective society/agency/cooperation (with the headquarter in Vienna), consisting of

  - undertakings, affected by spam, investing money to fight spam to save money caused by spam (ISP, telco, industry/chambers of commerce etc);
  - e-direct marketeers that want to use "eMail-Marketing" as a serious marketing-concept (incl chambers);
  - Software- and filter technology industry, creating and implementing objective standards;
  - Lobbyists to find the common sense and to convince politicians that spam needs action but also eMarketing needs support;
  - Lawyers to fight against spammers – internationally coordinated, with the support of the legal enforcement authorities and in legal proceedings with a spread of risks.

Max W. Mosing, Vienna, May 2007