European Union vs. Spam: A Legal Response

Nicola Lugaresi (lugaresi@jus.unitn.it)

Trento University, Law School, via Verdi, 53, 38100 Trento, Italy

1 Introduction

Unsolicited commercial communications now represent more than fifty per cent of the e-mail traffic in the European Union and around the world. This paper is about the legal EU approach to such an issue. Through the analysis of the evolution of the legislative framework, it aims to define, under a legal perspective, what spam is, to explain why the opt-in choice has been adopted by the EU, and to show the discipline of other related specific aspects.

The main reason why European Union has faced spam (assuming, for the time being, that spam is synonymous with unsolicited commercial electronic communications) is that spam affects fundamental rights of the individual. Not only is spam a global nuisance, but it concerns primarily people's privacy. It infringes the more visible side of privacy, the protection of personal data, as it involves not only the unfair and unlawful collection and use of private e-mail addresses, but also illegal intrusion into computers and servers. Moreover, it violates privacy in its broader and more sensitive sense - the "right to be let alone" - by filling in-boxes with loads of unwanted e-mail. In this respect, spam deprives individuals both of their capacity to control the amount of personal information to be known by others and of their capacity to control the flow of information entering their private sphere. Legal intervention to curb the flow of unsolicited commercial communications is therefore justified for several reasons, and is aimed to protect several interests, as EU Directives and other official EU documents acknowledge. Spam affects individuals, users, subscribers, consumers, companies, direct marketers, Internet service providers, traders, employers, organizations, public bodies, and, in the end, the Internet itself. The EU has for several years been aware of the risks to users' privacy raised by the public availability of electronic communications services over the Internet[1]. And EU has been aware that spam compromises electronic communications, interactive networks, terminal equipments[2], productivity at work[3], and e-commerce itself[4]. Moreover spam is often the means through which frauds are carried out, and the carrier of pornographic messages, hate speech, and viruses.

EU laws alone are not likely to solve the problem, for both jurisdictional and technical reasons. Notwithstanding the ineluctability, in the short-term, of spam, the EU could not refrain from intervening in order to protect a repeatedly violated fundamental right. EU laws focus on two goals - the practical goal of reducing the amount of Spam, and the ethical goal of attempting to guarantee the individual's control over personal relationships and contacts, both inbound and outbound. Unless legal regimes are coordinated and jurisdictional issues are resolved, the extent to which the first of these goals can be realized is substantially limited. With respect to the second, EU laws characterize privacy as a fundamental right, in all personal life expressions[5], and identify spam as a major problem that plays a critical role in market failures, unless strict rules are enacted and enforced. Such an approach was encouraged by the perception of the role of commercial communications in the information society[6]. As for enforceability, EU Directives apply to all unsolicited commercial communications received on and sent from networks in the European Union[7]. When e-mail is originated in third countries, the problem is that enforcement (and,

[1] Article 1, and recital 6, Dir. 2002/58/EC.
[2] Recital 30, Dir.2000/31/EC; recital 40, Dir.2002/58/EC.
[3] EC Communication on "spam" (2004), §1.2.
[4] Recital 60, Dir.2000/31/EC.
[5] Council Decision 1999/168/EC (Annex II, §a.i).
[6] Recital 29, Dir. 2000/31/EC.
[7] EC Communication on "spam" (2004), §3.5.1.

in particular, the identification of spammers) is quite complicated, due to little experience and jurisdictional obstacles. Jurisdictional issues clearly show the need for international co-operation. In these terms, European Union legal strategies, and the corresponding laws, must be regarded not as the ultimate answer to spam, but as an attempt to set up a rational discipline and as a possible model for a harmonized approach to reducing spam that rests on three elements. First, law enforcement bodies must make a serious commitment to enforcing laws through adequate actions: effective penalties, national and cross-borders complaints mechanisms and remedies, monitoring, coordination among national authorities, international co-operation, and available resources. Spam must be fought, not just denigrated. Second, regimes to control spam must come in different forms: legislation, self-regulation, architecture, and alternative dispute resolution, methods characterized by their flexibility and capacity to promptly adapt to new cases and technologies. Spam must be fought, with a combination of weapons. Third, social awareness of spam, the online behaviors that cause it, and the tools available to avoid it must be spread and reinforced, taking the form of education of users and market players, information, self-help, involvement of associations and privacy advocates[8]. Spam must be fought, by all the actors involved.

2 From opt-out to opt-in

Apart from broad political strategies, EU Directives on privacy, trade, and communications have affected, since 1995, the discipline of spam. The early interest was motivated by the need to protect citizens, and consumers, from "high-pressure selling methods"[9] and from "certain particularly intrusive means of communication"[10]. Unlike the CAN-SPAM Act of 2003 in the United States, though, the EU has not passed legislation specifically designed to combat the spam problem.

Directive 95/46/EC (Framework Data Protection Directive) does not deal specifically with electronic communications. Nevertheless, its provisions about the processing of personal data may provide mistakenly neglected and underestimated tools for the discipline of spam. E-mail addresses are considered "personal data"[11], which means that the manner in which they are processed must respect the rules set up by the Directive. Among other things, freely given, informed, specific[12] and unambiguous[13] consent must be provided by the addressee before the address is collected; principles of fair processing practices must be adopted[14]; collectors of e-mail addresses must specify explicit and legitimate collection purposes[15]; adequate information about the collection and use of the e-mail address must be provided to the addressee[16]. In particular, for instance, activities such as the harvesting of e-mail addresses on public Internet places as websites, chat rooms, newsgroups, and so on, are illegal under the terms of the Directive 95/46/EC, constituting unfair processing of personal data, and violating both the purpose limitation principle and the obligation of adequate information principle mentioned above[17]. Similarly, implied consent, use of pre-checked boxes, and broad general requests for consent would not meet the requirements of the Directive with respect to transparency and fairness[18].

Apart from the indirect protection provided by Directive 95/46/EC, the first tentative, and implicit legislative reference to spam is contained in Directive 97/7/EC (Distance Contracts Directive). While the terms of the Directive

[8] EC Communication on "spam" (2004), §3-5.
[9] Recital 5, Dir. 97//7/EC.
[10] Recital 17, Dir. 97//7/EC.
[11] Article 2(a), Dir.95/46/EC.
[12] Article 2(h), Dir. 95/46/EC.
[13] Article 7(a), Dir. 95/46/EC.
[14] Article 6(a), Dir. 95/46/EC.
[15] Article 6(b), Dir. 95/46/EC.
[16] Artt.10, 11, Dir. 95/46/EC.
[17] DPWP, Working Document - Privacy on the Internet (2000), Chapter 4, §IV; DPWP, Recommendation 2/2001, §28; EC Communication on "spam" (2004), §2.3.
[18] DPWP, Working Document - Privacy on the Internet (2000), Chapter 4, §V; Chapter 8, §4.

require prior consent with respect to automated calling systems and facsimile machines[19], for other "means of distance communication" (like e-mail) it states that they can be used only where there is no "clear objection" from the consumer[20]. The Directive 97/7/EC does not define what a "clear objection" is, implicitly suggesting an opt-out system. Similarly, Directive 97/66/EC (Telecommunications Sector Privacy Directive), no longer in force, confirmed the opt-in rule only with regard to automated calling systems without human intervention or fax machines for the purposes of direct marketing[21]. For other means, like e-mail, Member States were required to take "appropriate measures" to ensure that, free of charge, unsolicited calls were not allowed, which left national legislation free to determine whether to rely on opt-in, opt-out, or a mixed system[22]. Not surprisingly, Directive 2000/31/EC (Electronic Commerce Directive), took for granted that Member States could adopt opt-out systems for unsolicited commercial communications by electronic mail[23]. The opt-in system adopted for automated telephone calling systems and facsimile machines was not imposed on e-mail, under a confirmed, but questionable, distinction. Directive 2002/58/EC (Electronic Communications Privacy Directive), which repeals Directive 97/66/EC, finally overcomes the doubts and the resistance about the adoption of a consent-based marketing system for e-mail too[24]. The individual's interest in being spared unsolicited commercial information was finally deemed to be more relevant than the concern that opt-in could hinder the development of e-commerce, discriminating companies in the EU, possibly driving direct marketers to shift their activities outside of the European Union.

3 What spam is

The term "spam" is neither defined nor used by the cited EC Directives, which instead dwell on other definitions: "means of distance communications"[25], "commercial communication"[26], "communication"[27], "electronic mail"[28]. In particular, article 13 (devoted to "unsolicited communications") of the Electronic Communications Privacy Directive of 2002, refers to "electronic mail for the purposes of direct marketing". In other official EU documents, other than laws, spam is variously defined as "the sending in bulk of unsolicited advertising marketing material via e-mail"[29]; or "the practice of sending unsolicited e-mails, usually of a commercial nature, in large numbers and repeatedly to individuals with whom the sender has no previous contact" [30]; or "the repeated mass mailing of unsolicited commercial messages by a sender who disguises or forges his identity"[31]. Some features recur. Spam travels by e-mail, is unsolicited, comes in bulk, has a commercial nature. Therefore, it might be maintained that spam is a synonymous for unsolicited, bulk, commercial, electronic e-mail. Let's analyze article 13 of the Electronic Communications Privacy Directive of 2002 in order to verify this assertion.

Spam is e-mail. "Electronic mail" actually covers any electronic communications where the simultaneous participation of the sender and the recipient is not required, including, beyond "classic" e-mail, SMS, MMS, messages left on answering machines, voice mail service systems, "net send" communications addressed directly to an IP-address, newsletters sent by email[32]. Therefore spam encompasses more than simply "classic" e-mail.

---

[19] Article 10(1), Dir. 97/7/EC.
[20] Article 10(2), Dir. 97/7/EC.
[21] Article 12(1), Dir. 97/66/EC.
[22] Article 12(2), Dir. 97/66/EC.
[23] Article 7(2), and recital 14, Dir. 2000/31/EC.
[24] DPWP, Opinion 7/2000, §2, comment to article 13.
[25] Article 2(4), Dir. 97/7/EC.
[26] Article 2(f), Dir. 2000/31/EC.
[27] Article 2(d), Dir. 2002/58/EC.
[28] Article 2(h), Dir.2002/58/EC.
[29] DPWP, Working Document - Privacy on the Internet (2000), Glossary.
[30] DPWP, Opinion 7/2000, §2, comment to article 13.
[31] Commission – Summary of Study Findings (2001), §2.3.
[32] DPWP, Opinion 5/2004, §3.1.

Spam is unsolicited. In an opt-in system unsolicited communications - communications sent to a user without their prior consent - are illegal. In an opt-out system, they may not be[33]. The first communication, even if not solicited, is legal, so long as the sender complies with other rules governing the communication. Subsequent e-mails, if the recipient of the e-mail does not opt out of receiving additional communications, may be legal too, as they are tolerated (but not solicited). In an opt-in system, therefore, if spam coincides with unsolicited communications, spam is illegal. In an opt-out system, there are unsolicited legal communications (before recipient's opt-out), and unsolicited illegal communications (after recipient's opt-out). In these terms, it may be argued that spam should not coincide with "unsolicited" communications, but with "illegal" communications, sent in a manner that does not fulfill legal requirements. Which would justify the negative perception of the term "spam". In this case, the same unsolicited e-mail sent from a sender for the first time to a recipient in an opt-in system and to a recipient in an opt-out system would qualify as spam (illegal) for the former, but not for the latter. It depends on what law may want to describe with the term "spam": a relationship to a fact (not solicited), or a relationship to the law (not legal).

Spam is commercial. But article 13 of the Electronic Communications Privacy Directive of 2002 refers, more restrictively, to "purposes of direct marketing", eliminating from its title the adjective "commercial", which was contained in article 7 of the earlier Electronic Commerce Directive of 2000. Directive 2002/58/EC defines neither "direct marketing" nor "commercial". As for direct marketing[34], recital 30 of the Framework Data Protection Directive of 1995 describes the "purposes of marketing". Such purposes may be "carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example". In these terms, if "marketing" is stressed, this could lead to apply article 13 of Directive 2002/58/EC of 2002 to "any forms of sales promotion, including direct marketing by charities and political organizations"[35]. A different interpretation could rather stress the difference between activities carried out for commercial purposes and activities carried out by non-profit organizations, applying article 13 only to the former. On the other hand, it may be argued that the direct marketing purposes are more limited than commercial purposes. Which would lead to apply the cited article 13 to spam sent for direct marketing purposes, but not for commercial purposes other than direct marketing. In both cases, the commercial (or direct marketing) qualification may be considered, or not, as a distinguishing qualification for spam. Again, the legal system leaves two options opened. Either spam may be both commercial and non-commercial, or spam requires commercial (or direct marketing) purposes to be defined as such.

Spam is bulk. While spam is usually associated with mass mailing, the definition of spam in article 13 of Directive 2002/58/EC does not depend on a minimum amount of e-mail sent, which may lead to questionable consequences. For instance, a single e-mail, sent with a CV attached to be evaluated for a possible job may be defined as spam, as long as sending out CVs constitutes a direct marketing activity. On the other hand, placing a minimum number for commercial communications to qualify as spam might lower the level of protection. Thus in the EU legal system in force, quantity is not a necessary feature for spam, as article 13 of Directive 2002/58/EC does not specify that the sending of e-mail (or faxes) is illegal only when a minimum quantity is exceeded.

To sum up, while spam is commonly perceived as unsolicited, bulk, commercial (and illegal) e-mail, in legal terms it may take different forms, combining the cited features in different ways, and ranging from simple commercial communications; to e-mail for direct marketing purposes; to illegal electronic communications. Whether or not spam is legal depends upon the opt-in or opt-out choice exercised by the recipient of the communications, and on the legal system of reference.

---

[33] Article 7(1), Dir.2000/31/EC.

[34] A definition of "direct marketing" has been used in the FEDMA (Federation of European Direct Marketing) European Code of Practice for the Use of Personal Data in Direct Marketing (approved by the DPWP Opinion 3/2003): "The communication by whatever means (including but not limited to mail, fax, telephone, on-line services, etc…) of any advertising or marketing material, which is carried out by the Direct Marketer itself or on its behalf and which is directed to particular individuals."

[35] DPWP, Opinion 5/2004, §3.3.

4 The manner of consent

The opt-in system chosen by the Electronic Communications Privacy Directive of 2002 represents the arrival point of EU regulations on unsolicited commercial communications. The legislator thought that opt-in could protect individuals more effectively, and meet the expectations of users, Internet service providers and industry itself more properly[36] Moreover an opt-in system requires a simpler legislative framework, is more easily implemented, allows more efficient advertising[37], and, at least theoretically, ensures stricter rules, more likely to curb spam. According to article 13 of Directive 2002/58/EC, the use of "electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent"[38]. The opt-in "radical" choice is clear. Nevertheless, Directive 2002/58/EC introduces some succinct rules, and some exceptions to a straight opt-in model, that reveal some heritage of the previous opt-out system.

An interpretative issue may be related to e-mail addresses not associated with a subscriber, like addresses provided by companies or within a family. In these cases, as the prior consent must be given by the subscriber, the alternative to a lack of protection, is represented by the consent given by the subscriber[39], who is not, on the other hand, the actual user[40]. But, as e-mail addresses are personal data, it follows that an autonomous protection derives from the Framework Data Protection Directive of 1995[41]. Even if the address is not associated with a subscriber, and therefore protected by Directive 2002/58/EC, it is associated with the user, and therefore protected by Directive 95/46/EC. An analogous issue may be related to e-mail addresses contained in a mailing list. It may be argued that the prior consent must be given by the list-owner, which means that participants in the list may protect their privacy only unsubscribing from the list. Alternatively, it may be maintained that each participant may block unsolicited commercial communications for the whole list. Unless technical solutions allow to separately managing each e-mail address of the list, with respective preferences, the answer depends on the choice about who is to be protected, between a contractual vision (the subscriber to the communication service, the list owner) and a more personal vision (the user of the service, the list participant).

Electronic contact details, obtained from customers in the context of the sale of a product or a service, may be used for direct marketing of similar products or services[42]. This approach has been characterized as a "soft opt-in". The opt-in may not, in fact, be that soft, as customers must be given the opportunity to object, free of charge and in an easy manner, to the use of their details both when they are collected and on the occasion of each subsequent direct marketing message[43]. Together with the electronic details, the consent of the user is collected. The real difference with the "hard" opt-in is the factual circumstance of the collection of the consent - a sale - but in both cases data must be obtained in accordance with the Framework Data Protection Directive of 1995. In fact, the chance to object to such use is necessarily related to the provision of adequate information on the use itself. The "previous sale" exception is therefore limited in several ways, and it must be interpreted restrictively[44]. There must have been a "sale", not just a vague commercial relationship; the use of electronic contact details is limited to the "same company", which rules out subsidiaries or mother companies[45]; and direct marketing must be limited to "similar" products or services, where similarity should be judged from the reasonable expectations of the recipient[46]. In these terms, if correctly applied, the collection of the electronic details in the context of a sale represents an alternative method to negotiate, and possibly obtain, prior consent for commercial communications.

---

[36] DPWP, Opinion 7/2000, §2, comment to article 13.
[37] Commission – Summary of Study Findings (2001).
[38] Article 13(1), Dir. 2002/58/EC; recital 17, Dir. 2002/58/EC.
[39] Article 2(k), Dir. 2002/21/EC.
[40] Article 2(a), Dir.2002/58/EC.
[41] DPWP, Opinion 5/2004, §3.4.
[42] Article 13(2), Dir. 2002/58/EC.
[43] Recital 41, Dir. 2002/58/EC.
[44] DPWP, Opinion 5/2004, §3.5.
[45] DPWP, Opinion 5/2004, §3.5.
[46] DPWP, Opinion 5/2004, §3.5.

Directive 2002/58/EC prohibits the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender, or without a valid address where the recipient can exercise the opt-out[47]. Such a prohibition is motivated by effective enforcement of EC rules[48], but it sounds somehow redundant, as unsolicited communications are prohibited in any case. In an opt-out approach, disguising or concealing identities and return addresses would make a commercial communication illegal. In an opt-in setting, it would mainly reinforce the degree of illegality. It is possible, but unlikely, that a sender who has obtained a valid prior consent, violates the provision. It is more likely that disguising or concealing occurs when the sender has not collected any valid consent. Moreover, the "disguising and concealing" violates, again, the Framework Data Protection Directive of 1995, as others' personal data are processed without consent.

Finally, Directive 2002/58/EC states that the opt-in system applies to natural persons only. As for legal persons, Member States must ensure sufficient protection of "subscribers other than natural persons" from spam[49]. While the legal distinction between natural and legal persons looks clear, compliance by senders with two different systems - opt-in for natural persons, opt-out for legal persons - may not be that easy. E-mail addresses do not always show whether the recipient is a natural person or a legal person. In these terms, the sender must carefully verify the nature of the recipient[50], or risk engaging in an illegal activity. Including legal persons in a compulsory opt-in scheme might be a rational and simplifying choice.

5 The ancillary tools

Some doubts relate to ancillary legal tools that accompany the basic rules cited above. Notwithstanding the adoption of an opt-in system, the EU Directives in force contain some provisions setting up tools thought for opt-out systems. EU Directives take into consideration filtering and labeling as tools useful for better implementation, and in particular to avoid the costs that spam imposes for the recipient. Thus, the Electronic Communications Privacy Directive of 2002 promotes and encourages industry filtering initiatives[51], through e-mail systems arrangements that allow subscribers to view the sender and the subject line of an e-mail and to delete messages without having to download the content or attachments[52]. This means that Member States must ensure that such commercial communication by a service provider established in their territory is clearly and unambiguously identifiable as such "as soon as it is received by the recipient"[53], for instance with an "ADV" label in the subject line. Apart from issues about free expression and forced speech, that are more sensitive in the US than in the EU, an "ADV" label is more coherent with an opt-out system, where different kinds of commercial communications can be received. In an opt-in system, the commercial communications received either is legitimate, and solicited, with a prior consent, or is illegal, and in this case the label would not make it legal.

Directive 2002/58/EC leaves the protection of the legitimate interests of legal persons to Member States, which must ensure sufficient protection. The Directive may, in fact, establish an opt-out registry for spam[54], which is not compatible with an opt-in system. "Opt-out registers" (or "Do Not E-mail lists") were already considered by the Electronic Commerce Directive of 2000, which imposed service providers undertaking unsolicited commercial communications by electronic mail to consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications could register themselves[55]. Besides, "Do Not E-mail lists"

[47] Article 13(4), Dir. 2002/58/EC.
[48] Recital 43, Dir. 2002/58/EC.
[49] Article 13(5), Dir. 2002/58/EC.
[50] DPWP, Opinion 5/2004, §3.4.
[51] Recital 30, Dir.2000/31/EC.
[52] Recital 44, Dir. 2002/58/EC.
[53] Article 7, Dir. 2000/31/EC.
[54] Article 13(5), Dir. 2002/58/EC; recital 44, Dir. 2002/58/EC.
[55] Article 7(2), Dir.2000/31/EC; recital 31, Dir. 2002/58/EC.

may be dangerous for users' privacy, unless created as domain level registries. E-mail address based registers, collecting and possibly disclosing individual e-mail addresses, threaten privacy instead of protecting it. Moreover, particularly considering cross-borders activities, they may involve burdensome activities for users (especially if they change regularly their e-mail addresses, possibly as a self-help measure against spam) for direct marketers (who should constantly check them), and for authorities or organizations charged to manage and keep them up-to-date. Apart from security concerns, the risk is to end up with a Big Brother, or many scarcely known Smaller Brothers, which would make it even harder for users to orientate and for direct marketers to comply.

Codes of conduct are other tools considered by Directives, and they have been promoted since Directive 95/46/EC[56]. Before Directive 2002/58/EC, self-regulation had been considered the main regulatory instrument for fighting spam[57]. Directive 2000/31/EC encourages "professional associations and bodies to establish codes of conduct at Community level in order to determine the types of information that can be given for the purposes of commercial communication"[58]. The same Directive tries to make codes of conducts more transparent, favoring the voluntary dissemination of draft codes of conduct, the accessibility of them by the public, and the "involvement of associations or organisations representing consumers in the drafting and implementation of codes of conduct affecting their interests"[59]. Evidence showed that self-regulation alone, even if subjected to procedural steps aimed at making it more reliable[60] and transparent, failed. While self-regulation intended as self-limitation is clearly not suitable to discipline a sensitive matter as spam, even self-regulation intended as participated co-regulation cannot be the only regulatory reference, and legislation is needed, especially to make enforcement possible. Again, self-regulation, codes of conduct, quality labels and good marketing practices are far less necessary in an opt-in system than in an opt-out system, as an opt-in approach is a more autonomous, complete and enforceable approach than opt-out.

While EU Directives do not cite "Spam Boxes" as possible tools, some national Data Protection Authorities[61] have adopted such initiatives, backed by other official EU documents. Users may forward the spam they receive to "Spam Boxes", created by DPAs, activating enforcement mechanisms. "Spam Boxes", even without bounties, encourage consumers to report infringements, favoring a more diffused and effective enforcement of adopted legislation, and providing DPAs with data and statistics. "Spam Boxes" are an easy, direct and cheap way of complaining and reporting violations, a sort of "one-click away" hotline. The user need only forward the unwanted spam to the spam box, and does not have to explain how the spam occurred in writing or by calling.

Finally, contracts can be of help in the fight against spam, through the adaptation of terms and conditions of subscriber contracts to the opt-in system. Internet service providers (ISPs), e-mail service providers (ESPs), and providers of mobile services, should include obligations in contracts prohibiting the use of their services for sending spam, and provide information on anti-spam filters, and other tools that can be used by subscribers to control spam[62]. Effective contractual penalties should be set up in case of breach.

6 Conclusion

The evolution of the EU legal system shows how self-regulation and an opt-out system failed in curbing spam. The opt-in choice, adopted by Electronic Communications Privacy Directive of 2002, is the response EU considers more rational, proper, effective and respectful of the main interest to be protected: the individual's privacy. This rules out neither the need to sign international agreements, in order to co-ordinate different systems (opt-in and opt-out), nor

[56] Article 27, Dir. 95/46/EC.
[57] Recital 32, Dir.2000/31/EC; see also recital 41, Dir.2000/31/EC.
[58] Article 8(2), Dir.2000/31/EC.
[59] Article 16(2), Dir. 2000/31/EC.
[60] DPWP, Opinion 3/2003; see also article 30, Dir. 95/46/EC.
[61] For instance, by the French 'Commission Nationale Informatique et Libertés (CNIL)' and the Belgian 'Commission de la Protection de la Vie Privée (CPVP).
[62] EC Communication on "spam" (2004), §4.1.2.

to rely on other regulatory tools (as law alone is not sufficient). EU regulates, and puts forward a policy proposal at the same time. As for article 13 of Directive 2002/58/EC, which contains the basic rules on unsolicited commercial communications, it shows how some traces of the previous opt-out system have survived, making the discipline somehow less coherent in some parts. Finally, there is a need to define what spam is, as the frequently used term "spam" is not a legal term, which may involve some misunderstandings about the real object of the discipline.

References (EU materials)

EU Directives and Decisions:

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
http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett

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 contracts
http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31997L0007&model=guichett

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
http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l_024/l_02419980130en00010008.pdf

1999/168/EC: Council Decision of 25 January 1999 adopting a specific programme for research, technological development and demonstration on a user- friendly information society (1998 to 2002)
http://europa.eu.int/eur-lex/pri/en/oj/dat/1999/l_064/l_06419990312en00200039.pdf

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce")
http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services ("Framework Directive")
http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_108/l_10820020424en00330050.pdf

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")
http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf

Data Protection Working Party documents:

Data Protection Working Party - Opinion 7/2000 on the European Commission proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 (2 November 2000)
http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2000/wp36en.pdf

Data Protection Working Party, Working Document, Privacy on the Internet – An Integrated EU Approach to On-line Data Protection (21 November 2000)
http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2000/wp37en.pdf

Data Protection Working Party - Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union (17 May 2001)
http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2001/wp43en.pdf

Data Protection Working Party - Opinion 3/2003 on the European code of conduct of FEDMA for the use of personal data in direct marketing (13 June 2003)
http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp77_en.pdf

Data Protection Working Party - Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC (27 February 2004)
http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp90_en.pdf

Other EU documents:

Commission of the European Communities - Unsolicited commercial communications and data protection – Summary of Study Findings – January 2001
http://europa.eu.int/comm/internal_market/privacy/docs/studies/spamsum_en.pdf

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" (22 January 2004)
http://europa.eu.int/information_society/topics/ecomm/doc/useful_information/library/communic_reports/spam/spam_com_2004_28_en.pdf