

**PRINCIPLES AND REGULATIONS ABOUT ONLINE PRIVACY:  
“IMPLEMENTATION DIVIDE” AND MISUNDERSTANDINGS  
IN THE EUROPEAN UNION**

*Nicola Lugaresi, Associate Professor  
University of Trento, Law School and Department of Legal Sciences  
lugaresi@jus.unitn.it*

*1. Foreword: the European Union approach to privacy - 2. The “missing definition” misunderstanding: personal data protection is not privacy protection - 3. The concept of privacy: what privacy really is about - 4. Offline privacy and online privacy: different problems, same rules? - 5. The EU regulation of online privacy: improvements and inconsistencies*

**1. Foreword: the European Union approach to privacy**

European Union values privacy, online and offline. Who does not? EU repeatedly declares its love for privacy. But, as it often happens, the object of our own love is somehow unknown, the ways we feel or we decide to love someone are not the right ways, misunderstandings occur, and we may hurt, instead of protecting, what we love.

Speaking of general principles, privacy is acknowledged from EU as a fundamental right and freedom. Article 7 (“Respect for private and family life”) of the Charter of Fundamental Rights of the European Union (Nice, 2000) affirms that “everyone has the right to respect for his or her private and family life, home and communications”.

Article 7 of the Charter of Nice has drawn on article 8, §1, of the Council of Europe<sup>1</sup> Convention for the Protection of Human Rights and Fundamental Freedoms (Rome, 1950), whose wording is the same (apart from a politically correct amendment). Oddly, article 7 of the EU Charter does not draw on article 8, §2, of the CoE Convention, which prohibits interferences from

---

<sup>1</sup> The Council of Europe is an organization, different from European Union, open to any European state which accepts the principle of the rule of law and guarantees human rights and fundamental freedoms to everyone under its jurisdiction: almost all European countries (and all EU members) are part of CoE.

public authorities, with exceptions, in accordance with the law, due to public interests, or to rights of freedoms of others<sup>2</sup>.

Article 17 of the United Nations International Covenant on Civil and Political Rights (1966), which protects from “arbitrary or unlawful interference” not only “family, home or correspondence”, but also “privacy”, is another touchstone for following declarations of principles and implementing laws.

However, the exact borders of the concept of privacy, and consequently of its protection, cannot be drawn by the EU Charter, whose vagueness is consistent with its extremely general objective. What may trouble individuals is, on one side, that, among all the declarations of principles, article 7 of the EU charter is quite bare and partially incomplete in comparison with others, and, on the other side, that Directives and official EU documents do not provide criteria to clearly define what privacy is.

As regards privacy on the Internet, technical and jurisdictional issues make things more complex, and not surprisingly there are neither Regulations nor Directives specifically devoted to online privacy. On the other hand, both Directive 95/46/EC<sup>3</sup>, on the protection of personal data, and Directive 2002/58/EC<sup>4</sup>, concerning the electronic communications sector, also apply to privacy in the information society services, or, more precisely, to personal data on the Internet<sup>5</sup>, establishing a Community legal framework<sup>6</sup>.

Directive 95/46/EC provides a general framework for the protection of personal information, representing the horizontal privacy legislation, or rather the horizontal data protection legislation, whose provisions apply to cases more specific Directives do not regulate. For instance, it applies to private communications services, as the electronic communications Directive applies only to public communications services.

---

<sup>2</sup> See article 8, §2, CoE Convention of Rome: “there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.

<sup>3</sup> Directive 95/46/EC 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.

<sup>4</sup> Directive 2002/58/EC 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”).

<sup>5</sup> See Data Protection Working Party, Recommendation 2/2001 of 17 May 2001, providing a minimum set of obligations and concrete indications on how the rules set out in the personal data protection Directives “should be applied to the most common processing tasks carried out via the Internet” (§1).

<sup>6</sup> See recital 14, Directive 2000/31/EC.

On one hand, Directive 2002/58/EC adapts the contents of Directive 97/66/EC<sup>7</sup>, repealing and replacing it, to technological and market developments in the electronic communications services sector, in order to provide a satisfactory level of protection of personal data and privacy for users<sup>8</sup>; on the other hand, it particularizes and complements Directive 95/46/EC<sup>9</sup>.

Directive 2002/58/EC does not apply to activities concerning public and State security and defense<sup>10</sup>, not affecting the power of Member States to carry out lawful interceptions of communications and to adopt other measures, provided that they are necessary, appropriate and strictly proportionate to the intended purposes<sup>11</sup>.

Moreover, there are other Directives which may have provisions affecting privacy, such as Directives concerning distance contracts<sup>12</sup>, telecommunications terminal equipment<sup>13</sup>, e-commerce<sup>14</sup>, copyright<sup>15</sup>, digital signatures<sup>16</sup>, electronic communications networks and services<sup>17</sup>.

---

<sup>7</sup> Directive 97/66/EC of 15 December 1997, concerning the processing of personal data and the protection of privacy in the telecommunications sector: formally, Directive 97/66/EC referred therefore to telecommunications, while Directive 2002/58/EC refers to electronic communications.

<sup>8</sup> See recital 4, Directive 2002/58/EC; see also art.8, §4, Directive 2002/21/EC, framework Directive on electronic communications networks and services.

<sup>9</sup> See article 1, §2, Directive 2002/58/EC; see also recital 10 of the Directive: “in the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals”.

<sup>10</sup> See article 1, §3, Directive 2002/58/EC, according to article 3, §2, Directive 95/46/EC.

<sup>11</sup> See recital 11, Directive 2002/58/EC.

<sup>12</sup> Directive 97/7/EC of 20 May 1997, on the protection of consumers in respect of distance contracts.

<sup>13</sup> Directive 1999/5/EC of 9 March 1999, on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity; as for privacy protection, the Directive considers the incorporation of safeguards into apparatus of particular types, “to ensure that the personal data and privacy of the user and of the subscriber are protected”.

<sup>14</sup> Directive 2000/31/EC of 8 June 2000, on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (“Directive on Electronic Commerce”).

<sup>15</sup> Directive 2001/29/EC of 22 May 2001, on the harmonisation of certain aspects of copyright and related rights in the information society; as for privacy protection, the Directive states that any such copyright management information systems, which may, depending on their design, process personal data about the consumption patterns and allow for tracing of online behavior, “should incorporate privacy safeguards in accordance with Directive 95/46/EC”.

<sup>16</sup> Directive 1999/93/EC of 13 December 1999, on a Community framework for electronic signatures.

<sup>17</sup> Directive 2002/19/EC of 7 March 2002, on access to, and interconnection of, electronic communications networks and associated facilities (“Access Directive”); Directive 2002/20/EC of 7 March 2002, on the authorisation of electronic communications networks and services (“Authorisation Directive”); Directive 2002/21/EC of 7 March 2002, on a common regulatory framework for electronic communications networks and services (“Framework Directive”); Directive 2002/22/EC of 7 March 2002, on universal service and users’ rights relating to electronic communications networks and services (“Universal Service Directive”).

Furthermore, EU issues other official documents, like Recommendations, concerning other aspects, as the protection of minors and human dignity<sup>18</sup>, intertwined with privacy. On the contrary, there are no Regulations about privacy, as strict provisions directed to States and citizens, without any chance to adapt them to the respective legal systems, are inconsistent with the discipline of a fundamental right, like privacy.

Online privacy is not a specific target of the Directives in force, but it is not excluded, which means that their provisions must be adapted to online issues. Even if there is no Directive dealing in particular with online privacy, EU is not reluctant to regulate privacy, communications and the Internet. Though, in spite of its regulatory intervention and of the general statements of principle, EU regulation of online privacy, as resulting from the horizontal Directive and from the electronic communications Directive, is not always satisfactory.

From a comparative point of view, unlike the United States, which relies on a sectoral approach to privacy based on a mix of legislation, regulation and self-regulation<sup>19</sup>, EU relies on a deeper and more comprehensive legislative framework<sup>20</sup>. As a civil law system, where the role of case law is less relevant in the creation of law compared to common law systems, EU needs more precise legislation.

As for principles, while the EU has a specific article of its recent Charter of Rights devoted to privacy, US far more ancient Bill of Rights has no provisions about it. That said, expectations of privacy, both online and offline, should be higher in the EU than in the US. Which is not always the case.

The point is that privacy is something particularly inborn into American culture and society, while in the European Union the legislation, and not the common feeling of people, is the driving force towards the respect, protection and acknowledgement of the right to privacy. In a way, privacy is more an “imposed”, or at least “suggested”, right than a genuinely felt right, and EU citizens look less wary, especially towards Government, about invasions of privacy than US citizens.

Privacy, online and offline, is a wonderful right, freedom and principle. Its fascination comes from its intimate contents, which is its major problem as well when confused with abstractness. Protection of privacy cannot be complete and satisfying without defining its sides and

---

<sup>18</sup> Council Recommendation 98/560/EC of 24 September 1998, on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity.

<sup>19</sup> See L. LESSIG, *Code and other laws of cyberspace*, Basic Books, New York, NY (1999): 159.

<sup>20</sup> See the Safe Harbor Privacy Principles, issued by the US Department of Commerce on 21 July 2000, Annex I to the Commission Decision 2000/520/EC of 26 July 2000, on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions.

the means to protect it. As for EU, and apart from jurisdictional and technological problems concerning privacy online, there are some misunderstandings needing some analysis and focus. The main misunderstanding is about the concept itself of privacy that official EU documents imply (the concept of privacy is not defined in the cited Directives), and in particular, on the relationship with personal data protection. As far as online privacy is concerned, Directive 2002/58/EC has improved the general framework to some extent, but some lacunae and inconsistencies have survived.

## **2. The “missing definition” misunderstanding: personal data protection is not privacy protection**

While European Community law is inclined to define every concept and notion before starting the regulatory part, as almost any Directive and Regulation show in their “Definitions” introductory articles, there is no definition of privacy provided, either by the sectoral Directives or by other official documents. This is understandable on one side, as it is not an easy task to define privacy, but it is dangerous on the other side, as the lack of criteria may be misleading and detrimental for the interests at stake.

As regards online privacy in particular, this means that the protection of privacy is often adjusted to meet the needs of personal data protection, that is the real object of the Directives, which is a very restrictive approach, as privacy concerns many more interests than personal information<sup>21</sup>, and should not be limited to it.

The point is that data protection alone does not meet privacy needs. It may be a part of privacy, the more visible, and tradable part. It may be an instrument, a tool for the protection (or for the threat) of the other sides of privacy. It may be something different, obviously related, but still separate from privacy. The only sure thing is that there is no perfect coincidence.

EC Directives concern mainly personal data protection, but still they are known as “privacy” Directives (the title of Directive 95/46/EC does not even mention privacy), probably under the influence of English speaking countries<sup>22</sup>. The provisions of the Directives mention

---

<sup>21</sup> See J. REIDENBERG, *Setting Standard for Fair Information Practice in the U.S. Private Sector*, 80 *Iowa L. Rev.* (1995): 497.

<sup>22</sup> For example, the “Safe harbor” principles, issued by the US Department of Commerce having regard to the data protection Directive 95/46/EC, are named “Safe harbor privacy principles”.

privacy protection in several points, but without marking the boundaries with personal data protection.

Regulatory authorities and boards stemming from these Directives, whose names refer to data protection, are equally known as “privacy” bodies (the Italian body, the Personal Data Privacy Commissioner is commonly referred to as the “Garante” for privacy, not for personal data), even because they try to extend their jurisdiction beyond data protection. The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data (known as Article 29 Working Party, or as Data Protection Working Party), set up by article 29 of the Directive 95/46/CE, declares itself as the independent EU advisory body (according to article 29), on “data protection and privacy”<sup>23</sup>.

It is not just a semantic simplification, as data protection has absorbed most of regulatory efforts, leaving other sides of privacy exposed. That means that European Union protects personal data, but does not protect privacy, as long as personal data are not involved. The consequences are far more serious online than offline due to the lack of knowledge and to the limited technological resources individuals have in order to defend themselves, from both the Government and the private sector.

If citizens enter a cybercafé, sign up for an e-mail account through a webmail service, give false identities, pay with cash, avoid to provide personal information while browsing, and follow other precautions to preserve their anonymity, they are not covered by the “privacy Directives”, which define personal data as “any information relating to an identified or identifiable natural person”<sup>24</sup>. In fact, they cannot be identified, directly or indirectly, as requested by the Directive in order to meet the requisite of being identifiable. Nevertheless, they are likely to receive junk e-mail in their inbox, or personalized banners while navigating, which means their browsing has been tracked and they have been profiled. Moreover, third parties might read their correspondence, sent to other “paranoid” anonymous individuals reading and typing from a different Internet point.

Has their privacy being invaded? Or the fact that they are anonymous users makes them lose the protection provided by the horizontal Directive and the sectoral Directives? Is not privacy a right for individuals? They have been spammed, they have been analyzed, maybe their e-mail has been eavesdropped, no matter if it is known, or can be known, who they really are. Apart from

---

<sup>23</sup> Data Protection Working Party, Recommendation 1/2000 of 3 February 2000, on the implementation of Directive 95/46/EC.

<sup>24</sup> Article 2, Directive 95/46/EC; the same definitions applies to Directive 2002/58/EC.

practical consequences, their right to be let alone has been violated, their sphere of intimacy has been intruded.

An alternative way to protect anonymous individuals' privacy under EU Directives might be to broadly interpret the definition of personal data. The anonymous customers of cybercafés might be followed at home and identified, after all, so they are identifiable. In this case, everyone, everywhere, would be always identifiable, and the definition would lose its significance and its scope. The Directive could have referred to “any information relating to a natural person” no matter if identified or identifiable.

The protection of anonymity<sup>25</sup>, in the limits conceded by the legal system<sup>26</sup>, should not be restricted to the protection of the desire to stay anonymous<sup>27</sup>, with particular reference to electronic communications services<sup>28</sup>. It should comprehend the enjoyment of all the rights consistent with the state of anonymity<sup>29</sup>, including the protection of data like one's own e-mail address<sup>30</sup>. Many sides of privacy are consistent with such a state, and the dividing line between personal data and anonymous data is not clear in the regulations about privacy<sup>31</sup>.

Privacy is not just a relationship between individuals and their data, but it is something far more complex, deep and composite, between individuals and the external world. The fact is that while privacy issues have been present for a long time in the legal arena, data protection issues have

---

<sup>25</sup> See recital 9 of the Directive 2002/58/EC, considering the use of anonymous or pseudonymous data “where possible”; see also recital 14, Directive 2000/31/EC, stating that the e-commerce Directive “cannot prevent the anonymous use of open networks such as the Internet”.

<sup>26</sup> See the Opinion of the Economic and Social Committee of 28 November 2001 on child protection on the Internet, which foresees a new distinction to be redrawn between privacy and traceability after the attacks of 11 September.

<sup>27</sup> See CoE Recommendation No. R(99)5, which, aware “of the need to develop techniques which permit the anonymity of data subjects” (Preamble), and admitting that “complete anonymity may not be appropriate because of legal constraints” (§II.4), nevertheless recognizes that “anonymous access to and use of services, and anonymous means of making payments, are the best protection of privacy” (§II.3); Internet service providers are invited to inform users both “about the possibilities of accessing the Internet anonymously, and using its services and paying for them in an anonymous way”, and “of programmes allowing them to search and browse anonymously on the Internet”; when legal constraints stand against complete anonymity, ISPs should offer them “the possibility of using pseudonyms” (§III.4).

<sup>28</sup> See recital 33, Directive 58/2002/EC: “Member States should encourage the development of electronic communication service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services”.

<sup>29</sup> See CoE Recommendation No. R(95)4: “anonymous means of accessing the telecommunication network should be made available” (Appendix, §2.2).

<sup>30</sup> See CoE Recommendation No. R(99)5, stating that “e-mail address is personal data” (§II.4).

<sup>31</sup> The OECD Guidelines (1980) leave the drawing of such a distinction to each Member country; see also the Explanatory Memorandum to the OECD Guidelines: personal data are intended “in the sense of information relating to identified or identifiable individuals”, conveying information “which by direct (e.g. a civil registration number) or indirect linkages (e.g. an address) may be connected to a particular physical person” (§41).

emerged recently, distracting the attention of the legislator from the general framework. Certainly, personal data have two relevant features attracting legal provisions: they are “visible”, material, and they have an immediate economic value, as e-commerce and direct marketing demonstrate. But this does not justify why the other sides of privacy have been neglected.

As for the early general declarations of principles on fundamental rights, data protection does not have specific provisions. Article 8 of the CoE Convention of 1950 protects the right to private and family life, home, correspondence. Article 17 of the UN International Covenant of 1966 protects privacy, family, home and correspondence. Personal data are not mentioned, even if they are implicitly protected as a part of the individual’s privacy.

Then personal data appear as a separate object of protection. Sectoral Conventions add to general Declarations of rights. The CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, 1981) takes into account the risks provoked by automatic data processing. The link with privacy is not denied: the purpose of the Convention is to secure individual’s rights and freedoms, “and in particular his right to privacy, with regard to automatic processing of personal data relating to him” (article 1, CoE Convention of Strasbourg).

However, article 1 of the Convention is misleading as well. Defining this protection as “data protection” makes it look like data are protected, while, instead, the individual should be protected from others’ abuse of his/her data. The real object of the protection must be the individual first, not personal data and information<sup>32</sup>.

When I receive junk e-mail to my e-mail address, which has been published on the law school website, it is not the fact that my “public” e-mail address is on a spammer’s list that irritates me most. The address has not been stolen. Collecting e-mail addresses in online public spaces may be considered unlawful, as it is contrary to article 6, §1(a) (fair processing), article 6, §1(b) (specified, explicit and legitimate purposes) and article 7(f) (balance between legitimate interests pursued by the controller and interests for fundamental rights and freedoms of the data subject) of the Directive 95/46/EC<sup>33</sup>. But what really upsets me, is receiving unsolicited and unwanted bulk e-mail that I consider not only a nuisance, but also a violation of my privacy. Data are relevant, to some extent they can be considered under a proprietary point of view, but their protection is just functional to the protection of privacy, and they should not be the main targets of protection.

---

<sup>32</sup> See the Safe Harbor Privacy Principles, issued by the US Department of Commerce, using “personal data” and “personal information” as synonyms (“data about an identified or identifiable individual”).

On the other hand, one year before the CoE Strasbourg Convention, the Organisation for Economic Co-operation and Development (OECD), considering the increase in automatic data processing, and the consequent need to deal with privacy protection in relation to personal data, had issued a Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980). The Guidelines<sup>34</sup>, recognizing the interest of Member countries in protecting privacy and individual liberties, mix up the two objects of protection, and consider privacy as a competing value with the free flow of information, whose social and economic relevance is acknowledged.

The OECD Guidelines apply to personal data posing “a danger to privacy and individual liberties”, due to the manner in which they are processed or to the nature or context in which they are used<sup>35</sup>. It is clear that it is not as much important to protect data, as to protect the individual from the use of data. The principles stated are the bases of following Member countries and EU data regulations (collection limitation, data quality; purpose specification; use limitation; security safeguards; openness; individual participation; accountability<sup>36</sup>).

The Explanatory Memorandum to the OECD Guidelines involuntarily underscores the difficult distinction between privacy protection and personal data protection. After remarking the intensified legislative activities concerning the protection of privacy with respect to the collection and use of personal data, the Memorandum suggests a new classification, starting from an unproven proposition. The Memorandum distinguishes privacy in the classical sense, “i.e. abuse or disclosure of intimate personal data”, in opposition to a broadened concept of privacy identifying “a more complex synthesis of interests which can perhaps more correctly be termed privacy and individual liberties”<sup>37</sup>.

The process is logic, but it goes somehow backwards. Privacy is a complex concept, and its traditional sense, from Warren and Brandeis onwards<sup>38</sup>, has always contained material sides and

<sup>33</sup> See Data Protection Working Party, Working Document of 21 November 2000, on Privacy on the Internet (Chapter 4, §V); see also Data Protection Working Party, Recommendation 2/2001 of 17 May 2001 (§28).

<sup>34</sup> The OECD Explanatory Memorandum specifies that the Guidelines do not constitute a set of general privacy protection principles, as it is out of their scope to deal with other invasions of privacy (“by, for instance, candid photography, physical maltreatment, or defamation”) not associated with the handling of personal data (§38).

<sup>35</sup> OECD Guidelines, §2; see also the Explanatory Memorandum to the OECD Guidelines, §43, citing, without specifying, other dangers (“a broad variety of other possible risks”) implied than the ones provoked by the use of automated data processing methods.

<sup>36</sup> OECD Guidelines, §§7-14.

<sup>37</sup> OECD Memorandum, §2.

<sup>38</sup> See S. WARREN, L.D. BRANDEIS, *The Right to Privacy*, 4 *Harr. L. Rev.* (1890).

psychological, almost “metaphysical”, sides. The need to define “this” broad concept of privacy as something “more” (privacy and liberties) unnecessarily creates two levels of privacy. The protection of personal data is functional to the protection of privacy, as the protection of privacy may be functional to the protection and the promotion of other rights and freedoms, but privacy has its own dignity and its own peculiarities, and it needs neither to be split into nor to be merged with other rights, freedoms or liberties.

The EU legislator has drawn its inspiration from the OECD Guidelines on transborder flows on personal data, which provide minimum standards for domestic legislation, but are not legally binding, and from the CoE Convention on automatic processing of data<sup>39</sup>, which is binding among the ratifying countries. Unfortunately, while the general principles stated by the UN in the International Covenant, or by the same CoE in the Convention of Rome, considered privacy in itself, with no specific reference to personal data, OECD Guidelines and CoE Strasbourg Convention shifted their attention to data, flows of data, and processing of data, and privacy has become a sort of a side issue. If it is true that data protection is more suitable to be regulated than privacy protection, it is also true that this deep focusing on data has not helped the correct legal understanding of privacy issues.

Not surprisingly, data protection earned its own article, under Chapter II (“Freedoms”), in the EU Charter of Fundamental Rights, just after the article devoted to privacy. While article 7 protects private and family life, article 8, §1, of the Charter declares that “everyone has the right to the protection of personal data” concerning them, listing the related basic principles: fair process; specified purposes; consent or other legitimate basis; access and rectification; control by an independent authority.

Besides, while private and family life must be object of “respect”, personal data are the object of “protection”. Even if in a declaration of principles the two terms may be considered as equivalent, due to the political goals of the EU Charter, it may seem strange that an apparently less penetrating term is used with reference to the real right, privacy. On the other hand, data can be collected, used, misused, and protected, but not respected, while privacy, in its intimate and personal sense, can and must be not only protected, but also respected.

As far as “data protection Directives” are concerned, not only they refrain from identifying the concept of privacy, but they also tend to use the term “privacy” in a confused and extempore way, in various associations with personal data.

---

<sup>39</sup> See recital 11, Directive 95/46/EC.

Directive 95/46/EC acknowledges the value of the right to privacy as a fundamental right and freedom, to be respected by data-processing systems<sup>40</sup>, and to be harmonized, through an approximation of laws<sup>41</sup>. Likewise, Directive 2002/58/EC acknowledges the same value, but it refers more to general declaration of principles than to data protection Conventions. In these terms, it refers to article 7 and article 8 of the Charter of Nice<sup>42</sup> and, as regards confidentiality of communications, to the CoE Convention for the Protection of Human Rights<sup>43</sup>. Besides, Directive 2002/58/EC stresses the risks to privacy that digital networks and publicly available electronic communications services increasingly pose<sup>44</sup>.

A similar path has been followed by CoE Recommendations, devoted to the protection of personal data, related to payments<sup>45</sup>, held by public bodies<sup>46</sup>, or in the area of telecommunication services<sup>47</sup>. Although privacy is not cited in their titles, the CoE Recommendations highlight the risk and the infringements to the privacy of the individuals deriving from the misuse of automated data processing. Each Recommendation affirms the necessary respect for privacy: in itself<sup>48</sup>, connected to data protection<sup>49</sup>, connected to secrecy of correspondence and freedom of communication<sup>50</sup>. However, it is in the Recommendation devoted to the processing of personal data on the Internet that privacy appears in the title<sup>51</sup>. The Recommendation states that respect for privacy is a fundamental right of each individual, which may “also” be protected by data protection

---

<sup>40</sup> See article 1, recitals 2 and 10, Directive 95/46/EC.

<sup>41</sup> See recitals 7 and 9, Directive 95/46/EC.

<sup>42</sup> See recital 2, Directive 2002/58/EC.

<sup>43</sup> See recital 3, Directive 2002/58/EC.

<sup>44</sup> See recital 6, Directive 2002/58/EC.

<sup>45</sup> CoE Recommendation No. R(90)19, on the protection of personal data used for payment and other related operations (13 September 1990).

<sup>46</sup> CoE Recommendation No. R(91)10, on the communication to third parties of personal data held by public bodies (9 September 1991).

<sup>47</sup> CoE Recommendation No. R(95)4, on the protection of personal data in the area of telecommunication services, with particular reference to telephone services (7 February 1995).

<sup>48</sup> See CoE Recommendation No. R(90)19: “Respect for privacy shall be secured during the collection, storage, use, communication and conservation of personal data linked to the provision or use of a means of payment” (Appendix, §2).

<sup>49</sup> See CoE Recommendation No. R(91)10: “The communication, in particular by electronic means, of personal data or personal data files by public bodies to third parties should be accompanied by safeguards and guarantees designed to ensure that the privacy of the data subject is not unduly prejudiced” (Appendix, §2).

<sup>50</sup> See CoE Recommendation No. R(95)4: “Telecommunication services, and in particular telephone services which are being developed, should be offered with due respect for the privacy of users, the secrecy of the correspondence and the freedom of communication” (Appendix, §2).

<sup>51</sup> See CoE Recommendation No. R(99)5 for the protection of privacy on the Internet (Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways) (23 February 1999).

legislation<sup>52</sup>. At last, it is clear that data protection is just a part of privacy protection, and that personal data are just a part of the private heritage of the individual.

Summing up, privacy has not always been considered by EU legislation as a whole. Even if general declaration of principles consider privacy as the real right to be protected, the visibility, the attitude to be regulated, the economic relevance of data protection have expanded the attention devoted to data protection, as if the protection of individual's privacy might be fully satisfied by it. After a shy entry into declarations and legislation, data protection has gradually taken up almost all the efforts of the EU in the privacy sector, leaving the most intimate sides of privacy uncovered.

International Conventions on fundamental rights, and the EU Charter itself, show that personal data and privacy do not coincide<sup>53</sup>, and that data protection does not fully meet privacy protection expectations. Still, EU Directives do not try to define privacy and to protect the other sides of privacy, being content with protecting that limited part related to data collection, processing and use. Unsatisfactory privacy protection<sup>54</sup> may derive also from unsatisfactory data protection, but the main point is that even good legislation about data would not entirely protect privacy<sup>55</sup>.

### 3. The concept of privacy: what privacy really is about

The concept of privacy is not easy to outline<sup>56</sup>, as it assumes various relationships with other individuals and general interests. Moreover, the concept of privacy is not a solely legal concept, but it has philosophical and moral<sup>57</sup> origins, dating way back in time<sup>58</sup>. Furthermore, as far

---

<sup>52</sup> See §1, CoE Recommendation No. R(99)5.

<sup>53</sup> See the Opinion of the Economic and Social Committee of 28 November 2001 on network and information security: “the main aim is to protect privacy and personal data” (§3.1.9.); priority must be given to the protection of privacy and the confidentiality of individual data” (§3.2.1.1.1.).

<sup>54</sup> See Data Protection Working Party, Working Document of 21 November 2000, on Privacy on the Internet, which stresses how the “Working party has at several occasions identified some lacunae or controversial issues in the existing legislation” (Chapter 10, §2.2).

<sup>55</sup> See the Opinion of the Economic and Social Committee of 24 January 2001, on e-commerce, which stresses that “data protection does not always work” and that infringements of privacy, for example through cookies and profiling, are commonplace (§4.9.); see also Data Protection Working Party, Working Document of 21 November 2000, on Privacy on the Internet (Chapter 2, §V).

<sup>56</sup> See L. LESSIG, *Code and other laws of cyberspace*, Basic Books, New York, NY (1999): 142.

<sup>57</sup> See F.D. SCHOEMAN, *Privacy: Philosophical Dimensions of the Literature*, in *Philosophical Dimensions of Privacy: an Anthology* (Schoeman editor), Cambridge University Press, New York, NY (1984): 1.

<sup>58</sup> See A.F. WESTIN, *Privacy and Freedom*, Atheneum, New York, NY (1967): 8.

as online privacy is concerned, unlike other legal concepts related to fundamental rights and freedoms, the concept of privacy is more sensitive to technological changes.

Despite difficulties and changes, there are some cornerstones. Privacy is about choice, the choice of how to live. Privacy is about the chance to regulate, limit, control the flow of one's own personal data and information, broadly considered, or the access to them. Privacy is about the freedom and the capacity to take personal decisions without being subject to public or private scrutiny. And privacy is, first of all, related to a psychological side, to the protection of intimacy, to the formation and expression of emotions and feelings<sup>59</sup>.

There are two directions of privacy, as there are two directions between an individual and the world: inbound and outbound. The individual should control the traffic on both of them, filtering what is going out and filtering what is coming in. Individuals should decide what part of their intimate world can be known on the outside<sup>60</sup>, and what part of the outer world can be admitted to the inside.

In these terms, privacy must be connected to other fundamental rights and freedom, and, first of all, with the most important values for the person. In the EU Charter of Nice, privacy is protected by article 7, but it is naturally connected to other principles, as functional to them: human dignity (article 1<sup>61</sup>), mental integrity (article 3, §1<sup>62</sup>), freedom of thought (article 10<sup>63</sup>), freedom of expression and information (article 11<sup>64</sup>), the right to education (article 14<sup>65</sup>) and the rights of the child (article 24<sup>66</sup>). Likewise, in the UN International Covenant, the right to privacy (article 17) precedes the right to freedom of thought<sup>67</sup> (article 18, §1), the right to hold opinions without interference (article 19, §1) and the right to freedom of expression<sup>68</sup> (article 19, §2), which includes

---

<sup>59</sup> See J.C. INNESS, *Privacy, Intimacy and Isolation*, Oxford University Press, New York, NY (1992): 6.

<sup>60</sup> See M.E. KATSH, *Law in a digital world*, Oxford University Press, New York, NY (1995): 228.

<sup>61</sup> Article 1, EU Charter of Nice: "Human dignity is inviolable. It must be respected and protected".

<sup>62</sup> Article 3, §1, EU Charter of Nice: "Everyone has the right to freedom of thought, conscience and religion".

<sup>63</sup> Article 10, §1, EU Charter of Nice: "Everyone has the right to respect for his or her physical and mental integrity".

<sup>64</sup> Article 11, §1, EU Charter of Nice: "Everyone has the right to freedom of expression", which includes the "freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers".

<sup>65</sup> Article 14, EU Charter of Nice: "Everyone has the right to education".

<sup>66</sup> Article 24, EU Charter of Nice: "Children shall have the right to such protection and care as is necessary for their well-being" (§1); "In all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration" (§2).

<sup>67</sup> See also article 9, §1, CoE Convention of Rome.

<sup>68</sup> See also article 10, §1, CoE Convention of Rome, which includes the "freedom" to hold opinions into the freedom of expression.

the “freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice”<sup>69</sup>.

Privacy has many sides, going far beyond personal data. There are “visible” sides, related to personal data and to communications: “material” objects, which need protection. There are “sensitive” sides, related to needs and expectations: elusive objects, which nevertheless need protection, even stronger. The EU legal system protects data (Directive 95/46/EC), and communications (Directive 2002/58/EC), but not always consider the other sides, whose protection can only partially derive from data and communications protection.

The “sensitive” sides have not a direct material object to refer to, and they are cross-sectoral. Protect them is harder than protect material sides, but not impossible. The starting point is to realize, to know, that even if the “sensitive” sides share a sort of spirituality, nonetheless they are relevant for the law<sup>70</sup>. They are not just philosophical concepts, but irrepressible legal parameters to deal with, providing the right contents to the right to privacy.

Not surprisingly, privacy has been constantly perceived as a compound concept.

Privacy has been considered as a sum of expectations: solitude, the sheerest form of privacy, the desire to be let alone; intimacy, an exclusive relationship between two people, separate from others; anonymity, the wish not to be under surveillance; and data protection<sup>71</sup>. Privacy has been seen as the integration of three sides: informational privacy, about personal information and their staying private; accessibility privacy, about the protection from external intrusions; expressive privacy, about the freedom to express one’s own personality, limiting social control<sup>72</sup> on lifestyle choices<sup>73</sup>. Privacy has been divided into four areas: physical privacy, with reference to the exclusive right to one’s own body and home; decisional privacy, with reference to people’s choices in order

---

<sup>69</sup> According to art.19, §3, of the UN Covenant, the right to freedom of expression, carrying with it “special duties and responsibilities”, may be subject to certain restrictions; however, these restrictions “shall only be such as are provided by the law”, and necessary either “for respect of the rights or reputation of others”, or “for the protection of national security or of public order (*ordre public*), or of public health or morals”; article 10, §3, of the Coe Convention of Rome affirms that freedom of expression may be subject “to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary”.

<sup>70</sup> See E.L. BEARDSLEY, *Privacy: Autonomy and Selective Disclosure*, in *Privacy – Nomos XIII* (Pennock & Chapman editors), Atherton Press, New York, NY (1971): 56.

<sup>71</sup> See A.F. WESTIN, *Privacy and Freedom*, Atheneum, New York, NY (1967): 7.

<sup>72</sup> See F.D. SCHOEMAN, *Privacy and Social Freedom*, Cambridge University Press, New York, NY (1992): 94.

<sup>73</sup> See J.W. DECEW, *In Pursuit of Privacy. Law, Ethics, and the Rise of Technology*, Cornell University Press, Ithaca, NY (1997): 73.

to their activities and behaviors; informational privacy, with reference to personal data; formational privacy, with reference to the protection of the inner sides of the individual<sup>74</sup>.

All these theories share three commonalities: firstly, the relevance of individual's will, who must be allowed to decide, in an informed and responsible way, what to keep to itself and what to share with others; secondly, the link with the most intimate and private sphere of the individual, protecting not only privacy but also dignity, personality and freedom; thirdly, the impossibility of reducing to unity the compound concept of privacy without missing something relevant.

All these aspects were already outlined in the first, creative, original, fundamental and oft-quoted elaboration of the concept of privacy, designed as the right to be let alone<sup>75</sup>. The right to privacy was considered, ahead of time, as an autonomous right with its relevance and dignity<sup>76</sup>. Apart from the references to practical criteria, like public interests, consent, proportionality, the most interesting part was the definition itself, more philosophical than legal. Without denying the material sides of the right to privacy, connected to property or possession, the inviolate personality was the core of the right. The protection of personality, with reference to one's own feelings more than one's reputation, was the real goal<sup>77</sup>. This "spiritual approach", wider than the legal approach<sup>78</sup>, is all but inconsistent with online privacy issues.

Cleared up that the concept of privacy does not concern only the more evident and material sides (data protection, communications confidentiality), but more impalpable aspects (intimacy, solitude, anonymity, personality) as well, it follows that the concept, both common and legal, of privacy is particularly wide-ranging and complicated. Privacy is a right of the individual, a minimum and functional guarantee for other rights, marking boundaries between citizens and Government and among citizens.

The protection of privacy, considered in its broadest significance, may have been hampered by a sort of social suspicion, as if privacy were not consistent with society and democracy. The right to be let alone is not incompatible with human sociability and curiosity<sup>79</sup>, and it is not incompatible with the very concept of society. Sociability should not refrain people from having the chance to

---

<sup>74</sup> See S. SCOGLIO, *Transforming Privacy. A Transpersonal Philosophy of Rights*, Praeger, Westport, CT (1998): 1.

<sup>75</sup> See S. WARREN, L.D. BRANDEIS, *The Right to Privacy*, 4 *Harv. L. Rev.* (1890): 193.

<sup>76</sup> See D.A. ELDER, *The Law of Privacy*, Clark Boardman, New York, NY (1991): 1.

<sup>77</sup> See S.H. HOFSTADTER, G. HOROWITZ, *The Right of Privacy*, Central Book Co., New York, NY (1964): 17.

<sup>78</sup> See R.F. HIXSON, *Privacy in a Public Society. Human Rights in Conflict*, Oxford University Press, New York, NY (1987): 29.

<sup>79</sup> See C. TAPPER, *Computer Law*, Longman, New York, NY (1983): 119.

protect their privacy, as it is a matter of balancing<sup>80</sup> competing values<sup>81</sup>, where will, consent, and proportionality<sup>82</sup> are the drawing boundaries criteria.

In these terms, privacy is neither an obstruction<sup>83</sup> nor a luxury<sup>84</sup> to democracy, as privacy is not narrow-mindedness and is not a complete isolation and refusal to society, which would be, anyway, a personal choice to be respected as well. Actually, privacy is functional to democracy<sup>85</sup>, as they share the foundation stone, consent, expressed both to Government, legitimizing their power, and to that part of private life to share with selected others and with the society as a whole<sup>86</sup>.

Privacy is a state of separation, under different degrees, from others, but it is a sought and craved state<sup>87</sup>. The misunderstandings between law and privacy come from this fine and ethereal character. While the infringements of other fundamental rights, as personal freedom, personal integrity and freedom of speech, turn often into clear facts and behaviors, the infringements of the right to privacy turn often into less perceptible, but not less serious, facts and behaviors. Online, the perceptibility of privacy infringements is even lower than offline.

This leads to the aspect of abuses. Abuses happen not only when clearly defined events cause identifiable and assessable damage, but also when mere threats to one's own privacy make someone feel uneasy. The legal concept of abuse must therefore be broadly interpreted when related to privacy, as solely so a real protection can be guaranteed. That is why privacy abuses must include even little, daily violations slowly drawing on a valuable, intimate<sup>88</sup> and vulnerable<sup>89</sup> heritage, and must not be restricted to economic losses.

E-mail interception and contents disclosure are privacy infringements, as extraction and selling of e-mail addresses are. Online well grounded worries concern tracking, profiling, spamming, personal data circulation, electronic eavesdropping, and the legal system has to provide people with

---

<sup>80</sup> See VAN DEN HAAG, E., *On Privacy*, in *Privacy – Nomos XIII* (Pennock & Chapman editors), Atherton Press, New York, NY (1971): 153.

<sup>81</sup> See J. GOLDMAN, *Privacy and Individual Empowerment in the Interactive Age*, in *Visions of Privacy: Policy Choices for the Digital Age* (Bennett & Grant editors), University of Toronto Press, Toronto, CA (1999): 101.

<sup>82</sup> See A. ETZIONI, *The Limits of Privacy*, Basic Books, New York, NY (1999): 10.

<sup>83</sup> See A.F. WESTIN, *Privacy and Freedom*, Atheneum, New York, NY (1967): 23.

<sup>84</sup> See A.F. WESTIN, *Privacy and Freedom*, New York, NY, Atheneum (1967): 52.

<sup>85</sup> See C.J. FRIEDRICH, *Secrecy versus Privacy: the Democratic Dilemma*, in *Privacy – Nomos XIII* (Pennock & Chapman editors), Atherton Press, New York, NY (1971): 105.

<sup>86</sup> See C.D. RAAB, *Privacy, Democracy, Information*, in *The Governance of Cyberspace* (Loader editor), Routledge, New York, NY, London, UK (1997): 155.

<sup>87</sup> See M.A. WEINSTEIN, *The Uses of Privacy in the Good Life*, in *Privacy – Nomos XIII* (Pennock & Chapman editors), Atherton Press, New York, NY (1971): 88.

<sup>88</sup> See R.S. GERSTEIN, *Intimacy and Privacy*, in *Philosophical Dimensions of Privacy: an Anthology* (Schoeman editor), Cambridge University Press, New York, NY (1984): 265.

<sup>89</sup> See F.D. SCHOEMAN, *Privacy and Social Freedom*, Cambridge University Press, New York, NY (1992): 19.

an adequate level of protection. Law should not regulate and stiffen all that happens online, but law cannot refrain from intervening when the rules that are followed are not consistent with community legal sensitivity.

Economic issues affect privacy as well, determining a different kind of attack, based on profit search, market development, and private initiative<sup>90</sup>. Privacy may be defined as a fundamental right, but as strange as it may seem, it is not inalienable: on different levels negotiations are conducted, exchanges are carried out. The problem is that privacy is dispossessed, and, paradoxically, the acknowledgment of the economic value of personal data has not lead to a greater citizens' awareness. When personal data became a tradable good, and when Internet favored their collection and circulation, the subjects of the data were deprived of the control on them, and they have not shared the consequent benefits. Data are financially relevant in great numbers, when they are aggregated; individual's data are important to their subject, but not financially exploitable.

The economic approach, a sort of market-driven protection of privacy, has determined a devaluation of the right to privacy from a fundamental right to a commodity<sup>91</sup>. Moreover, it is not a commodity to everyone. Furthermore, when individuals realize that they have implicitly disclaimed their rights to get nothing in exchange, and they want to take their intimacy back, the economic side turns against them. They must pay (in terms of money or time) to use technical means, they must pay to know what others know, they must pay to protect themselves from further intrusions, they must pay to make data collectors and users follow the rules. Self-help, the adoption of privacy-enhancing measures<sup>92</sup>, can be useful at times, but they are often an unjustified burden for users. Law should have intervened in order to balance it back, in order to defend the weak and the inexpert. Instead, law has kept to itself, leaving technological and economic rules to step in.

Summing up, the complex, composed, and fascinating concept of privacy, may be divided into five elements, autonomous and complementary at the same time<sup>93</sup>.

The first element is the right to be let alone, the right to decide one's own level of integration with others, the right not to be under public or private scrutiny, surveillance and control. To be let alone is the easiest and comprehensible request, but at the same time the most

---

<sup>90</sup> See A.W. BRANSCOMBE, *Who Owns Information? From Privacy to Public Access*, Basic Books, New York, NY (1994): 178.

<sup>91</sup> See S.G. DAVIES, *Re-Engineering the Right to Privacy: how Privacy Has Been Transformed from a Right to a Commodity*, in *Technology and Privacy: the New Landscape* (Agre & Rotenberg editors), The MIT Press, Cambridge, MA (1997): 143.

<sup>92</sup> See Data Protection Working Party, Working Document of 21 November 2000, on Privacy on the Internet (Chapter 9), clearly shows the broad array of this kind of measures, but at the same time shows how costly and time consuming self-help may be, especially for the non-technological savvy.

radical as well. It is the traditional side of privacy, and the basis for the other sides, but, even if it has been considered as a synthesis of them, privacy is more. While the expectation could be solitude, avoiding external contacts, the use of the Internet is not inconsistent with such an expectation, as the individual may look for it in some occasions only, or referring to some categories of people. Solitude is not something absolute, and intimacy must be always protected. The object is one's own personal sphere, which the individual should be able to define according to one's desires. When online, as when offline, the right to be let alone means the right to choose: choose the people to communicate with, choose the information to share. The protection online is not just virtual, but real and physical as well: the computer is a part of one's home and a personal means of expression.

The second element is the right to intimacy between two (or more) people, the right to communicate maintaining communications private, the right not to be tapped or snooped. It is a relational privacy, which shares with the right to be let alone the voluntary separation from others. In this case, both online and offline, two or more people, who want to save the exclusivity of their relationship, seek the separation.

The third element is the right to anonymity, the right not to leave tracks, the right not to see any matching between one's own identity and data, facts, behaviors. Online, where anonymity is often reduced into pseudonymity<sup>94</sup>, it means that browsing patterns must remain private, that there should be no profiling. Anonymity can guarantee the capacity to express one's own personality and to make choices without social constraints. Respecting the laws in force, people should be free to visit sites, to establish personal relationships, to buy goods and services, to read news and information, and to behave as they deem appropriate, without worries to be identified.

The fourth element is the right to personal data protection, the right to control them, the right to know where personal information may be. Online, personal data protection is relevant, but more for its functional role than for the object of the protection itself: without identifying personal data, other activities cannot be possible. But invasions of privacy are possible through the misuse of non-identifying data.

The fifth element is the right to the personality of one's own decisions, the right not to be influenced, the right to express oneself, the right to choose behaviors and lifestyles. Solitude and

---

<sup>93</sup> See N. LUGARESI, *Internet, privacy e pubblici poteri negli Stati Uniti*, Giuffrè, Milan, Italy (2000): 5.

<sup>94</sup> See CoE Recommendation No. R(99)5, suggesting, if permitted by law, the use of a "pseudonym so that your personal identity is known only to your ISP" (§II.4). See also Directive 1999/93/EC on electronic signatures, allowing certification service providers to indicate "in the certificate a pseudonym

anonymity may be connected, but its essence is broader, as it entails, on one hand, the right to have access to all the information needed and wanted, and, on the other hand, the right to be out of social control, the right to choose one's own path among those allowed by the legal system. The right to personality online should comprehend the right to live as a different persona.

#### 4. Offline privacy and online privacy: different problems, same rules?

If regulating privacy offline is not an easy task, regulating online privacy is even harder. Besides definition problems, common to both the offline and the online world, the regulation of privacy on the Internet adds more complex technological and jurisdictional issues. Law oscillates between the implementation of traditional concepts and rules, through the use of analogy, and the identification of a new array of concepts and rules. The result, when it comes to the protection of privacy, is that at times online privacy looks like the child of a lesser God, as if there were an Internet divide diminishing privacy value.

Moreover, the data-oriented approach is even more dangerous and unsatisfactory online than offline, as the other parts of privacy are likely to be harmed more frequently and seriously online. Nonetheless, regulations and general documents tend either to limit privacy protection on the Internet to the data part, or to mix privacy protection and data protection.

The CoE Recommendation No R(99)5, devoted to the “protection of privacy on the Internet” contains guidelines for the protection of individuals “with regard to the collection and processing of personal data on information highways”<sup>95</sup>. The extensive Working Document of the Data Protection Working Party devoted to “privacy on the Internet”, refers in its subtitle to “an integrated EU approach to online data protection”<sup>96</sup>. The Directive 2002/58/EC asserts that publicly available electronic communications services over the Internet poses new risks for users’ “personal data and privacy”<sup>97</sup>.

---

instead of the signatory's name”. See also Data Protection Working Party, Recommendation 2/2001 of 17 May 2001 (§22).

<sup>95</sup> See CoE Recommendation No. R(99)5: “respect for privacy is a fundamental right of each individual which may also be protected by data protection legislation” (Appendix, §I, Introduction).

<sup>96</sup> See Data Protection Working Party, Working Document of 21 November 2000, on Privacy on the Internet, which opening statement (Chapter 1: Introduction) explains that its object concerns the issue of “on-line data protection”.

<sup>97</sup> Recital 6, Directive 2002/58/EC.

Social, economic, and technological changes, like more precise social organization, stricter security needs, faster economic developments, more direct personal data relevance, more invasive electronic communications, entail limitations of privacy<sup>98</sup>. Still, the concept of privacy should not be different online and offline. There are different problems, threats, paths, subjects, interests, remedies, but the concept itself, under a theoretical point of view, does not change. However, dealing with online privacy issues, as spamming, tracking, profiling, cookies, allows investigating different aspects of privacy, highlighted by Internet peculiarities.

Looking for similarities between online and offline behaviors may help in the understanding of what real threats to privacy on the Internet are. The common perception might be that people are more cautious online than offline. Still, users often accept online behaviors that they would not ever accept offline, as if the loss of privacy were a natural requirement in order to browse, communicate with others, buy goods and services, acquire news and have access to information. The fact is that individual's sensitivity is mainly directed to security matters, as in credit cards online transactions, while privacy matters remain partially hidden or unresolved.

Commonly, people do not realize, or, if they do, are not shocked that their steps online are tracked and registered. But their reaction would be much different if a file were kept on the books, magazines and newspapers they read, on the movies, shows and programs they watch, on the communications they have with friends, lovers, acquaintances, on the stores they enter into and their purchases, or even just the goods they look at or the services they inquire about.

In a way, the relationship between rules and exceptions is overturned when it comes to online privacy. The protection of privacy should be the rule, and restrictions should be the exceptions. On the contrary people expect their privacy to be curbed, with unnatural resignation. The duty of the law is to tip back the scales in favor of privacy.

A technical and economic oligarchy, which regards privacy as a nuisance, has led to that. Assuming that too much privacy may make the Internet less flexible, fast, rich, alluring, and that the restrictions on privacy are just a little, irrepressible price to be charged, privacy online has been neglected. To some extent, it is true that too much privacy may change the way the Net is used, but in the sense that the privacy-oriented users often face the need to take longer paths when they are online. Maintaining that it is an unavoidable choice is misleading, as regulations and technological means can be adopted. Besides, it is not just a technical option, as a fundamental right is involved. The protection of the private area of citizens cannot be considered just an obstacle, but, on the contrary, it must constitute a main beam of the regulation building of the Internet.

---

<sup>98</sup> See V. PACKARD, *The Naked Society*, Van Rees Press, New York, NY (1964): 15.

Moreover, conceding that many more personal information circulate online, it is argued that the enormous stream of data protects privacy, such as in a big city, where the interest and curiosity of people are lower than in a small town, where less frequent social contacts do not prevent the knowledge of more private facts. Again, as a matter of fact, it may be true, but the question is not about statistics, but about individuals and about the minimum level of protection each of them should enjoy in their fundamental rights. The consequences of a free flow of personal and sensitive information can be devastating, and it would be, again, misleading into maintain that the protection of privacy lies in the increase in data circulation.

What it really matters should be individual's will, without putting down to it meanings and contents that cannot be known from the outside of individual's mind. Each individual should have the right to limit the access to their intimate sphere, castle, or ivory tower, and therefore to decide who to let enter and to what extent. Instead, consent on the Internet has become an exception, so that people, in order to leave others out from their private sphere, cannot rely on adequate access restrictions expressly stated by the law, and must actively dedicate themselves to find appropriate means, bearing the related costs. The greatest anomaly is the unjustified devaluation of people's consent, which is deemed disclaimed at the same moment they log in, as if a contract had been signed, with its inequitable clauses. The greatest mistake that can be made is to consider the loss, or the restriction, of one's own privacy as a necessary evil, as a price to pay to the Net, as an abstract entity. Nobody has signed the fine print clauses; nobody has waived an inalienable fundamental right.

## **5. The EU regulation of online privacy: improvements and inconsistencies**

The aim of EU laws is twofold: on one side, support the development of the Internet and foster the participation of citizens; on the other side, guarantee fundamental rights and freedoms online. As regards regulations, while general principles clearly state the need to a comprehensive protection of privacy on the Internet, Directives often underestimate, and sometimes neglect, relevant sides of privacy.

Directive 97/66/EC, on the protection of privacy in the telecommunications sector (now repealed by Directive 2002/58/EC), clearly showed the divide between online privacy and offline privacy, and the questionable approach often followed. The use of automated calling systems without human intervention or fax machines for the purposes of direct marketing was allowed only

in respect of subscribers giving their prior consent<sup>99</sup>. As for other means, like e-mail, the protection was lower and indirect, as Member States had to take “appropriate measures” to ensure that, free of charge, unsolicited calls were not allowed, leaving national legislation free to determine whether to apply an opt-in or an opt-out system<sup>100</sup>. The opt-in system adopted for automated telephone calling systems and facsimile machines was not imposed on bulk e-mail, under an objectionable distinction<sup>101</sup>.

In the same terms, Directive 97/7/EC, on distance contracts, requires the prior consent of the consumer with reference to automated calling system without human intervention and facsimile machine<sup>102</sup>, while, for other means of distance communication, it states that they can be used only where there is no clear objection from the consumer<sup>103</sup>, without defining what a clear objection can be.

Directive 97/66/EC and Directive 97/7/EC were enacted after directive 95/46/EC, and they had to comply with the principles of the CoE Convention of Rome. Still, they considered spamming as less intrusive than automatic calling machines, without justifying their choices, and on the contrary recognizing the consumer’s right to privacy, particularly with reference to freedom from intrusive means of communication, and conceding the need to take appropriate measures to ensure the protection of those consumers who do not wish to be contacted<sup>104</sup>. Not surprisingly, the Directive 2000/31/EC, on e-commerce, took for granted that Member States could adopt opt-out systems for unsolicited commercial communications by electronic mail<sup>105</sup>.

However, CoE Recommendation No. R(95)4, acknowledging the distress or discomfort caused by direct marketing practices, and promoting codes of conduct to limit these

---

<sup>99</sup> See article 12, §1, Directive 97/66/EC.

<sup>100</sup> See article 12, §2, Directive 97/66/EC.

<sup>101</sup> See recital 14, Directive 2000/31/EC: “the implementation and the application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communication”, with no distinction about e-mail.

<sup>102</sup> See article 10, §1, Directive 97/7/EC.

<sup>103</sup> See article 10, §2, Directive 97/7/EC.

<sup>104</sup> See recital 17, Directive 97/7/EC.

<sup>105</sup> See article 7, §2, Directive 2000/31/EC, requiring, in this case, that Member States ensure that the service providers established in their territory “consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves”.

consequences<sup>106</sup>, adopted an opt-out system for direct marketing “by telephone or by other telecommunication means”<sup>107</sup>, and an opt-in system for advertising automatic call devices<sup>108</sup>.

Only with Directive 2002/58/EC electronic mail has been equaled to automatic calling machines and facsimile machines<sup>109</sup>, requiring the prior consent and adopting therefore a common opt-in system<sup>110</sup>. Besides, in order to facilitate enforcement (at least within EU), the electronic communications Directive prohibits the use of false identities or false return addresses while sending unsolicited e-mail for direct marketing purposes<sup>111</sup>.

The different discipline for e-mail contained in Directive 97/66/EC, which lasted five years, was determined by a mix of lack of knowledge, lack of courage, and a wrong sense of resignation. The grounds, on which the opt-in system was introduced with reference to automatic calling machines and faxes, stood for e-mail as well<sup>112</sup>. Sending bulk e-mail is even easier and cheaper than using other means for the sender, and it is not true that it is less annoying for the receiver. The receiver can use self-help remedies, like filters<sup>113</sup>, when they work, or just delete junk mail without reading it, when clearly identifiable as such<sup>114</sup>. But, when users receive loads of

---

<sup>106</sup> CoE Recommendation No. R(95)4: “domestic law or codes of practice should apply to the time when calls may be made, the nature of the message and the manner in which the message is communicated” (Appendix, §7.9.).

<sup>107</sup> CoE Recommendation No. R(95)4: direct marketing “may not be directed at any subscriber who has expressed the wish not to receive any advertising material”; as for direct marketing by phone, “appropriate means should be developed for identifying those subscribers who do not wish to receive any advertising material over the telephone” (Appendix, §7.10.).

<sup>108</sup> CoE Recommendation No. R(95)4: “Automatic call devices for transmitting pre-recorded messages of an advertising nature, may only be directed at subscribers who have given their express and informed consent”; the consent may be revoked at any time.” (Appendix, §7.11.).

<sup>109</sup> See Data Protection Working Party, Opinion 7/2000 of 2 November 2000, on the proposal for the privacy and electronic communications Directive, which “welcomes and supports the proposals to address unsolicited electronic mail in the same way as automatic calling machines and facsimile machines”, as in all these situations “the subscriber has no human interface and supports parts or the whole of the costs of the communication”, and “the degree of invasion into privacy and the economic burden are comparable”.

<sup>110</sup> See article 13, §1, Directive 2002/58/EC; see also §2, which adopts a mixed opt-in and opt-out system when electronic contact details for electronic mail are obtained in the context of the sale of a product or a service: 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”.

<sup>111</sup> See article 13, §3, Directive 2002/58/EC.

<sup>112</sup> See Data Protection Working Party, Opinion 7/2000 of 2 November 2000, on the proposal for the privacy and electronic communications Directive, which states that, with reference to article 13 of the proposed Directive, “spam constitutes a specific form of privacy violation”, as the user “has no human interface, supports the cost of the communication and normally receives spam within the protected area of his private home”.

<sup>113</sup> See recital 30, Directive 2000/31/EC, promoting filtering initiatives.

<sup>114</sup> See article 6 and article 7, §1, Directive 2000/31/EC, imposing such an identification; see also the Opinion of the Commission of 17 June 2002, on the proposal for the Directive on privacy and electronic

unsolicited commercial e-mail a day, screening them out becomes a time-consuming and irritating task; besides, spamming should not result in additional costs, as connection costs, for the users<sup>115</sup>. In other words, it is not just an economic loss, but privacy, in its immaterial sense, has been invaded, often in a deceitful way.

Directive 2002/58/EC finally overcomes the doubts about the adoption of an opt-in system<sup>116</sup>. The customer's interest in being spared unsolicited commercial information is more relevant than the concern that an opt-in system could hinder the development of e-commerce, discriminating companies in the EU<sup>117</sup>. Moreover, the volume of spamming may also cause difficulties for networks and terminal equipments, which further justifies the adoption of an opt-in system<sup>118</sup>.

Certainly, EU regulations will not solve the problem, due to jurisdictional problems. But it is senseless not to regulate either because the problem would stand anyway or because it would mean that some direct marketing activities may be moved outside of European Union.

Regarding the ineluctability of spamming, law cannot surrender, as it is dealing with a fundamental right. Besides, rules enacted have not only a practical goal, but also an ethical goal, stating the relevance of privacy in all individuals' life expressions<sup>119</sup>.

As for possible economic losses, the race to the bottom applied to fundamental rights would be inexcusable, as it would miss the hierarchy of interests and priorities. Free speech, freedom of expression, freedom of information are relevant competing values. But when it comes to spamming, they cannot be appealed to, as the invasion of a sacred private sphere is not necessary to their goal. As convenient as spamming may be, advertising and direct marketing online can follow other ways.

In these terms, Directive 2002/58/EC has filled up an unjustifiable gap. With reference to different online privacy invasions, like cookies and other similar devices, the Directive on privacy

communications, recognizing that "technical modalities allowing e-mail users to view the subject line of a message before downloading it, may continue to be a useful tool" (amendment 45 – recital 44a).

<sup>115</sup> See recital 30, Directive 2000/31/EC.

<sup>116</sup> See Data Protection Working Party, Opinion 7/2000 of 2 November 2000, on the proposal for the privacy and electronic communications Directive: "opt-in is a well-balanced and efficient solution in order to remove obstacles to the provision of commercial communications whilst protecting the fundamental right of privacy of consumers".

<sup>117</sup> See the Opinion of the Economic and Social Committee of the 24 January 2001, on the proposal for the privacy and electronic communications Directive (§2.6).

<sup>118</sup> See recital 40, Directive 2002/58/EC; see also recital 30, Directive 2000/31/EC.

<sup>119</sup> See Council Decision 1999/168/EC of 25 January 1999, adopting a RTD programme on a user-friendly information society, underscoring "the needs and expectations of the typical users", and the "socioeconomic and ethical aspects" (Annex II, §a.i.).

and electronic communications has tried to intervene as well. The Directive acknowledges the right to be protected against such intrusive behaviors and links between these devices and spamming<sup>120</sup>. Directive 2002/58/EC states that terminal equipments of users, and any information stored, are part of the private sphere of the users, according to the CoE Convention on human rights. This means that the use of spyware, web bugs, hidden identifiers and other similar devices, storing hidden information or tracing the activities of the users should be allowed only for legitimate purposes and with the knowledge of the user concerned, as they may seriously intrude upon the privacy of the user<sup>121</sup>. Under sharable premises (the terminal equipment is part of one's own "castle", the cited devices are intrusive for users' privacy), the conclusion of the Directive is partially disappointing, as it requires knowledge, but not consent, relying more on self-help than on compulsory protection.

As far as cookies<sup>122</sup> are concerned, the Directive distinguishes between useful and legitimate cookies, which can analyze the effectiveness of website design and advertising, verify the identity of users engaged in online transactions, and facilitate the provisions of information society services, and other cookies. Again, the Directive requires knowledge, but not consent, and sets up an opt-out system: the users must be provided with clear and precise information, in accordance with Directive 95/46/EC, about the purposes of cookies or similar devices and about what is placed on their terminal equipment; users should have the opportunity to refuse to have a cookie stored; the system must be as user-friendly as possible<sup>123</sup>.

Does the sectoral Directive provide a satisfying discipline? It depends on what we are going to compare it with. If we compare it with the present level of enforcement, it is. If we compare it with the horizontal provisions on personal data, it is not, as the level of protection provided is lower than the one provided by the Directive 95/46/EC. In fact, Directive 95/46/EC applies to the Internet as well, and, as for electronic communications, applies to all matters not specifically covered by Directive 2002/58/EC<sup>124</sup>.

---

<sup>120</sup> See the Opinion of the Economic and Social Committee of 28 November 2001, on network and information security, recognizing consumers' right "to genuinely effective protection against improper personal profiling by spy software (spyware and web bugs), and other means", and promoting the adoption of effective measures to curb spamming, "which often also arises out of such misuse" (§3.1.9.).

<sup>121</sup> See recital 24, Directive 2002/58/EC.

<sup>122</sup> For a cookies "official" description, and the risks for privacy caused by their use, see Data Protection Working Party, Working Document of 21 November 2000, on Privacy on the Internet (Chapter 2, §4).

<sup>123</sup> See recital 25, Directive 2002/58/EC.

<sup>124</sup> See Data Protection Working Party, Working Document of 21 November 2000, on Privacy on the Internet (Chapter 3, §I).

Cookies (and other similar devices) may contain personal, and even sensitive, information, related to an identified or identifiable natural person, and as such they are subject to the horizontal Directive<sup>125</sup>, according to its article 2, §1, which defines “personal data”<sup>126</sup> and the “processing of personal data<sup>127</sup>” for the purpose of the Directive.

Directives 95/46/EC requires that personal data must be processed fairly and lawfully; collected for specified, explicit and legitimate purposes; adequate, relevant and not excessive in relation to these purposes; accurate and kept up to date; preserved in a form permitting identification of data subjects for no longer than is necessary<sup>128</sup>. Do cookies and other devices meet these requirements? Is the sectoral Directive dealing with these aspects?

Apart from some exceptions (legal obligations, vital interests, public interests clauses), the processing of personal data is allowed only if the data subject has unambiguously given his consent<sup>129</sup>. As regards sensitive data<sup>130</sup>, their processing is prohibited unless the data subject has given his explicit consent, or under other peremptory exceptions<sup>131</sup>. Is the sectoral Directive consistent with the horizontal Directive? Do clear and precise information, a user-friendly system, and the opportunity to refuse, necessarily imply an unambiguous or an explicit consent?

Besides, Directive 95/46/EC requires that the controller of data must provide the data subject with, at least, the identity of the controller, the purposes of the processing, the recipients of the data, the existence of the right to access to and the right to rectify the data<sup>132</sup>. Moreover, Directive 95/46/EC contains further provisions about data subject’s right of access<sup>133</sup> and right to

---

<sup>125</sup> See Data Protection Working Party, Working Document of 21 November 2000, on Privacy on the Internet (Chapter 3, §I).

<sup>126</sup> Article 2, §1, a), Directive 95/46/EC: “Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”. See also article 2, a), CoE Convention of Strasbourg.

<sup>127</sup> Article 2, §1, b), Directive 95/46/EC: “any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction”. See also article 2, b), CoE Convention of Strasbourg, with reference to “automatic processing”.

<sup>128</sup> Article 6, §1, Directive 95/46/EC. See also article 5, CoE Convention of Strasbourg.

<sup>129</sup> Article 7, Directive 95/46/EC.

<sup>130</sup> Article 8, §1, Directive 95/46/EC, defining as “special categories”, data “revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership”, and data “concerning health or sex life”. See also article 6, CoE Convention of Strasbourg.

<sup>131</sup> Article 8, §2, Directive 95/46/EC.

<sup>132</sup> Article 10, Directive 95/46/EC.

<sup>133</sup> Article 12, Directive 95/46/EC.

object<sup>134</sup>, security of processing<sup>135</sup>, notification to the supervisory authority<sup>136</sup>. Are all these provisions respected?

I do not think the replies to all the above questions are positive. It is true that the horizontal Directive applies when the sectoral Directive does not provide with specific provisions. But what would be the interpretation in this case? It may be maintained that, as Directive 2002/58/EC takes into account cookies and other devices, there is no room for Directive 95/46/EC, which applies only when there is a lack of provisions, and not a different discipline, in the sectoral Directive. Personal and sensitive data hold, processed, or transmitted by cookies and other similar devices would then have a lower protection than other personal data, and the enactment of the sectoral Directive would paradoxically weaken the protection provided by the EU legal system.

Three aspects need to be pointed out.

The first aspect is about unambiguous consent (or explicit consent, with reference to sensitive data). The features of browsers, which allow closing down cookies, do not meet the requirements of Directive 95/46/EC. Unless the user permanently closes down cookies (with other navigation problems), the pop up window, not always written in the user's language, does not provide all the information needed. Providing all the information requested by the Directive may be burdensome, but this is not a legitimate exemption. The approach of cookies and other similar devices is more an opt-out approach than an opt-in approach, provided that there is an option.

The second aspect is about jurisdiction. If the server is outside European Union, it may be maintained that jurisdiction is lacking. On the other side, cookies are stored on the terminal equipment of the user. Apart from being part of the private sphere of the user, as Directive 2002/58/EC has clarified, the hard disk of a computer is part of the territory of the Member States, which means that part of the processing (any operation performed upon personal data, including collection, according to article 2, Directive 95/46/EC) of data takes place in the European Union, and it is therefore subject to its law. It may be argued that a data controller, using cookies, cannot know all the world's regulations about cookies. The situation is quite different from contents put on websites, to which users, even minors, can connect and read objectionable consent (not considering here censorship issues). As far as cookies are concerned, there is an active, intrusive behavior, not protected by free speech and freedom of expression principles.

---

<sup>134</sup> Article 14, Directive 95/46/EC.

<sup>135</sup> Article 17, Directive 95/46/EC.

<sup>136</sup> Article 18, Directive 95/46/EC.

The third aspect is about regulation. Even if a more Internet-oriented regulation may be desirable, depending on points of view, the general framework can be often sufficient to protect online privacy<sup>137</sup>. It is a matter of implementation and enforcement of a legislation that is less technologically savvy, but it is more focused on principles, which, sometimes, helps.

So, on one side the regulatory approach of the EC should lead to proper and specific pieces of legislation about privacy on the Internet, and not rely on general disciplines about personal data or electronic communications (that is, parts of privacy). On the other side, sectoral legislation, concerned with technological issues, must not leave behind any sides of fundamental rights, and consequently provide a lower protection for them online than offline.

---

<sup>137</sup> See the Opinion of the Economic and Social Committee of 24 January 2001, on the proposal for the privacy and electronic communications Directive: “the same privacy issues should be regulated in the same way, regardless of whether electronic communications or “traditional” handling are involved” (§2.1).

## DOCUMENTATION

### United Nations

*The United Nations International Covenant on Civil and Political Rights* (adopted 12 December 1966; entered into force 23 March 1976)  
[www.unhchr.ch/html/menu3/b/a\\_ccpr.htm](http://www.unhchr.ch/html/menu3/b/a_ccpr.htm)

### Organisation for Economic Co-operation and Development

*Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (23 September 1980)  
[www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-document-43-1-no-no-10255-0,00.html](http://www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-document-43-1-no-no-10255-0,00.html)

### Council of Europe

#### **Conventions**

*Convention for the Protection of Human Rights and Fundamental Freedoms* (Rome, 4 November 1950; entry into force 3 September 1953; as amended by Protocol No.11)  
<http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm>

*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Strasbourg, 28 January 1981)  
<http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm>

#### **Recommendations**

*Recommendation No. R(90)19 of the Committee of Ministers to Member States on the Protection of Personal Data used for Payment and Other Related Operations* (13 September 1990)  
<http://cm.coe.int/ta/rec/1990/90r19.htm>

*Recommendation No. R(91)10 of the Committee of Ministers to Member States on the Communication to Third Parties of Personal Data Held by Public Bodies* (9 September 1991)  
<http://cm.coe.int/ta/rec/1991/91r10.htm>

*Recommendation No. R(95)4 of the Committee of Ministers to Member States on the Protection of Personal Data in the Area of Telecommunication Services, with Particular Reference to Telephone Services* (7 February 1995)  
<http://cm.coe.int/ta/rec/1995/95r4.htm>

*Recommendation No. R(99)5 of the Committee of Ministers to Member States for the Protection of Privacy on the Internet (Guidelines for the Protection of Individuals with Regard to the Collection and Processing of Personal Data on Information Highways)* (23 February 1999)  
<http://cm.coe.int/ta/rec/1999/99r5.htm>

### European Union / European Community

#### **Charter**

*Charter of Fundamental Rights of the European Union* (7 December 2001)

<http://ue.eu.int/df/docs/en/CharteEN.pdf>

#### **Directives**

*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](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](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/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31997L0066&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31997L0066&model=guichett)

*Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity*

[http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31999L0005&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31999L0005&model=guichett)

*Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*

[http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31999L0093&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31999L0093&model=guichett)

*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/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32000L0031&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32000L0031&model=guichett)

*Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society*

[http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32001L0029&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32001L0029&model=guichett)

*Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities ("Access Directive")*

[http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0019&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0019&model=guichett)

*Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services ("Authorisation Directive")*

[http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0020&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0020&model=guichett)

*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/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0021&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0021&model=guichett)

*Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services ("Universal Service Directive")*

[http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0022&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0022&model=guichett)

*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/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0058&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0058&model=guichett)

#### **Other documents**

*Council Recommendation 98/560/EC of 24 September 1998 on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity*

[http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31998H0560&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31998H0560&model=guichett)

*Council Decision 1999/168/EC 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/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31999D0168&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31999D0168&model=guichett)

*Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce*

[http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32000D0520&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32000D0520&model=guichett)

*Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security*

[http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002G0216\(02\)&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002G0216(02)&model=guichett)

*Opinion of the Commission of 17 June 2002 pursuant to Article 251 (2), point (c) of the EC Treaty, on the European Parliament's amendments to the Council's common position regarding the proposal for a Directive of the European Parliament and of the Council on the processing of personal data and the protection of privacy in the electronic communications sector, amending the proposal of the Commission pursuant to Article 250 (2) of the EC Treaty (COM 2002 338 final)*

[http://europa.eu.int/information\\_society/topics/telecoms/regulatory/new\\_rf/documents/com\\_2002\\_338\\_en.pdf](http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/documents/com_2002_338_en.pdf)

#### **Data Protection Working Party documents**

[http://europa.eu.int/comm/internal\\_market/en/dataprot/wpdocs/index.htm](http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm)

*Recommendation 1/2000, on the Implementation of Directive 95/46/EC* (3 February 2000)

[http://europa.eu.int/comm/internal\\_market/en/dataprot/wpdocs/wp30en.pdf](http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp30en.pdf)

*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 COM (2000) 385* (2 November 2000)

[http://europa.eu.int/comm/internal\\_market/en/dataprot/wpdocs/wp36en.pdf](http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp36en.pdf)

*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/en/dataprot/wpdocs/wp37en.pdf](http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp37en.pdf)

*Recommendation 2/2001, on Certain Minimum Requirements for Collecting Personal Data Online in the European Union* (17 May 2001)

[http://europa.eu.int/comm/internal\\_market/en/dataprot/wpdocs/wp43en.pdf](http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp43en.pdf)