International Journal of Communications Law & Policy

Special Issue Global Flow of Information, Autumn 2005

EUROPEAN UNION LEGISLATION & FREE CONTRACTS FOR INTERNET ACCESS IN THE UNITED STATES AND ITALY: TOWARDS A CONSUMER RIGHTS FRAMEWORK

Simone Francesco Bonetti[†]

ABSTRACT

This paper seeks to add to the debate regarding the high level of privacy and consumer protection provided by European Union legislation, as compared to the United States. The first part of the paper provides an overview of the highly complex system of consumer protections by linking several regulatory initiatives in the wake of the European Parliament and Council Directive 00/31/EC. The result is a new legal framework for e-consumer protection that includes privacy protection.

In the second part of the paper, the different free Internet access contract models in the U.S. and Italy are examined in order to test the implementation of the above-mentioned legislation from a European Community point of view. The analysis highlights the importance of a legal framework that seems capable of establishing the correct balance between the rights and duties of the e-consumer. At present, however, such a balance is not achieved by common U.S. and Italian free Internet access contracts.

[†] The present work is based on my previous paper: Simone Francesco Bonetti, La Tutela dei Consumatori nei Contratti Gratuiti di Accesso ad Internet: i Contratti dei Consumatori e la Privacy tra Fattispecie Giuridiche e Modelli Contrattuali Italiani e Statunitensi, 6, DIRITTO DELL'INFORMAZIONE E DELL'INFORMATICA, 1087, 1088-1140 (2002). I thank Professor Anita Allen, Professor Beth Simone Noveck, the editors and the copy editors of the International Journal of Communication Law and Policy, for their helpful comments on a prior draft of this paper. Thank you, too, to Professor Jack Balkin and Professor Guido Calabresi for their valuable support at Yale. This (conference) paper was presented during the special panel "*Comparative Perspectives on Communication and Internet Regulation*" held in the CyberCrime and Digital Law Enforcement Conference, March 26-28, 2004, Yale Law School.

1. TWO PRISMS: CONSUMER PROTECTION & ANALYSIS OF CONTRACT MODELS

From a comparative point of view, one of the most important examples of an insufficiently regulated area is the free Internet access contract. The European Union has drafted legislation that would cover these free access arrangements, and this may be considered as the best attempt to regulate the network environment and address national legislation.

It has become common for companies in the United States and Europe to offer free Internet access in exchange for subscribers' personal data.[1] Under such arrangements, the Internet service provider (henceforth "the Provider" or "ISP") provides an Internet connection, and perhaps other related services, in exchange for the right to process and communicate a subscriber's personal data. The data thus imparted to third parties generally includes information relating to the subscriber's on-line activities. The Provider also retains the right to terminate the contract for lack of use.[2] Data indicate that ISPs are springing up that offer not only basic Internet connectivity but additional value-added services, such as electronic mail, free website hosting, newsgroups, chatrooms (simultaneous communication between several persons), SMS messaging, the sending or receiving of fax messages using an assigned telephone number, the sending and receiving of electronic mail using a mobile telephone, and the use of the Internet connection for normal telephone communications (Voice Over Internet Protocol, or VoIP).[3]

Typically, in order to enter such an arrangement, would-be subscribers access a Provider's website, where they are guided through the completion of a series of forms. These forms require the subscribers to: (1) read about and consent to the collection and processing of personal data; (2) enter personal information; (3) read and accept the offer; (4) choose a user name and password. Once this process is complete, the Provider confirms activation of the requested service. The typical agreement covers three important elements: the fact that the contract is free of charge; some form of consumer protection; and a privacy policy.

---

[1] The various Italian contracts considered, from the many examples available, are: Kataweb, at http://login.kataweb.it/registrazione/kwfreeint/utenteregistrato.jsp?origin=kataweb; Ciaoweb, at http://registrazione. ciaoweb.http://www.infinito.it/web/1,2647,RegCompNew,00.html; Libero, at http://registrazione.libero.it/; Tiscali, at http://selfcare.tiscali.it/servlet/SelfProvisioningServlet; Jumpy, at http://servizi.mediaset.it/Servizi/registration Check. jsp?portal=jumpy; Tin.it, at http://registraclubnet.virgilio.it/folfree/entrataflusso.do. United States examples are: Address.com (not yet available), at http://www.address.com; Winfire.com (not yet available), at http://www.winfire.com; Netzero.com, at http://account.netzero.net/s/landing?action=viewProduct&productId=free& group=free; Juno.com, at http://account.juno.com/s/landing?action=viewProduct&productId=free&group=free2Plat. From the date of publication of my research on this subject in 2002 some of the American contracts have been changed, now they concedes a limited time of free connections.

[2] Only in some contracts is the Provider given the possibility of terminating the contract at any time at its indisputable discretion, with a brief period of notice or without a period of notice, such as in Infinito, supra note 1; Tin.it, supra note 1; and address.com ,supra note 1.

This paper considers the legal aspects surrounding such contractual agreements. First, as a preliminary matter and from a civil law perspective, it is questionable whether these contracts are truly "free" of charge. The other two elements, consumer protection and privacy protection, shall be examined through two prisms: the applicable E.U. legislation, and the analysis of the terms of the contract models.

The European Parliament is attempting to develop a wider-ranging structure of consumer rights, with the intention of offering a higher level of protection and consisting of different community rules.[4] With respect to free-access contracts, these rules may be divided into two groups of applicable legislation. The first refers to consumer protection: Council Directive 93/13/EEC of 5 April 1993 on "unfair terms in consumer contracts and European Parliament" and Council Directive 97/7/EC of 20 May 1997, on "the protection of the consumers in respect of distance contracts". The second body of laws deals with privacy protection: European Parliament and Council 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" and European Parliament and Council Directive 02/58/EC of 12 June 2002 on "privacy and electronic communications, concerning the processing of personal data and the protection of privacy in the electronic communications sector".

An analysis of this legislation reveals a clear correspondence between the various directives, as expressed in the European Parliament and Council Directive 00/31/EC on electronic commerce. In fact, it is possible to highlight the correspondence, in accordance with the provisions of the Directive on electronic commerce, between the various rules concerning e-consumer protection. The new figure of the e-consumer thus becomes the object of a complex system of protection in which the regulations concerning consumer contracts and privacy should be considered together.

The e-consumer rights, however, have not been assimilated by the access contracts that have been examined. The existing contracts show that, once again, the ISPs prevail over their subscribers, and do not recognize the e-consumer's rights. In the coming years, these rights will have to be protected widely and uniformly both at a European Community level and in the U.S. in order to ensure the continued development of e-commerce, and confirm the international vocation of the Web, in accordance with consumers' trust or, put another way, the e-consumers' trust.

Finally, it is useful to summarize some of the questions that will be examined in this research, and the various terms that are still subject to fierce debate: the electronic mail service, the real implementation of Directive 02/58/EC (Directive on privacy and electronic communications),

[3] Many of these services are accessible to subjects differing from the subscribers, namely so-called "users", who are "all the natural persons using one or more publicly available telecommunications services, for private or business purposes, without necessarily having subscribed to such services" (Article 2, letter a, Directive 02/58/EC).

[4] See European Parliament and Council Directive 00/31/EC of 8 June 2000, **"**Directive on electronic commerce".

and finally, the Provider's liability. The latter is significant in the context of free-access contracts, with an articulate system of terms that attribute all "risk" connected to the use of the Internet to the subscriber. The terms referring to the subscriber's illegal use of the service were found to be "not unfair". Otherwise, the terms exempting the Provider from all liability with regard to the subscriber's risks linked to Web access is in contrast with the provisions of Article 4 of Directive 02/58/EC.

2. A PRELIMINARY NOTE: ON THE CHARGE-FREE NATURE OF FREE ACCESS CONTRACTS

Under the free-access contract, as defined in the introduction, ISPs may often provide services beyond mere Internet connectivity. This heterogeneity and the wide range of services offered to the subscriber do not seem to affect the unitary nature of the contract, which is a series of transactions composed of various performances. From a civil law perspective, distinguishing between charge-free services and paid services is not always a simple operation when interpreting legislation. In particular, equating the concepts of onerousness and amount due (as consideration) does not seem wholly correct.

The amount due and onerousness cannot be considered equivalent concepts because onerousness exists even in the absence of reciprocal and legally binding commitments if the party undergoing an economic disadvantage achieves an advantage over the party to whom he has transferred an asset. In this way, the notion of onerousness, not limited to the existence of fair and valuable consideration, acquires a wider range of meaning. This wider range is suggested, for instance, in the Italian legal literature.[5] In this view there exist legal transactions in which, eventually, it is not just the contract itself but the economic operation that acquires relevance.[6]

On the other hand, the lack of fair and valuable consideration (leaving aside onerousness) would seem to exclude the possibility of bilateral free-access contracts if the meaning attributed to bilaterality is equivalent to synallagmaticity[7] according to the predominant interpretation as

[5] PAOLO MOROZZO DELLA ROCCA, GRATUITÀ, LIBERALITÀ E SOLIDARIETÀ, 13-20 (Giuffrè 1998) and Oberdan Tommaso Scozzafava, "La Qualificazione di Onerosità o Gratuità del Titolo", II, RIVISTA DI DIRITTO CIVILE, 68, 75 (1980).

[6] MOROZZO DELLA ROCCA, supra note 5, 6; See also Enrico Gabrielli, "Il Contratto e le Sue Classificazioni", I, RIVISTA DI DIRITTO CIVILE, 705, 722, (1997).

[7] According to this predominant interpretation bilateral contract is essentially the equivalent of the synallagmatic contract in which "the parties obligate themselves reciprocally, so that the obligation of each party is correlative to the obligation of the other", see BLACK'S LAW DICTIONARY 325 (7th ed. 1999).

established, for instance, by the Italian Civil Code of 1865.[8] The Civil Code in force today, as opposed to the Code of 1865, uses the expression contracts with fair and valuable consideration to signify synallagmatic contracts. Thus, the term "bilateral", no longer bound by the limit of the adequate consideration, could be thought to refer more generally to contracts "which act as sources of duties binding both the contractual parties",[9] as in the case of the free-access contract, in which even the beneficiary can be seen to have certain duties.[10] According to today's Civil Code, the free-access contract can be characterized as bilateral, considering the existence of obligations both on the part of the ISP and on that of the subscriber. With respect to the ISP's obligations, Directive 95/46/EC prescribes the fair processing of personal data to be performed within the limits detailed in the contract. This includes listing the purposes for which the data are being processed, and the communication of personal data only to subjects specified in the provision, and with the consent of the person whose data are processed.[11]

The contracts examined specify that the data acquired will be used for commercial purposes and organized using profiling systems that collect and evaluate the data in a non-homogeneous way through the use of automated procedures. This is done in such a way so as to deduce the attitudes, behaviours, interests and personal and commercial characteristics of the customer. With regard to the communication of data, in nearly all the contracts examined, the entities to whom this information may be transferred include subsidiary corporations as well as third parties who have made agreements with the Provider. In fact, in most Italian contracts, it is compulsory for the consumer to give consent to the use of his or her commercial profile for the marketing or promotional objectives of the Provider or of other subsidiary corporations. On the other hand, the consumer has the option of giving or not giving consent for processing and communication of data to third parties who will use it for marketing or commercial objectives, or in order to verify the level of client satisfaction with such products or services. In this sense, the subscriber may choose to give or to withhold consent because the processing is not purely linked to the provision or improvement of the service, but rather is also processed in order to be communicated to subjects other than the Provider or its subsidiary corporations. If the subscriber consents to having his data transferred to third parties, there would seem to be an onerous characteristic in the contract because the benefit obtained by the Provider following the conclusion of the contract does not seem possible, unlike in the charge-free contract, if one considers the existence of agreements with third parties.

[8] Regarding the distinction between bilateral and unilateral contract see Tommaso Messineo, Contratto (dir. Priv.), in ENCICLOPEDIA DEL DIRITTO, X, 784, 910-913 (1961)
[9] Scozzafava, Il Comodato, TRATTATO DI DIRITTO PRIVATO, OBBLIGAZIONI E CONTRATTI, 620
[10] These duties obviously cannot exceed the value attributed to the service, because, otherwise, the contract would no longer be considered charge-free. Cf. MASSIMO BIANCA, IL CONTRATTO, 467 (Giuffrè, 1987).
[11] See art. 10 and 11, Directive 95/46/EC

In contrast, most of the U.S. contracts examined are not onerous in the same way. This is because data processing and communication are performed either with the objective of personalizing the access service and increasing the efficiency and the speed of Internet access for the subscriber[12] or, in the case of Providers' web portals, for offering other commercial opportunities. Some of these opportunities may be managed by other companies, but they are in any case offered to subscribers who can freely decide whether or not to accept.[13] However, in some forms of contract, one sees obligations for the subscriber regarding software that uploads the results of computation to the Provider's computer.[14] The costs of the uploading process are borne exclusively by the subscriber, as shown by the provision in which it may be necessary, in order to complete data transmission, to prolong the connection time or, in the case that the computer remains inactive for a long period of time, to initiate an automatic connection by means of the software supplied.[15] In this case, one could say that the subscriber performs a true "return service", and this, if the interpretation is accepted, would seem to suggest a synallagmatic relationship, and therefore its onerous characteristics.

In the case of free-access contracts, it seems possible to exclude the "liberality" of the service, considering that the Provider, by concluding the contract, aims at promoting its own economic interests, though this may be independent of whether this result is attained or not. "Liberality", according to Italian Courts, for instance, refers to a spontaneous action "*nullo iure cogente*"[16] in which there are no particular objectives in the conclusion of the transaction except that of conferring the donee[17] a benefit in terms of assets. As "liberality" is not an objective factor, but relates to the agent who makes the transfer free of charge, it should be inferred from the concrete situation in which the donor performed the action. On the contrary, "it remains purely a free (not a liberal) transaction in those cases in which the party was induced to perform the action,

[12] According to Giovanna Maccaboni, La Profilazione dell'Utente Telematico fra Tecniche Pubblicitarie Online e Tutela della Privacy, 3, DIRITTO DELL'INFORMAZIONE E DELL'INFORMATICA, 425, 435 (2001), this system of personalising the access seems to represent a clear example of an "auto profiling system" implemented by the same "users" who give their personal data. Through this system the Provider can improve the efficiency and speed of the connection to the web and offer "personalized browsing" to the subscribers and the author is worried about this "system" of personalizing the access through the personal data profiling. In fact it contradicts the concept of the "man is the measure of all things", in favor of "the market is the measure of all things".

[13] See, by way of example, the paragraph entitled "your member profile helps us personalize your Internet experience", under the section "Privacy Statement", Juno contract, supra note 1, which states that: "we use the information our subscribers provide to personalize their Internet experience and to meet the needs of our advertisers".

[14] See "Terms of Service", Address.com, supra note 1, "Address.com's free internet service is browser-based, meaning we make certain modifications to your web browser that allow us to serve advertising, control your web surfing, and restrict your ability to perform some functions".

[15] In section 2.3, Juno contract, supra note 1, Juno clearly states that the subscribers are responsible for obtaining and maintaining the equipment and telephone services necessary to access and use the Service and for any telephone charges associated with connecting to and using the Service such as the advertising information ad solicitation provided by Juno or by (or on behalf of) other entities as per article 2.4.

[16] i.e. done or performed without obligation to do so.

not spontaneously… but for a certain reason which can be objectively ascertained and which is not irrelevant in terms of law."[18] Thus the "economic reason for the gift"[19] should be evaluated according to an analysis of the case referring to the economic function specifically linked to each individual transaction, and not to a typical abstract model.

3. THE E.U. CONSUMER RIGHTS FRAMEWORK & THE ELECTRONIC COMMERCE DIRECTIVE

E-commerce in recent years has seen a notable growth in terms of both of sellers and consumers. This has created the "utopia" of a global market in which the free exchange of goods and services is possible within an extensive cybernetic space. This space is characterized by the fact that it is "virtual in appearance" and requires "no physical movement of vehicles or objects, but just that of electronic impulses".[20] These impulses are created by a number of computers that translate the instructions imparted by operators according to a digital system that enables representation, data processing (information technology) and, finally, data transmission or reception by means of the Internet. The system enables a rapid, efficient circulation of information, which is "passed back and forth", in the form of "electronic impulses", among computers connected to Internet by means of the Access Provider,[21] providing Internet access either in return for payment or free of charge.[22] In fact the latter solution is that adopted by most consumers, which means "any natural person who is acting for the purposes which are outside his trade, business or profession".[23]

The Directive on Electronic Commerce regards the range of Information Society Services, defined as "any service normally provided for remuneration, at a distance, by electronic means and

---

[17] The term "Donee" means "one to whom the gift is made", see BLACK'S LAW DICTIONARY 504 (7th ed. 1999).

[18] Vincenzo Mariconda (case note Cass., sez. I, 20 novembre 1992, n.12041), Trasferimenti atipici e nullità per mancanza di causa, II, CORRIERE GIURIDICO, 174, 178-179 (1997). See also Francesco Gazzoni (case note Cass. 9 ottobre 1991, n.10612) Babbo Natale e l'obbligo di dare, I, GIUSTIZIA CIVILE, 2896, 2896-2898 (1991).

[19] See also Francesco Caringella, Alla ricerca della causa nei contratti gratuiti atipici (case note Cass., sez. I, 20 Novembre 1992, n. 12401) I, FORO ITALIANO, 1506, 1507-1522 (1993) ; Alberto Gianola, Verso il riconoscimento della promessa atipica, informale, gratuita, ma interessata (case note Cassazione 14 November 1994, n. 9562), I GIURISPRUDENZA ITALIANA, 1921, 1921-1922 (1995);Gianluca Sicchiero, Osservazioni sul contratto gratuito atipico (case note Trib. Roma 11 Gennaio 1995) I, 2, GIURISPRUDENZA ITALIANA, 945, 946-950 (1995).

[20] Guido Alpa , preface to EMILIO TOSI ET AL. , I PROBLEMI GIURIDICI DI INTERNET XIII (Emilio Tosi ed., Giuffrè 1999).

[21] Providers can be subdivided into Network Service Providers (N.S.P.), which run large national and international telecommunications networks; Internet Access Providers (A.S.P), which, obtain Internet access from the former and provide connections for final users, both to private citizens and companies, to the Point Of Presence (POP), connected permanently to the web; Internet Service Providers (I.S.P.), which provide, in addition to the connection, further services, such as: E-mails or web hosting; Internet Content Providers (I.C.P.) provide information to the users or to the public on the web.

[22] In nearly all cases, the gratuitous nature of the service refers purely to access to the Internet, and does not regard the cost of the telephone connection to the Provider.

[23] See Article 2, second paragraph, letter (b), Directive 93/13/EEC.

at the individual request of a recipient of services".[24] Information Society Services span a wide range of economic activities that take place online, including the sale of goods and the transmission of information via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service.[25] In addition, Information Society Services are not solely restricted to services giving rise to online contracting, but they also extend to services that are not remunerated by those who receive them in so far as these services represent an economic activity. Good examples include the offering of online information or commercial communications, and the provision of tools allowing for search, access and retrieval of data. The free-access contract therefore seems to be covered by the Electronic Commerce Directive.

3.1 PART ONE: CONSUMER PROTECTION LEGISLATION

The availability of charge-free contracts has been one of the catalysing factors in the rapid spread of the Internet, though the effect is less marked today. It caused a rapid increase in the number of "non-professional" individuals on the Web, or consumers,[26] who had already become a subject of particular interest for European legislators. In recent years, the various E.U. Directives have generated a body of law, namely "consumers' rights": a true branch of the legal system implemented by the Member States "in which general statute intersects with special law".[27] The Directives concern the protection of consumers in the various phases into which relationships with suppliers can be subdivided: information and advertising, financing, making of contract, the possible existence of damages following the acquisition of products and services. The following Directives may be applied to the free contract for Internet access.

The Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts deals with the set of general provisions concerning contracts between supplier and consumer, the

[24] Article 2, letter a, Directive 00/31/EC, repeats the definition of information society services as defined within Article 1, second paragraph, Directive 98/34/EC, of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standard and regulations, as amended by Directive 98/48/EC, of the European Parliament and of the Council of 20 July 1998. The following terms contained in the definition of information society have been explained by the same Article: at "a distance": "means that the service is provided without the parities being simultaneously present"; by "electronic means": "signifies that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means"; at "the individual request of a recipient of services": "means that the service is provided through the transmission of data on individual request".

[25] See point 18 of the preamble, Directive 00/31/EC.

[26] Article 2, second paragraph, letters (a) and (b), Directive 93/13/EEC, defines the consumer as: "any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business, or profession", and the "Seller or Supplier" (hereinafter referred to as "the Supplier") as : "any natural or legal person who, in contracts covered by this Directive, is acting for purposes relating to his trade, business, or profession whether publicly owned or privately owned ".

[27] GUIDO ALPA, IL DRITTO DEI CONSUMATORI, 13 (Giuffrè 1999).

subject matter of which is the conveyance of goods or the performance of services. In particular, legislation refers to all those "unfair terms" that, not singularly negotiated and notwithstanding good faith, adversely affect the consumer by causing a significant imbalance as regards the rights and obligations ensuing from the contract.[28] The contract term shall always be regarded as not individually negotiated where it has been drafted in advance and the consumer has therefore not been able to influence the substance of the term, particularly in the context of a pre-formulated standard contract.[29] In the Annex an indicative and non-exhaustive list of the terms that may be regarded as unfair has been provided. According to Article 6, first paragraph, unfair terms should be considered not binding on the consumer and "the contract shall continue to bind the parties upon those terms if it is capable of continuing in existence without the unfair terms".

The E.U. Directive on the protection of the consumers in respect of distance contracts, which covers the contracts concluded by means of distance communication,[30] applies to the free contract for Internet access. According to this Directive, the supplier (ISP) uses exclusively "one or more means of distance communication up to and including the moment at which the contract is concluded" for all contracts "concluded between a supplier and a consumer and regarding goods or services".[31]

Consumer protection now represents an important element within the institutional Treaty on the European Union (TEU). Thus Article 3, letter t, TEU, specifies, among the objectives of the Union, "a contribution to the strengthening of consumer protection". Article 153 TEU states that "in order to promote the interests of consumers and to ensure a high level of consumer protection, the Community shall contribute to protecting the health, safety and economic interests of consumers, as well as to promoting their right to information, education and to organise themselves in order to safeguard their interests", and the Community shall contribute through: "(a) measures adopted pursuant to Article 95 in the context of the completion of the internal market; (b) measures which support, supplement and monitor the policy pursued by member states". The latter actions should not prevent "any Member State from maintaining or introducing more stringent protective measures" compatible with the Treaty and notified to the Commission (Article 153, fifth paragraph). Finally, in Article 95 TEU, third paragraph, a high degree of consumer protection is specified, even in the Commission's Directive proposals. The above-mentioned provisions seem therefore to affect on one hand the Directives themselves, as in the case of Directive 93/13/EEC at Article 8, in which it is stated that Member States are permitted to adopt stricter norms to guarantee

[28] See Article 3, Directive 93/13/EEC.
[29] See Art.3, second paragraph, Directive 93/13/EEC.
[30] European Parliament and Council Directive 97/7/EC, of 20 May 1997.
[31] See Article 2, point 1, Directive 97/7/EC.

a more adequate level of consumer protection, and on the other hand the necessary attainment of harmonisation between different community Directives which should ensure an increase in consumer protection.

The principle of consumer "protection" has once again been confirmed at community level in the Directive 00/31/EC on Electronic Commerce. This Directive "complements Community law applicable to Information Society Services without prejudice to the level of protection for, in particular, public health and consumer interests, as established by Community acts and national legislation implementing them".[32] The community acts[33] and the Directive on Electronic Commerce should offer "a high level of protection of objectives of public interest and in particular the protection of minors and of human dignity, the protection of consumers and public health".[34] The Directive also makes the following provision for consumer protection: first, Member States may adopt appropriate measures limiting the freedom to provide Information Society Service from another Member State in the cases in which this is necessary in order to guarantee protection of consumers, including investors, to avoid serious and grave risk of damage to their interests.[35] Second, the implementation of regulations listing the information that needs to be supplied prior to the order being placed by the recipient of the service,[36] the minimum information on service

[32] See Article 1, third paragraph, Directive 00/31/EC.

[33] Point 11 of the preamble makes reference above all to the following Directives: Council Directive 93/13/EEC of 5 April 1993, concerning unfair terms in consumer contracts and Directive 97/7/EC of the European Parliament and of the Council, of 20 May 1997, regarding the protection of the consumer in respect of distance contracts. Both "form a vital element for protecting consumers in contractual matters; those Directives also apply in their entirety to information society services". In addition, it also refers to all those Directives included in the Community acquis: "Council Directive 84/450/EEC of 10 September 1984, concerning misleading and comparative advertising; Council Directive 87/102/EEC of 22 December 1986 for the approximation of the laws, regulations and administrative provisions of the Member States regarding consumer credit; Council Directive 93/22/EEC of 10 May 1993 on investment services in the securities field; Council Directive 90/314/EEC of 13 June 1990 on package travel, package holidays and package tours; Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998, on consumer protection regarding the indication of prices of products offered to consumer; Council Directive 92/59/EEC of 29 June 1992 on general product safety; Directive 94/47/EC of the European Parliament and of the Council of 26 October 1994 on the protection of the purchaser in respect of certain aspects on contracts relating to the purchase of the right to use immovable properties on a timeshare basis; Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 on injunctions for the protection of consumers' interests; Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States regarding liability for defective products; Directive 99/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees; the future Directive of the European Parliament and of the Council concerning the distance marketing of consumer financial services, and Council Directive 92/28/EEC of 31 March 1992, on advertising of medicinal products. The Directive also states the continuing application of Directive 98/43/EC of the European Parliament and of the Council of 6 July 1998, on the approximation of the laws, regulations and administrative provisions of the Member States as regards advertising and sponsorship of tobacco products, adopted within the framework of the internal market, and of the Directives regarding the protection of public health". Finally, it states that "this Directive, 00/31/EC, complements information requirements established by the abovementioned Directives and in particular Directive 97/7/EC".

[34] See point 10 of the preamble, Directive 00/31/EC.

[35] See Article 3, fourth paragraph, letter a, point i), Directive 00/31/EC.

[36] See Article 10, Directive 00/31/EC, which states, in addition, that the service provider has to provide at least the following information, clearly, comprehensibly and unambiguously, prior to the order being placed by the recipient of the service: the different technical steps to follow to conclude the contract; whether or not the concluded contract will

suppliers and on commercial communications,[37] and finally the unsolicited commercial communication,[38] with precise reference to the Directive 97/7/EC and Directive 97/66/EC (which has been repealed by Directive 02/58/EC). Finally, the E.U. adopted rules providing that the placing of the order cannot be modified except when otherwise agreed by parties who are not consumers.[39]

However, there is still uncertainty as to whether the Electronic Commerce Directive is of a general or specific nature in its relation with the above-mentioned laws. This is important, for instance, when it comes to ascertaining the degree of relevance of the various additions, while the new figure of the e-consumer seems to have acquired formal definition in the already complex, articulate framework of consumer protection laws.

---

be filed by the service provider and whether it will be accessible; the technical means for identifying and correcting input errors prior to the placing of the order; the languages offered for the conclusion of the contract; an indication of any relevant codes of conduct to which the service provider subscribes, and information on how those codes can be consulted electronically. This does not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communication. Finally, the contract terms and general conditions provided to the recipient must be made available in a way that allows him to store and reproduce them.

[37] See Article 5, Directive 00/31/EC, which specifies that "the service provider shall render easily, directly and permanently accessible to the recipients of the service and competent authorities, at least the following information: the name of the service provider; the geographic address at which the service provider is established; the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner; where the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and his registration number, or equivalent means of identification in that register; where the activity is subject to an authorization scheme, the particulars of the relevant Supervisory Authority; as concerns the regulated professions: any professional body or similar institution with which the service provider is registered, the professional title and the Member State where it has been granted, a reference to the applicable professional rules in the Member state of establishment and the means to access them; where the service provider undertakes an activity that is subject to VAT, the identification number referred to in article 22, first paragraph, of Council Directive 77/388/EEC of 17 May 1977 on the harmonization of the laws of the Member States relating to turnover taxes, common system of value added tax, uniform basis of assessment. Prices should be indicated clearly and unambiguously, and in particular, must indicate whether they are inclusive of tax and delivery costs". Article 6, Directive 00/31/EC, determines that commercial communications comply at least with the following conditions: "the commercial communication shall be clearly identifiable as such; the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable; promotional offers, such as discounts, premiums and gifts, shall be clearly identifiable as such, and the conditions which are to be met to qualify for them shall be easily accessible and be presented clearly and unambiguously". The same conditions are applied to competitions or games. In fact "the exclusion of gambling activities from the scope of application of this Directive covers only games of chance, lotteries and betting transactions, which involve wagering a stake with monetary value; this does not cover promotional competitions or games where the purpose is to encourage the sale of goods or services and where payments, if they arise, serve only to acquire the promoted goods or services" (see point 16 of the preamble).

[38] In fact the Directive specifies the obligation, for service providers, to clearly identify unsolicited commercial communication by electronic mail sent to recipients, and to regularly consult and respect the opt-out registers containing the names of natural persons who do not wish to receive such communications.

[39] See Article 11, Directive 00/31/EC, which states the following principles: a) "the service provider has to acknowledge the receipt of the recipient's order without undue delay and by electronic means"; b) "the order and the acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them"; c) "the service provider makes available to the recipient of the service appropriate, effective and accessible technical means allowing him to identify and correct input errors, prior to the placing of the order". Letter a and c do not apply "to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communication".

3.2 PART TWO: PRIVACY AND DATA PROTECTION LEGISLATION

When concluding a free contract for Internet Access, the subscriber has to enter his or her personal data, including first name, surname, sex, residence, profession, and the number of a valid identification document into one of the online subscription forms. These data, along with other data collected during connection, are placed by the Provider into three different databases: the first includes personal data and usernames, the second consists of an archive of passwords, and the third (known as the "Log") contains the automatic recording of principal data regarding the duration of connection, the number of operations performed, the IP numbers assigned to the subscriber's computer for the various connections,[40] and the websites visited. Use of the Log enables the Provider to link the data contained in the records with a particular user. In this way it is possible to "monitor" the subscriber's Web activity, partly to check the efficiency of the service, and partly, with special relevance to the various contractual and extra-contractual purposes. These include so-called "profiling", or in order to permit the verification by judicial authorities of possible illegal activities. "Monitoring" does not refer to the processing of all data, but in most cases, as stated in the various forms, it is limited to non-sensitive data[41] useful in creating the subscriber's commercial profile. For sensitive data the written consent of the subscriber and the request for the Supervisory Authority's authorisation (if general authorisation already granted by the Supervisory Authority is not applicable) would be required. With regard to the personal data processed, the subscriber in any case has the rights granted in Directive 95/46/EC: to a lawful and fair processing and "quality" of personal data[42] (Article 6); to express his informed consent (Articles 7 and 10)[43] as also confirmed by the Directive 02/58/EC;[44] to have access to the collected data;[45] to rectify, update, complete the

[40] The IP number is defined as dynamic in that, due to the high number of subscribers and the limited number of IP numbers available, the Provider assigns a different number randomly, for every access by a single computer.

[41] Article 8, first paragraph, Directive 95/46/EC, states that "Sensitive" data is "personal data allowing the disclosure of racial and ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations, or organizations of a religious, philosophical, political or trade-unionist character, as well as of health conditions and sex life".

[42] The expression "quality of personal data" summarizes what is indicated in legislation at letters b, c, d, e, of Article 6, first paragraph, Directive 95/46/EC, stating that data should be: collected and recorded for specific, explicit and legitimate objectives, and used in further processing operations in a way that is not inconsistent with said purposes; accurate and, when necessary, kept up-to-date; adequate, relevant, and not excessive in relation to the purposes for which it was collected or subsequently processed; kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which it was collected or subsequently processed.

[43] The data subject's consent is the fundamental element, along with the information which enables him to understand the way in which, and the purposes for which, his personal information is collected. The information thus loses its characteristic of neutrality and becomes the central point of Directive 95/46/EC.

[44]The Directive 02/58/EC at Article 6, specifies, however, that the subscriber's consent is not necessary for "processing for the purpose of subscriber billing, or for interconnection payments", up until the end of the period during which "a bill may lawfully be challenged or payment may be pursued". The period could apparently extend to the ten-year duration after which unclaimed civil rights lapse. In addition, in third paragraph, for the purpose of marketing electronic communications services or for the provision of value added services, "the provider of a publicly available electronic

data:[46] or to object to the processing of his personal data (Article 14); finally, security in the processing of his personal data (Article 17).

The Internet is "overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications service over the Internet opens new possibilities for users but also new risks for their personal data and privacy".[47]

---

communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent". Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time". Furthermore "The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3" (fourth paragraph). The application of Article 6 is allowed according to Article 7, letter c, Directive 95/46/EC, because the data subject's consent shall not be required "if the processing is necessary for compliance with a legal obligation to which the controller is subject". This rule, a notable exception to the principle of consent to data processing, received considerable criticism from the various European Supervisory Authorities for Data Protection (hereinafter referred to as 'the European Supervisory Authority') during the conference held in Athens on 10 and 11 May 2001, when further confirmation was made of the position that had been stated in April 2000 in Stockholm: "the storing of data for a long, indeterminate period should be considered as a violation of the fundamental rights guaranteed by Article 8 of the European Convention for the protection of Human Rights and Fundamental Freedoms and by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, as well as by articles 8 and 7 of the Charter of Fundamental Rights of the European Union". In this sense, clear disagreement was expressed in relation to "the project according to which Internet Service Providers – in order to provide access to police engaged in the fight against cyber crime – should store data regarding web traffic for a longer period than that necessary for the purposes" of billing alone. According to the European Supervisory Authorities, if it were necessary to store data for longer periods, Providers would have to demonstrate the necessity for the extended period of storing, which in any case should be as short as possible. Directive 00/31/EC, in Article 15, seems to adopt an intermediate stance between the two contrary positions, as it states that the Member States shall not impose a general obligation on providers for monitoring "when providing services covered by Articles 12 (mere conduit), 13 (catching), and 14 (hosting)", but Member States may specifies the obligation of "promptly informing the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service" and of "supplying the respective authorities, on demand, with information enabling the identification of recipients of their service with whom they have storage agreements". In fact the "Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities" (see point 48 of the preamble), but "Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature. This does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation" (see point 47 of the preamble). Whereas the Computer Crime Treatise also includes the obligation for providers to conserve copies of their subscribers' traffic. This approach seems to have become prevalent, seeing that many countries have agreed to the Treatise, including, recently, Italy. The same conclusion has been achieved in Art.15, Directive 02/58/EC, which specifies that "Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union".

[45] See Article 12, second paragraph, letter a, Directive 95/46/EC.
[46] See Article 12, second paragraph, letter b), Directive 95/46/EC.
[47] See point 6 of the preamble, Directive 02/58/EC.

Directive 02/58/EC[48] may be considered the latest important initiative addressing the E.C.'s move to complete the legislative framework on the protection of both personal data and privacy in the communications sector, characterised by "new and advanced digital technologies".[49]

The issue of privacy of email needs to be examined thoroughly. Email service consists of correspondence between given persons:[50] according to Directive 02/58/EC, electronic mail "means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient".[51] The transmission of the email "is completed as soon as the addressee collects the message, typically from the server of his service provider".[52] The Directive confirms the principle of confidentiality in communications[53], making reference to Article 5, Directive 02/58/EC, which also prohibits any form of interception or surveillance by others than the senders or the receivers, except when legally authorized. Thus it is forbidden for Providers to acquire knowledge of, duplicate or cede to third parties, correspondence, even in the form of a summary or abstract of its content. There is an exception in the case of communications containing information which by virtue of its nature or express indications given by the sender is destined to be made public.

It may be considered that documents or messages transmitted via the Internet should be considered by the Provider as the property of the sender up until it has been received by the recipient. Interpretation of this latter paragraph is complex unless one first considers the difference between the electronic mail service and conventional "paper" mail. In the case of email, when the access contract is concluded, the Provider gives the subscriber an email address which consists of the user name and the address domain. The latter identifies the email server in which there is an area of memory, the mailbox, into which the post received is memorized and then sent to the receiver-subscriber's computer, when it is connected to the server (downloading). The route taken by email thus seems to consist of a dual journey: the first from the sender to the recipient's address, and the second from the mailbox to the subscriber's computer by means of downloading (consigning to the receiver). Both operations necessitate the activity of two separate Providers, namely, that of the sender and that of the recipient. The term "consigning to the receiver" would

[48] The provisions of the Directive 02/58/EC particularize and complement European Parliament and Council 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 and European Parliament and Council Directive 02/21/EC of 7 March 2002 on "a common regulatory framework for electronic communications network and services (framework directives)".

[49] See point 5 of the preamble, Directive 02/58/EC. Note that Directive 02/58/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 repealed the former European Parliament and Council Directive 97/66/EC

[50] The e-mail address, consisting of the "user name" and of the "address domain", can be considered personal data.

[51] See Art.2, second paragraph, letter h), Directive 02/58/EC.

[52] See Point 27 of the preamble, Directive 02/58/EC.

[53] See point 15 of the preamble, Directive 00/31/EC.

therefore seem to indicate the moment at which the email "physically" moves from the mailbox to the memory of the receiver's computer, extending the sender's right of property up to this last phase of the route. In such an system, it seems that there are real dangers of violation of secrecy. Therefore it would seem opportune to compile clear, shared rules establishing the minimum security requisites for controlling the area of memory that has to guarantee not just privacy, but also the secrecy of the messages' contents.

The Electronic Commerce Directive confirms the articulate and complex provision discussed above.[54] Emphasis is given to the fact that the above-mentioned Directives 95/46/EC and 97/66/EC are wholly applicable to Information Society Services in that they are sufficient to guarantee secure but unrestricted circulation of personal data among the different Member States. According to this Directive, the Internet constitutes an open network and one cannot prevent its anonymous use.[55] This statement is not just an important sign of recognition of the Web's particular structure, but above all it seems to represent a significant indication for all future Directives. On the other hand, the statement does not appear to forbid the Provider from keeping a log, in which the Provider keeps a user's information. In fact, ascertainment of identity pertains exclusively to access in relation to the provider-user relationship, but it does not prevent the subscriber from protecting his or her privacy by remaining anonymous and requesting an email address different from his or her real name. Anonymity can also be maintained during access to the Web by paying for a temporary connection or by using a public Internet point.[56]

4. The Emergence of a General Consumer Rights Framework

According to the above analysis of the European Directives, there appears to be clear coordination and therefore the emergence of a wider-ranging structure of consumer rights, with the intention of offering a high level of protection.[57] The new figure of the e-consumer thus becomes the object of a complex system of protection in which the regulations concerning consumer contracts and privacy should be considered together. However, this chapter examines these two elements separately, inasmuch as this examination enables any differences in terms for free

[54] See point 14 of the preamble, Directive 00/31/EC.
[55] See point 14, last paragraph of the preamble, Directive 00/31/EC.
[56] The European Supervisory authorities Working Group, in Recommendation 3/97 of 3 December 1997, concerning anonymity on the internet, confirms the need to protect said forms of anonymity while considering those circumstances in which "it is opportune and those in which it is not" by means of a "careful examination of fundamental rights, not just those concerning privacy, but also the freedom of expression (guaranteed both by Article 10 of the European Convention for the protection of Human Rights and Fundamental Freedoms, and by Article F.2 of the Treaty of the European Union) and other important political objectives such as crime prevention", proposing solutions analogous to those adopted for "preceding technology" in the field of telecommunications.
[57] See Article 1, third paragraph, Directive 2000/31/EC.

Internet-access contracts, considering Italian and U.S. contract typologies to be revealed. Following recent discussions on the high level of privacy and consumer protection of the E.U. legislation in comparison to that of the U.S., the different formularies of the free-access contracts in the U.S. and Italy are examined in order to test the real protection of e-consumer rights according to the E.U. legislation.

4.1 DO THE ITALIAN AND U.S. CONTRACT MODELS COMPLY WITH PRIVACY LEGISLATION?

Articles 7(a), 8, and 10, Directive 95/46/EC, referred to by all the Italian contracts examined, require that the data subject give his or her informed consent to the processing of data referring to the subject. The Directive appears to attribute great importance to the breadth and completeness of the information regarding personal data, which differs in content according to the purposes of processing: contractual, statistical, or marketing. In the latter case, information regarding personal data seems to occupy a central role in all free and onerous contracts in which the Provider subjects the data collected to a complex profiling procedure. Typically, such procedures involve communicating the information successively to different subjects, or using it in order to send advertising messages by email.

The Italian Supervisory Authority has highlighted the need for personal data protection in the Internet-access contracts under consideration.[58] It underlined the importance of precise, analytical information according to the indications contained in Article 10, Directive 95/46/EC, in order to attain real privacy protection. This protection should be understood not so much as confidentiality, but rather as transparency in processing data collected both during access and during monitoring of connections. The information regarding the way personal data shall be processed should, according to the Supervisory Authority, therefore be given before the request to provide personal data. It should contain, in one paragraph, in clear, concise form, the various ways in which the information collected will be processed, along with a succinct reference to the rights of access attributed to data subjects by Article 10, Directive 95/46/EC, together with an indication of the office or service where one may exercise these rights. Finally, due consideration is given to the importance of defining all the categories of further subjects to whom the information collected may be communicated and who in turn should obtain the consent of contracting parties, also on behalf of successive subjects.

[58] See Newsletter of the Italian Supervisory authority 24 – 30 Jannuary, "Accesso Gratuito ad Internet e tutela dei dati" at http://www.garanteprivacy.it/garante/doc.jsp ?ID=47192.

According to the Italian Supervisory Authority, the Providers could ask for the consent of contracting parties on behalf of these subjects only when supplying precise information as well as a list of these subjects that can easily be consulted by the data subjects.[59] These statements have caused various Providers to reformulate their contracts.[60] In some contracts, however, the information is still incomplete – and far more frequently, there is no list of the various companies to whom the data collected may be communicated. Such failures infringe the general criterion of proportionality between the information to be supplied and the principle of "fair treatment" as indicated by Article 11 of Directive 95/46/EC.

In U.S. contracts, the information is given in a clear manner but not succinctly, although Providers generally include a series of "Frequently Asked Questions" and answers regarding matters of information collection, data subjects' rights, and security of processing and access.[61] In this respect there are a number of significant differences in comparison with Italian contract models. Above all, the information collected is divided into "Personal Information", supplied at the moment that the contract is concluded (for example, name, address, telephone number etc.), and "Non-Personal Information", defined as information not pertaining to a given person. It is produced by an automatic procedure in which "an aggregated base" comprising the various data relative to the subscriber, or subscribers, is collected and analyzed (hardware and software used, sites visited, IP number assigned for each access). Typically, this is done without any procedure of association to personal data, unlike the above-mentioned situation with data-logs in Italian contracts.

Two important points thus emerge regarding non-personal information; that is, with respect to the nature of non-personal data and the use of an automatic procedure for the collection of various types of information. Both are open to criticism if examined according to privacy legislation. In the first case, the information seems to indicate the non-personal character of the data quite clearly, in conformity with an initial interpretation of Article 1, second paragraph, letter a, Directive 95/46/EC. Here the term "personal data" is used to signify "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".

However, non-personal information may be used to identify the user and it seems that, from an initial examination of the rule, insufficient importance is dedicated to the various correlation

[59] See Report by the Italian Supervisory Authority for the year 2000, page 74.
[60] In particular see the following contracts: Ciaoweb, supra note 1, and Infinito, supra note 1.
[61] See by way of example, the NetZero contract, supra note 1, Privacy Statement: "What is personal identifying information (and other information) does NetZero collect from you?; Where do we collect information from you? How

techniques that the Provider can use, and that this is a legitimate doubt. This suspicion appears to be confirmed by examining "all the means likely reasonably to be used either by the controller or by any other person to identify the said person".[62] This reading is supported by the large amount of data collected, and the sophisticated techniques used for processing, which, notwithstanding the large number of subscribers, offer elements reinforcing the personal nature of the information. The case of unlimited surveillance deals in so-called "sensitive" data. Finally, further confirmation is offered by Article 20, Directive 95/46/EC, referring to the processing likely to present specific risks to data subjects' fundamental rights and freedoms. According to art.20, Directive 95/46/EC, Member States shall determine the processing operations and lay down appropriate safeguards. It is therefore important to consider the second element – the various "instruments" used during collection. In Italian contracts, collection is normally performed by means of the data-log or access recorder, while in some U.S. contracts data is collected and stored inside the subscriber's computer and transmitted to the server by means of the browser supplied on conclusion of the contract.[63] The browser is modified to this end and allows the use by the Provider of further devices, namely cookies and occasionally gif file types or Web Beacons.

Cookies make it possible to personalise certain features of the browser or advertising banner according to the tastes demonstrated by the subscriber. Gifs or Web Beacons are simply one-pixel-sized transmitters in contact with a server that provide continuous information on the sites visited. If the gifs belong to the same advertising company, they can communicate with the cookies present in the computer. Both are potentially worrisome devices as far as privacy is concerned, but cookies are more easily visible because they are contained within a browser directory, and particularly so when clear and precise information is given on them in the contract.[64] Gifs, on the other hand, are invisible by their very nature. Gifs can operate, and in some cases interact, with cookies without it

---

is your information used? Who is collecting your information? With whom do we share your information? How many you access or update your information? How does NetZero protect your personal information?".

[62] See the criterion of interpretation indicated in point 26 of the preamble, Directive 95/46/EC.

[63] The U.S.A. contracts deal with the "software (browser) license agreement" which governs the use of the software design for Internet access, personal data collection and up-load.

[64] See Privacy Statement, Juno, supra note 1, which clearly states that the Provider uses cookies, and adds important information about how they operates in the computer. In Point 25 of the preamble, Directive 02/58/EC, the so-called 'cookies' are considered "a legitimate and useful tool". In fact where such devices are "intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices as to ensure that users are made aware of information being placed on the terminal equipment they are using". Anyway, the users should have the opportunity to refuse to have a cookie or similar devices stored on their terminal equipment. This is particularly important where users other than the original users have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those device during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent

being possible, at least for the subscriber, to detect their presence, as for example in an advertising email. Thus they create a dangerous but highly efficient system which is definitely contrary to the sovereign principle of transparency in the processing of personal data, even when terms describing their functioning and objectives are provided.[65] As regards gifs and cookies (for the latter, only in the case that the contract does not clearly and fully state their existence), their use by the Provider would seem to constitute an infringement of Article 5, Directive 02/58/EC.[66] The latter provision also outlaws any form of interception or surveillance by others than the senders or the receivers, except when legally authorised to do so.

As regards the communication of data collected, U.S. contract models once again make a distinction between non-personal and personal data. The former can be freely communicated together with personal data processed by means of an aggregated base, a solution that complies with Article 11, Directive 95/46/EC, second paragraph. On the other hand, in the case of personal data, its communication is possible only with the consent of the subscriber, who can give consent individually for all those third parties who have concluded commercial agreements with the Provider and who are of interest to it.

In this case it should be possible to devise a contractual solution that provides greater protection to the data subject with regard to consent given for the communication of personal data. A different situation is the transfer of data to another data controller, as provided in some U.S. contracts under which the Provider undertakes to transfer data only in the case that the new controller resolves to accept the same privacy statement. More specifically, according to the Directive 95/46/EC, data may be transferred to another controller, provided that it is intended for a processing operation that is carried out for purposes similar to those for which it has already been collected. Therefore, it confirms what could be defined as "continuity of purpose" with regard to the processing of personal data. In this context, the purpose itself can be expressed in three stages:[67] the

should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.

[65] See point 24 of the preamble, Directive 02/58/EC, which correctly underlines the dangers of "so-called spyware, web bugs, hidden identifiers and other similar devices". These can "enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users". But, in contrast with these premises, the Directive, in the same point 24, states that "the use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned". In the United States, the Gif is at the center of a heated debate, and the White House has determined that Gifs should not be used in the government site for the anti-drugs campaign, and the same has been decided, more generally, at a Federal level. There have been many lawsuits in this respect, regarding the violation of consumer privacy protection (on this point, see Italian Privacy Supervisory Authority, Newsletters of 4 – 10 June 2001, "U.S.A. Il sito della difesa U.S.A. raccoglie dati su navigatori" at http://www.garanteprivacy.it/garante/doc.jsp?ID=43452, and of 17 – 23 July 2000, Privacy, "USA. Un nuovo dispositvo per spiare la navigazione su Internet" at http://www.garanteprivacy .it/garante/doc.jsp?ID=46238.

[66] On this point see also point 15 of the preamble, Directive 00/31/EC.

[67] See Article 6 and point 28 of the preamble, Directive 95/46/EC.

collection for precise purposes ("principle of pertinence"); processing uniquely for the purpose for which it was collected ("principle of non-unlawful use"); and the elimination or transformation into anonymous data of the data no longer necessary ("principle of the right to oblivion").[68] Transfer of data therefore has to respect the same breadth and precision in limitations on purpose,[69] outside of which any processing should be considered as illegal.

There appears to be particular importance attached to the term of the U.S. contracts regarding subscriber rights concerning access to, alteration of, or erasure of his or her personal data. However, the term gives subscribers a lesser degree of control of their own data when compared to the provisions of Article 12, Directive 95/13/EC. [70] This is particularly so when considering the role of the Supervisory Authority, which carries out an important task of monitoring the way in which data subjects' rights are protected.[71] However, in some U.S. contracts analysed,[72] Providers are members of the TRUSTe certification program. This is an independent, non-profit initiative whose mission is to build up Internet users' trust and confidence in the services by promoting TRUSTe's principles of disclosure and information consent. Providers agreed to disclose their information practices and to allow their privacy practices to be reviewed for compliance by TRUSTe. The adoption of the so called "privacy seal" provides a third-party control and completes a self-regulatory system which is based, not on laws but on users' trust. Art. 27 of Directive 95/46/EC seeks to provide a wide and compelling implementation of privacy law by encouraging the adoption of codes of ethics and conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive. It is important to underline the importance of adopting a code on "telecommunications services provided by means of telematica and particularly Internet", which will "make the public and commercial telecommunications network's users aware of the processing of personal data within the adoption of interactive information according to lawful and fair processing of personal data".[73] The above-mentioned code imports new and important duties regarding the lawful processing of personal data, but it cannot be compared to the TRUSTe privacy programme, either for the code process between the Supervisory

[68] RODOTÀ, TECNOLOGIE E DIRITTI, 62 (1995).

[69] On the other hand, Spanish law requires that the data-subject receive prior notification of the transference to another controller(see Article 25) and his consent is necessary (see Article 11). Such consent is considered as void in the case that the transferee is undetermined or indeterminable, or when the purpose of the transference is not clear.

[70] On this point see the Privacy Statement of the NetZero.com contract, supra note 1, which deals only with a complex procedure in order to modify the personal data provided at the beginning of the contract,

[71] See Article 28 Directive 95/46/EC.

[72] Now the following providers are no longer members of the TRUSTe certification program: Juno.com; Winfire.com; Netzero.com, see supra note 1.

[73] See Report by the Italian Supervisory Authority for the year 2000, at http://www.garanteprivacy.it/garante/navig/jsp /index.jsp , page 54.

Authority and Providers, or the relevance of the code that may be considered in the different States' "real atypical sources of law providing rules for a lawful proceeding of personal data".[74]

The terms of security of the provided services in U.S. contracts include a dual distinction between security in data processing and security in Web access. The former regards protection in the case of various dangers concerning "loss, misuse and alteration"[75] of the personal data collected. Thus, Article 17, first paragraph, of Directive 95/46/EC, provides that Member States must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Furthermore, it is affirmed that "having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected".

On the other hand, Web access security seems to be a particularly important and complex element when one considers that users generally visit sites, download programs, and receive emails. These are all potentially vulnerable activities as a result of the possible presence of viruses that could damage the computer's software or hardware, and problematic also in the case that the computer is being used by a minor, as a result of the images and content of the texts encountered. In some U.S. contracts, precise indications of the various risks are given, along with suitable measures and respective costs that can increase user security during access with regard to the various dangers deriving from access to the web.[76] This constitutes a point of difference with respect to all Italian contract models, in which possible dangers are, normally, mentioned only in reference to the subscriber's obligations, such as the safe custody of a password. The importance of Web access security, however, receives authoritative confirmation in Article 4, Directive 02/58/EC,[77] which

[74] See Report by the Italian Supervisory Authority for the year 2000, supra note 73, page 16.

[75] By way of example, see: Privacy Statement, Juno.com, supra note 1, which states: "All information provided to us by our subscribers is stored on secure computers, where it is made available only to Juno staff members or representatives who need it to do their jobs. (For example, it may be necessary for Juno staff members or representatives to examine system operational and accounting logs and other records to resolve service-related problems). If we need to share any of your personal information with any company performing services for us, that company must agree to confidentiality restrictions and security measures to safeguard such information".

[76] In particular see the Privacy Statement, Juno.com, supra note 1, (now in different sections) which treats problems concerning security and respective solutions thoroughly, as can be seen from the various terms which are, in some cases, subdivided into a number of points: "Guarding against online fraud" (password security, what to do if you receive unwanted e-mail, how to avoid common Internet schemes, unauthorized use of your account); "Internet Security"; "Internet Security software"; "Password Protection"; "Worms and Virus".

[77] The Directive 02/58/EC, states about the "confidentiality of the communications" at Article 5, and in point 20 of the preamble underlines the importance of the web access security: "Service providers should take appropriate measures to safeguard the security of their services, if necessary in conjunction with the provider of the network, and inform subscribers of any special risks of a breach of the security of the network. Such risks may especially occur for electronic communications services over an open network such as Internet or analogue mobile telephony. It is particularly important for subscribers and user of such services to be fully informed by their service provider of the existing security

specifies that the "provider of a publicly available telecommunications service" must inform subscribers of "a particular risk of a breach of network security", with indications of "possible remedies, including the relevant costs". The first paragraph of the same article, however, states that the provider should "take the technical and organisational measures" in terms of data processing security, with respect to just the area of pertinence mentioned to safeguard security of the service provided and of personal data[78]. The two paragraphs therefore appear to indicate on the one hand the limit of ordinary risk and the Provider's liability, and on the other clearly indicate a precise security obligation regarding the service and personal data with the provision of measures necessary for protecting the subscriber from the various dangers linked to access, with the limits as indicated in the third paragraph, for example the supply of anti-virus software and a firewall.[79] Furthermore, they confirm the protection of personal data at the dynamic stage of reception or transmission of data between Provider and subscriber,[80] for example the password and the user-name entered every time that the user logs in.

Finally, regarding email, the terms of the various Italian and U.S. contracts examined follow the general principle of secrecy of correspondence. Therefore, the Provider undertakes not to verify, censure or check content, except for the automatic cancellation of the contents of the mailbox memory, either at the withdrawal from the contract or, in the case in which the subscriber does not use the service for a certain period of time, with prior warning. Although the secrecy of correspondence in this case is guaranteed, another party has been forgotten: the sender. According to the interpretation attributed to the term "consignment" (successful downloading of messages to the receiver's computer), the regulation leads one to surmise that the Provider has the obligation, in the above-mentioned cases, of retransmitting messages to their respective senders. The same thing happens now to the sender when the address is unknown, in which the sender-Provider sends back the message to the sender explaining why the deliver has been unsuccessful.

---

risks which lie outside the scope of possible remedies by the service provider. Service providers who offer publicly available electronic communications services over the Internet should inform users and subscribers of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform subscribers of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge except for any nominal costs which the subscriber may incur while receiving or collecting the information for instance by downloading an electronic mail message. Security is appraised in the light of Article 17 of Directive 95/46/EC".

[78] See Article 17, first paragraph, Directive 95/46/EC.

[79] Both features are important means of defence for the subscriber's computer. The anti-virus software detects and, in some cases, eliminates, viruses. The firewall is a device that enables computer systems to be isolated from illegal intrusion from the web by means of various techniques: software (filtering data parcels) or hardware (gateway at programme level, gateway at connection level, proxy server).

[80] Conversely, at the moment of processing and storing in a data bank, Directive 95/46/EC would apply.

4.2. DO THE CONTRACTS MODELS EXAMINED COMPLY WITH THE EU UNFAIR CONTRACT TERMS LEGISLATION?

A careful examination of the contractual documents the customer is invited to print from the Web page before the contract is concluded reveals several points. These include the identity of the ISP, the essential characteristics of the service, the duration of the validity of the offer, the minimum duration of the contract, and the possibility of terminating the contract at any time. Thus the contracts comply with Directive 97/7/EC, in particular Article 4, (prior information), Article 5 (written confirmation of information or confirmation in "another durable medium available and accessible to subscriber") and Article 6 (assertion of the right of withdrawal). The latter point specifies that the consumer can exercise the right of withdrawal within a period of at least seven working days after the day of conclusion of the contract or from the day on which the obligations of information in writing were met. In the case that the Provider has not met the obligations of "written confirmation of information", the term in which the right of withdraw can be exercised is three months, starting from the day on which the contract was made. In addition the consumer is expressly invited to give his or her consent as regards the dispatch of email advertising messages according to the terms of Article 10, second paragraph, regarding the possibility of using distance communication techniques only if the recipient has given his or her consent.[81]

Furthermore, the contract according to Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts requires examination. The "evaluation" of the degree of unfairness of a term or terms should refer to the list that confers a value as "a general clause" to Article 3, first paragraph, Directive 93/13/EEC. This provision specifies the unfair nature of terms included in contracts concluded between consumer and supplier which, "contrary to the requirement of good faith, cause a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer". The Directive includes a series of elements useful in

[81] The legislation thus includes prior consent on the part of the recipient, the so-called opt-in technique, for distance communications such as "telephone, electronic mail, automatic calling systems without human intervention, or facsimile machines or electronic mail for the purposes of direct marketing" (Article 13, first paragraph, Directive 02/58/EC), Otherwise, the so-called opt-out technique is used, both in Article 13, first paragraph, Directive 02/58/EC, regarding means of distance communication, other than those referred to in paragraph 1, and in Article 7, of the Directive 00/31/EC. The latter does not change the structure of the above-mentioned rule because, as stated in the article itself, it does not prejudice "Directive 97/7/EC, regarding consumer protection in distance contracts and Directive 97/66/EC, regarding personal data processing and the protection of privacy in the telecommunications sector" (Directive 97/7/EC is no longer in force, in fact it has been repealed by Directive 02/58/EC). In cases differing from those detailed by these Directives, pursuing to Article 7, second paragraph, the Member States shall take "measures to ensure that service providers undertaking unsolicited commercial communications by electronic mail consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves". The area thus covered by the directive is confirmed by point 30 of the preamble that reads "the

assessing the degree of unfairness. These are, in particular, "the nature of goods or services for which the contract was concluded", "the time of conclusion of the contract", "all the circumstances attending the conclusion of the contract", and "all the other terms of the contract or of another contract on which it is dependent".[82] Such elements, according to some commentators, seem to refer to consumer contracts without any limitations (notwithstanding the above considerations) as regards the terms included or not included in the "list" or otherwise relating to standardised contract models: "They confirm the important notion of an economic operation as a formally logical unit consisting of a unitary, composite sequence. This sequence comprises the contract, the patterns of behaviour linked to this in order to achieve the desired results, and the objective situation within which the system of rules and other patterns of behaviour are located."[83] The definition of a contract in terms of economic operation seems to lend weight to provisions on consumer protection, the absence of which, at the moment of the implementation of these provisions, could produce deformation according to an abstract forecast of unfairness not relating to significant elements such as sale price or the existence of a fee. This leads to the conclusion that the asserted "costlessness" of the contract could become a relevant factor in the examination of the unfair quality of terms.

Therefore, some of the "safeguards" included in the Directive 93/13/EEC on unfair terms in consumer contracts would appear to have no particular reason to be there, because there would seem to be no possibility of an imbalance in favour of the supplier in the free contract for Internet access. However, this assertion, which prevents the application of the "safeguards", is subject to a significant limitation as regards the area of privacy, because privacy constitutes an important element that is wholly within the sphere of consumer protection. Therefore privacy certainly appears to have a certain degree of relevance to the discussions on unfairness. While if unfairness were totally extraneous to privacy, as regards consumer protection, there would have to be a set of rules that would actually impede, or render problematic, the application of elements protecting the consumer, such as obliging the consumer to fulfill all her obligations when the supplier does not perform hers, or unduly restricting the evidence available to him.

Therefore the next section will examine common Italian and American contract models.

4.3 Identifying Unfair Terms in the Contracts under Examination

The unfair terms identified in the various contract models can be separated into two groups. The first comprises the terms that depart from the principle according to which the contract is

question of consent by the recipients of certain forms of unsolicited commercial communications is not addressed by this Directive, but has already been addressed, in particular, by Directive 97/7/EC and by Directive 97/66/EC".

[82] See Article 4, first paragraph, Directive 93/13/EEC.

legally binding for the parties. The second group comprises terms relative to the supplier's self-help and limits on defence of consumer rights.[84]

The first group can be subdivided into three subgroups. The first Group consists of the terms that revoke the principle of "no alterableness of the terms of the contract". In some contract models, in particular in the U.S., the subscriber is required to agree to terms with which he or she had no real opportunity of becoming acquainted before the conclusion of the contract, and to a term that gives the Provider the right of "adding to" or "altering" the terms of the contract at a later stage. With regard to the latter possibility, the unfair nature of the term can possibly be excluded if one can identify a "valid reason" as indicated in subparagraph J, Annex, Directive 93/13/EEC. The term is considered as unfair when it gives the supplier the power of altering unilaterally the terms of the contract "without a valid reason specified in the contract" and simply in consequence of his or her unchallengeable discretion. The term that attributes *jus variandi* should be dealt with "valid reason", because otherwise it becomes unfair, as in the term included in a number of access contracts giving the Provider the possibility of modifying the service at will, or even in *pejus*, reserving the right to suspend, interrupt or modify the service at its own unchallengeable discretion. As regards terms irrevocably binding the consumer to terms with which he had no real opportunity of becoming acquainted before the conclusion of the contract (considered as unfair according to subparagraph i), Annex, Directive 93/13/EEC), the interpretation to be preferred should be that they are unfair only if they tangibly prejudice the consumer's position because they produce a significant imbalance and are in contrast with the principle of good faith. The contrary solution would contradict the logic of consumer protection as expressed by the legislation in question. The terms concerning the right of modifying the subject matter of the contract are unfair if they give the supplier the right to "giving the seller or supplier the right to determine whether the goods or services supplied are in conformity with the contract, or giving him the exclusive right to interpret any term of the contract".[85] The first part of the rule deals with the assessment of the conformity of the goods or service supplied. The second part of the law under examination completes the above-mentioned limit to *jus variandi* imposed onto the supplier by legislation, and it specifies the unfair nature of the term relative to the supplier's exclusive right to the interpretation of any term in the contract, if this be based on criteria of interpretation determined purely according to the Provider's discretion, and not linked to other elements such as technical details.

[83] Enrico Gabrielli- Andrea Orestano, Contratti del consumatore, DIGESTO DELLE DISCIPLINE PRIVATISTICHE, Sezione civile, Aggiornamento, 225, 250 (UTET 2000).
[84] See Giorgio De Nova, La novella sulle clausole vessatorie e la revisione dei contratti standard, RIVISTA DI DIRITTO PRIVATO, 229 (1987).
[85] See Subparagraph K), Annex, Directive 93/13/EEC.

The second sub-group regards terms that contravene the principle of "irrevocable consent". The contracts examined reveal terms that are unfair according to Subparagraph G, Annex, Directive 93/13/EEC, and which enable the supplier to terminate the contract at any time without "reasonable notice", except where there are "serious grounds for doing so".[86] The unfair character of such terms can be identified in the absence of any prior warning, or in an excessively brief period of forewarning, again in relation to an assessment that concerns the incongruous disadvantage for the consumer, and therefore the significant imbalance in the parties' rights and obligations arising under the contract, as per Article 3, first paragraph, Directive 93/13/EEC. As regards "serious grounds for doing so", the norm refers to a significant degree of non-performance of the contract and to the repercussions that extraordinary and unforeseeable events may have on the contract. In this sense, there seems to be an increase in the protection of the consumer as regards terms that enable the Provider to terminate the contract in the case that the subscriber does not wish, for example, to subject himself to a wide-ranging and illegal application of *jus variandi*.

The third sub-group includes the terms that contravene the principle according to which "the contract has to be performed". In this case, the terms in question regard the Provider's exemption from all liability, which contradicts Subparagraph (a) and (b), Annex, Directives 93/13/EEC regarding consumer contracts. These provisions seem to provide for the supplier's liability even in the case of negligence, rendering unfair a term that excludes or limits the consumer's legal rights vis-à-vis the supplier in the event of total or partial non-performance by the supplier of any of the contractual obligations. In accordance with what has been stated, terms assessed unfair include those in which the subscriber undertakes to give his/her warranty to the company providing the service, that the company be exempt from any damage, loss, liability, cost or expense, including legal costs, deriving from any contravention of the regulation.

However, considering the free nature of the service, and the impossibility on the part of the Provider of monitoring and promptly preventing illegal activities performed by subscribers on the Web, an assessment of unfairness would seem to be less severe in the case of terms referring to the subscriber's exclusive liability in the case of illegal use of the service. In fact the subscriber has to be aware of all the provisions necessary to avoid committing illegal activities online.[87] Therefore the Provider's liability appears to be limited, in the various contract models examined, to the collection and processing of personal data, including the provisions of Directive 95/46/EC that state

[87] In Italian contracts, terms are formulated along general lines, with reference to the prohibition on using the service in a way that contravenes the laws of the Italian State or any other country, and/or conventions, treatises, agreements or international regulations. Some American contract models differ in that the same terms are clearer and more detailed, such as the following actions have been clearly pointed out: Unlawful purposes, Unwanted Materials, SPAM. Unauthorized Trademark Use.

that personal data must be kept and controlled by the Provider,[88] and the Provider shall be liable for damage resulting from the processing of personal data or the failure to take measures required for data security.[89] On the other hand, the total liability of the subscriber can be identified in the case of illegal activities carried out over the Web,[90] in conformity with the Directive on Electronic Commerce, which specifies that the ISP is not liable in the case in which it meets the following conditions:[91]

a. Does not modify the information;
b. Complies with conditions on access to the information and rules regarding the updating of the information, as specified in a manner widely recognised and used by industry;
c. Does not interfere with the lawful use of technology, as widely recognised and used by industry, to obtain data on the use of the information;
d. Acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

Finally, the term giving the Provider the possibility of transferring its rights and obligations under the contract to indeterminate subjects, as is the case for nearly all the contract models examined, can be included in the same sub-group. The term appears to be unfair because it allows the supplier to substitute a third party in his own place as regards the rights and obligations under the contract, with the risk that "the guaranties for consumer may be reduced".[92] A more detailed examination of the rule seems to exclude unfairness in the case that the Supplier indicates specific elements assisting the determination of the third party in order to avoid a future, imponderable reduction of the guarantees for the consumer.

[88] See Article 3, Directive 95/46/EC.
[89] See Article 17, 23, 24, Directive 95/46/EC.
[90] An offence committed on the web does not seem to have its own independent character, but preserves the same characteristics of unlawfulness that it has outside the web. The European Commission, in Communication of 16 October 1996, Information on unlawful and harmful content on the Internet, states that "what is illegal outside the web is also illegal on the web".
[91] This rule is included in the fourth section, "Liability of intermediary service providers" of the Directive, which provides for the exemption of liability not just of Service Providers (Article 13) but also Access Providers (Article 12), of and Hosting Service Provider (Article 14). In particular regarding the Internet Access Provider, Article 13 states that the provider is not liable in the case he meets three conditions, the provider: "a) does not initiate the transmission; b) does not select the receiver of the transmission; c) does not select or modify the information contained in the transmission".
[92] See Subparagraph (p), Annex, Directive 93/13/EEC.

The second group comprises terms regarding the Supplier's self-help and limits on defence of consumer rights. These terms exclude or hinder the consumer's right to take legal action or exercise any other legal remedy. In various contract models, one notes terms that impose forfeitures, or limitations on the consumer's right to raise objections, or unduly restrict the evidence available to him or a burden of proof which, according to the applicable law, should lie with another party of the contract. These terms seem to be unfair in the light of a preliminary examination, according to Subparagraph q, Annex, Directives 93/13/EEC.

Finally, according to Article 12, Directive 97/7/EC and Article 7, Directive 93/13/EEC, Member States shall take the measures needed to ensure that the consumer does not lose the protection granted by these "Directives by virtue of the choice of the law of a non-member country as the law applicable to the contract if the latter has close connection with the territory of one or more Member States".

5. CONCLUSION

This study reveals the complexity of a discipline undergoing continuous development. Gradually, one can denote, in the wake of the Directive on Electronic Commerce, a correspondence between the various rules concerning consumer protection, with great importance attributed to privacy regulations. However, the various rules on privacy protection seem to have been incorporated into Italian contract models only to a minimum extent, as had already been revealed by the analysis performed by the Italian Supervisory Authority with respect to free Internet-access contracts. As a result, a number of suggestions are made with the objective of compiling information regarding personal data processing that complied with the provisions contained in the Italian Privacy Code with particular reference to obligations concerning personal data processing.

In addition, with regard to various petitions promoted by an Italian consumer defense association (CODACONS) against some of the leading telephone operators providing free Internet access and services,[93] the Italian Competition Authority has highlighted the importance of personal data collection in profiling and in the Provider's capability of sending the consumer advertising email messages. Both have been defined as true burdens subject to consumer consent according to the provisions in legislation for privacy and distance contracts, complying with the above mentioned directives. Therefore, the hypertextual links labeled "free access" are considered in all

[93] See Ruling n° 10270 (Tiscali "Mail Spamming"); Ruling n° 10279 (Libero-Infostrada message on the Internet), and Ruling n° 10278 (Kataweb messages on the Internet) at http://www.agcm.it/tema0210.htm.

respects as advertising messages[94] and have been judged by the Competition Authority to be lacking significant information necessary for the consumer to evaluate the actual benefits of the service advertised.

Referring to the "second" element (consumer protection), various unfair terms were identified once again in Italian contract models, but above all in those of the U.S. In Italian contracts, an examination of the sequence of terms revealed the lack of a clear structure. This was so in particular as regards the description of the access service itself and the subscriber's liability. Most of the American contracts, on the contrary, are organised more clearly, using a hypertext structure that makes their reading and comprehension easier and more extensive, partly as a result of the use of question-and-answer schemes.

In conclusion, it does not seem possible to identify a "winner" in the comparison between Italian and American contracts in matters of privacy and consumer protection. But the examination and critiques of the various terms that contravene existing legislation allow us to identify a model of reference, and highlights the importance of a legal framework that is capable of establishing the correct balance between the rights and duties of the e-consumer.

[94] On this point, see Italian Supervisory Authority for Competition, Ruling no.10278, which considers that "considering the medium used for publication and the contract, both the button on the Kataweb home page, and the pages linked to it by means of hypertext links, form a single advertising message. In fact, in this sort of case, on one hand there is a logical connection between the link from the single word to the page containing the adhesion form and the information concerning the services offered, and on the other hand the activation of the "Free Internet" link connects the user directly and univocally to these web pages. In this light, the "slogans" under examination can be considered as part of a more complete and unique message whose content is divided amongst a series of screen-views, though the latter do not appear as fragmented and they cannot be mistaken for a different context or moment in time".