is essential that the structures be in place to ensure the implementation of the *acquis communautaire*.

It would be a mistake to paint too rosy a picture. Some of the most problematic issues still have to be tackled in the negotiations. The Commission has given the benefit of the doubt in many areas as regards preparation. Thus, although the overall picture is encouraging, very serious issues of preparation remain, as the assessments for both political and economic criteria show. The strong sense of optimism engendered by progress, must be tempered by the realization that the conditions have not yet been met. It is still quite possible that there may be a slippage in the time-frame, or that not all ten States may accede at the same time.

The accession seems near, furthering the aim set out in the recital to the EEC Treaty in which the original treaty-makers, with the goal of preserving and strengthening peace and liberty, called "upon the other peoples of Europe who share their ideal to join in their efforts". That heroic aspiration fulfilled, the Europe of 25 or 27 or more will have to take the necessary steps to create a European framework which is more democratic and nearer its citizens.

Common Market Law Review 38: 1337–1384, 2001.

A EUROPEAN COMMUNITY REGULATORY FRAMEWORK FOR ELECTRONIC COMMERCE

AURELIO LOPEZ-TARRUELLA *

1. Introduction

The Lisbon European Council, held on 23–24 March 2000,[1] was the starting point for a global policy of the European Union *vis-à-vis* the Information Society. It set the ambitious objective for Europe to become the most competitive and dynamic economy in the new environment. At that summit, the Heads of States endorsed the principles, embedded in the Commission *eEurope* Initiative,[2] which should inform the steps to be taken by the European Union in order to gain most benefit in all socio-economic areas from the technologies of the so-called Information Society. Moreover, the Commission and the Council were asked to work on an Action Plan for that purpose. In that document,[3] specific key target areas are identified where action must be taken in a first stage – ending before 2002 –, in order to accelerate the uptake of digital technologies across Europe and to ensure that all Europeans have the necessary skills to use them. On 19–20 June, in Feira (Portugal), the European Council endorsed the Action Plan.[4] The key target areas are: the consolidation of a cheaper, faster and secure Internet;[5] investment in people and skills;[6] and stimulation of the use of the Internet. In this last area, the Commission

* Assistant of Private International Law. University of Alicante (Spain).

1. See Presidency Conclusions. Available at http://ue.eu.int/Info/eurocouncil/index.htm

2. Commission Communication "eEurope – An Information Society for All". COM (1999)687 final. Available at http://europa.eu.int/comm/information_society/eeurope/documentation/index_en.htm

3. Commission and Council Action Plan "eEurope 2002". Available at http://europa.eu.int/comm/information_society/eeurope/documentation/index_en.htm

4. See Presidency Conclusions at 22. Available at http://ue.eu.int/Info/eurocouncil/index.htm

5. For that purpose measures shall be taken in order to achieve: a) cheaper and faster Internet access, b) faster Internet for researchers and students, c) secure networks and smart cards.

6. A key-target that implies: a) introduction of European youth to the digital age; b) working in the knowledge-based economy; c) participation for all in the knowledge-based economy.

addresses the need to accelerate the consolidation of electronic commerce.[7] For this, up-to-date legislation that fully meets the needs of business and consumers is essential. The existing Single Market regulatory framework has proved its efficiency for traditional forms of business, but it must now be adapted to work for electronic commerce.

Internet is one of the features associated with the new Information Society. Among other merits, it constitutes a new media where economic relations can take place. Electronic commerce consists of the use of such communication media for doing business.[8] Initially, it allowed businesses to communicate easily among themselves, so that commercial transactions were facilitated.[9] However, once Internet became accessible to the general public and World Wide Web was created, a new kind of economic actor appeared, the "Information Society service providers" whose activity is to provide services in or related to the Internet. Another feature of the new Information Society is that the provision of services and the exchange of information is replacing in economic relevance the production and trade of goods.[10] Improvements in computer technologies facilitate the digitalization, processing and storing of great quantities of information that can be transmitted electronically or can be made accessible to several recipients in different places for its retrieval at their request.[11] The global nature of the Net enables service providers

7. For this purpose, the following should also be promoted: a) government online: electronic access to public services; b) health online; c) European digital content for global networks; d) intelligent transport systems.

8. See the Commission Communication "A European Initiative for Electronic Commerce" (COM(1997) 157 final), at 5 and *Electronic Commerce – An Introduction*: "Any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact". Available at http://europa.eu.int/ISPO/ecommerce /answers /introduction.html.

9. The so-called business-to-business sector of electronic commerce. An example in this category would be a company that uses a network for ordering from its suppliers, receiving invoices and making payments. This category of electronic commerce has been well established for several years, particularly using Electronic Data Interchange (EDI) over private or value-added networks. See Rowland and McDonald, *Information Technology Law* (Cavendish, London, 1997), pp. 225–242 and Julia Barceló, *Comercio electrónico entre empresarios* (Tirant lo Blanch, Valencia, 2000). The use of EDI was also the object of Commission Recommendation 94/820 of 19 Oct. 1994 relating to the legal aspects of electronic data interchange, O.J. 1994, L 338/98.

10. Unlike tangible goods, intangible goods such as digitalized contents accessible over Internet, can be reproduced. You can only distribute a tangible good once, but you can distribute as many copies of intangible goods as you want. This circumstance is said to involve changes in the conception of the economic markets, see Rifkin, "Réseaux contre marchés", *Le Monde Diplomatique*, No. 568, 22–23.

11. Information to be digitalized for its subsequent storing, processing and electronic delivery includes text, audio and video files. The coalescing of the broadcasting, electronic communications and information technology sector has been addressed in the European Commission "Green Paper on the Convergence of the Telecommunications, Media and Information Technology Sectors" (COM(1997)632 final). See also Grewlich, "Cyberspace: Sector-specified regulation and competition rules in European telecommunications", 36 CML Rev. (1999), 937–938.

to reach clients in any country: websites can be visited from any place in the world. Furthermore, distances are not relevant on Internet: contracts can be concluded with someone at the other side of the world as easily as with someone living in the same city.

The Internal Market provides an excellent framework for businesses to consolidate and to benefit from a potential 400 million-person market: while the Internet eradicates physical borders, the Internal Market removes legal borders.[12] However, electronic commerce affects many fields of law where numerous legal adaptations are needed and a number of uncertainties must be removed to clarify the regulatory framework. The European Community is aware of this problem. In fact the *eEurope* Action Plan states as a fundamental method for achieving the targets to "accelerate the setting of an appropriate legal environment".[13] In this sense, a fundamental legal instrument has already been adopted: Directive 2000/31 on Electronic Commerce.[14] Its objective is to harmonize national legislation so that European service providers can benefit from the freedom to provide Information Society services in a "Single Online Market".

The main purpose of the present article is to study that fundamental Directive, whose transposition in the Member States is due by 17 January 2002.[15] However, due to the vast amount of matters Internet affects, the picture would be incomplete if we did not also refer to other legal instruments applicable to electronic commerce. These are, for instance, Directive 2001/29 on the harmonization of certain aspects of copyright and related rights in the Information Society,[16] and Directive 1999/93 on a common framework for electronic signatures.[17] As another author has affirmed, Directive 2000/31 contains six directives in one:[18] it deals with six legal matters which could have been regulated in six different legal instruments. In our opinion, it was

12. "L'Internet et le Marché intérieur ont pour point commun de supprimer les frontières, physiques pour le premier, juridiques pour le second": see Crabit, "La Directive sur le commerce électronique. Le projet 'Méditerranée'", (2000) *Revue du Droit de l'Union européenne*, 753.

13. See Action Plan at p. 2.

14. Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of Information Society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce, O.J. 2000, L 178/1). Documents issued through the long procedure of adoption can be accessed in the University of Alicante Intellectual Property and Information Technologies Internet Portal: http://www.uaipit.com

15. Art. 22.

16. O.J. 2001, L 167/10.

17. O.J. 2000, L 13/12.

18. Desantes Real: "La Directiva sobre el Comercio Electrónico. Mercado interior y servicios de la Sociedad de la Informacion" in Mateu de Ros and Cendoya Mendez de Vigo (Eds.),

a better option to regulate all these issues in a single instrument. Establishment of the freedom to provide Information Society services was not an easy objective to attain, taking into account the horizontal nature of the Directive, the vast scope of the coordinated field, and the uncertain relation of Private International Law rules with the country of origin principle. This being so, harmonization was needed on certain specific aspects where Member States' legislations turned out to be extremely divergent, in order to facilitate the completion of the Single online market. Those questions needed to be addressed in the same instrument to ensure coherence, as the solutions provided are interlinked.[19]

The present paper, following the structure of the Directive itself, first explains the basic principles for the establishment of the freedom to provide Information Society services, and then it deals with some other legal questions which may crop up in the different steps of the service provider's economic activity: promotion of products and services, electronic contracts, liability of intermediary service providers, law enforcement mechanisms. Lastly, brief considerations on the external dimension of the European Union's Information Society policy are given. We conclude with some brief remarks.

2. Free movement of Information Society services

The basic purpose of Directive 31/2000 is to remove legal obstacles and uncertainties and to harmonize existing legislation in the Member States in order to ensure the free movement of Information Society services within the European Community.[20] In conformity with the proportionality principle, the Directive only harmonizes specific aspects of the economic activity of service providers so that the freedom of movement can be guaranteed.[21] Other legal aspects affecting electronic commerce were excluded from the scope of application[22] insofar as they were either the object of specific instruments or legislative proposals – that is the case with the protection of personal data,[23]

Derecho de Internet. Contratación Electrónica y Firma Digital (Aranzadi, Pamplona, 2000), p. 323–338.

19. See Commission Proposal for a Directive on certain legal aspects of electronic commerce in the internal market (COM(1998)586 final), p. 15.

20. Art. 1.

21. Recital 10.

22. Art. 1(5).

23. Governed by Directive 95/46 of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (O.J. 1995, L 281/31) and Directive 97/66 of 15 Dec. 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (O.J. 1998, L 24/1).

with the field of taxation[24] and with the regulation of cartels[25] –, or because freedom to provide service was impossible to guarantee given the lack of mutual recognition or sufficient harmonization to guarantee an equivalent level of protection of general objectives.[26]

The establishment of the freedom to provide Information Society services is based on three principles:

– country of origin principle: service providers' activities are supervised by the competent authorities of and are subject to the law of the Member State where they are established (2);

– non-authorization principle: the pursuit of those activities can not be subject to prior authorization (3); and

– transparency obligation: there is a minimum amount of information that service providers must provide about themselves and their economic activity (4).

Notwithstanding the fact that these principles are similar to those adopted in other recent Community instruments on free movement of services,[27] due to the inherent global nature and technical features of the Internet, and the great number of activities which Information Society service providers may pursue (1), their implementation in this field requires detailed explanation.

2.1. *Information Society Service Providers: The horizontal nature of Directive 2000/31*

Despite the fact that the concept of service provider ("ISP") is very recent, the Directive on electronic commerce is not the first in which the term is used.

24. Proposal for a Council Directive amending Directive 77/388/EEC as regards the value added tax arrangements applicable to certain services supplied by electronic means and Proposal for a Regulation of the European Parliament and of the Council amending Regulation 218/92 on administrative co-operation in the field of indirect taxation (VAT) (Doc COM(2000)349 final, O.J. 2000, C 337 E/65.)

25. Commission Proposal for a Directive on a common regulatory framework for electronic communication networks and services (COM(2000)393 final, O.J. 2000, C 365 E/1). Recently, a public consultation has been opened by the Commission pursuant to a Draft Commission Directive on competition in the markets for electronic communication services, O.J. 2001, C 96/2.

26. See Recital 12. Those areas are: a) activities of notaries or other professions involving a direct and specific connection with the exercise of public authority, b) representation and defence of a client before a court, and c) gambling activities.

27. In the Television Broadcasting sector, Council Directive 89/552/EEC of 3 Oct. 1989 on the co-ordination of certain provisions laid down by Law, Regulation or Administrative Action in Member States concerning the pursuit of television broadcasting activities (O.J. 1989, L 298/23), modified by Directive 97/36 of 30 June 1997 (O.J. 1998, L 6/43); in the field of digital signature service providers, Directive 99/93, cited *supra* note 16; in the field of services of conditional access, Directive 98/84, cited *supra* note 28; or in the field of protection of personal data, Directive 95/46, cited *supra* note 22.

Before it, "Information Society service" had already been defined in Directive 98/34[28] and Directive 98/84.[29] Article 2(a) of Directive 2000/31 refers the definition to those legal texts in order to avoid differing interpretations. An Information Society service is "any service normally provided for remuneration, at a distance, by means of electronic equipment, for the processing and storage of data, and at the individual request of a recipient of the service".[30] The last element of the definition is essential to distinguish this service from other services provided at a distance and by electronic means which are not Information Society services, such as television or radio broadcasting. The definition covers an extremely wide range of economic activities that can take place on-line. These are activities which already exist but which are now being developed on-line, such as the selling of products, the provision of services, marketing and commercial communications; however, other activities are specific to the present Internet world – provision of Internet access, search engines, electronic mails, hosting, access to data – or to a near-future Internet world – video-on-demand, computer networks, applications service providers. It is irrelevant whether the recipients pay in exchange or not. The definition is broad enough for the provisions of the Directive to cover any new service of the Information Society that may appear in the near future.[31] Unlike the other Directives on freedom to provide services, the Directive on electronic commerce covers any kind of activity taking place on the Internet. For this reason it has been affirmed that the Directive is of a horizontal nature. As will be seen, this characteristic has specific consequences for the application of the country of origin principle.

The natural or legal persons providing these services are called "Information Society Service Providers", or simply "service providers". The Directive makes a distinction between "service providers" and "established service providers".[32] While the first concept refers to any natural or legal person providing an Information Society service, the second defines those providing Internet services as an economic activity using a fixed establishment for an indefinite period.[33] Only this category is bound by and benefits from the

28. Directive 98/34 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services (O.J. 1998, L 204/37), amended by Directive 98/48/EC (O.J. 1998, L 217/18).

29. Directive 98/84 on the legal protection of services based on, or consisting of, conditional access, O.J. 1998, L 320/54.

30. Recital 17.

31. E.g. think of the convergence between the Internet and mobile phone thanks to the WAP (wireless application protocol) technology.

32. See Art. 2(b) and (c).

33. For instance, a person who has a website where he exhibits his drawings and poems is a "service provider" in the sense of letter b), the owner of the server where the website of that person is hosted is an "established service provider".

provisions of the Directive.[34] A service provider is established where it is geographically located and where it actually pursues an economic activity for an indefinite period.[35] Although it might seem a little strange, the location of the technical means required to provide the service, or the location of the computer where the information is stored is irrelevant. It cannot be otherwise: the Directive would be easily avoidable as providers would choose to place their websites in computers located in countries with very permissive rules.[36] In cases where a service provider has several places of business in the Community, the ECJ has clarified in the field of TV broadcasting, the Member States with supervisory powers shall be the one where this organization has the "centre of the activities" of the service concerned.[37] The determination of this has many legal implications: first, because the Directive only applies to Information Society services provided by persons established in the European Community; second because it determines what national provisions a provider must comply with in accordance with the country of origin principle of Article 3(1); finally, insofar as the domicile or residence of a person is used as a connecting factor for determining the jurisdiction of a court or the law applicable to a cross-border situation.[38]

2.2. *The Country of Origin principle and its relation with Private International Law Rules*

The country of origin of the Information Society service can only be determined once the service provider's place of establishment has been located. According to Article 3(1), every Member State shall ensure that services provided by persons established on its territory comply with national legal requirements falling within the "co-ordinated field" of the Directive. The co-ordinated field covers *every* legal requirement applicable to *any* of the services provided on the Internet, regardless of whether they are of a general nature or specifically designed for Internet services. It is not limited to those aspects covered by the Directive, but extends to all the legal requirements applicable to the specific activity. According to the definition in Article 2(h), those

34. See Recital 18.

35. Case C-221/89 [1991] ECR I-3905, at 20.

36. As such, services provided by European companies through an access provider located in Israel are subject to the provisions of the Directive. An American company providing its services in Europe through a provider located in Spain, might be subject to different requirements from those of the Directive.

37. Case C-56/96, [1997] ECR I-3134.

38. See e.g. Art. 2 of the Brussels Convention of 1968 on jurisdiction and the enforcement of judgments in civil and commercial matters (O.J. 1998, L 27/1.) or Art. 4(2) of the Rome Convention on the law applicable to contractual obligations (O.J. 1998, C 27/34).

requirements refer to the taking up of the activity – qualifications, authorizations or notifications – and the pursuit of the activity, i.e. requirements concerning behaviour of the service providers, requirements regarding the quality or content of the service including those applicable to advertising and contracts, or requirements concerning the liability of the service provider. As such it covers every field of law regardless of the public or private nature of the norms.[39]

Service providers complying with the legal requirements of their Member State of establishment can provide Information Society services to citizens located in any EC country. It is for the competent authorities of the country of origin to monitor the legality of those services. According to Article 3(2), Member States cannot restrict those services for reasons falling within the co-ordinated field. Pursuant to the principle of mutual recognition, they are obliged to trust in the diligence of the country of origin's competent authorities and therefore to recognize those services.[40] By definition, Information society services governed by the Directive are cross-border, thus the law governing these services must be determined by the conflict of law rules of the State concerned. As will be analysed below, this implies that restrictive measures may not come from the law of the State of destination but from another State's law.[41] Taking into consideration the ECJ case law on freedom to provide services, it must be understood that this prohibition is absolute: it covers any restrictive measure, regardless of its discriminatory or non-discriminatory nature.[42]

The establishment of a co-ordinated field of such a vast scope was a choice of the Commission that was respected by the Council and the Parliament. As such, every legal requirement of the service would be supervised by the country of origin so providers would provide their service in other Member States under the same conditions as in their home country.[43] No room is left for the State of destination to control the provision of the service. This approach is consistent with the ECJ interpretation of freedom to provide services in *Alpine Investments*.[44] In that case, the Court was faced with the problem of

39. See Crabit, op. cit. *supra* note 12, 766.

40. On the mutual recognition "rule" in general, see Gardeñes Santiago, *La aplicación de la regla de reconocimiento mutuo y su incidencia en el comercio de mercancías y servicios en el ámbito comunitario e internacional* (Madrid, Eurolex, 1999).

41. See *infra*, remainder of this subsection.

42. Case 205/84, *Commission* v. *Germany*, [1986] ECR 3793; Case C-76/90, *Dennemeyer*, [1990] ECR I-4239; Case C-154/89, *Commission* v. *France*, [1991] ECR 682; Case C-180/89, *Commission* v. *Italy*, [1991], I-718; Case C-198/89, *Commission* v. *Greece*, [1991] 735; Case C-384/93, *Alpine Investments*, [1995] ECR I-1167; Case C-3/95, *Reiseburo Broede*, [1996] ECR I-6511; Case C-272/94, *Guiot*, [1994] ECR I-1915.

43. See Crabit, op. cit. *supra* note 12, 767–768.

44. *Alpine Investments*, cited *supra* note 42.

whether to extend the *Keck* doctrine on free movement of goods to this field or not. According to the *Keck* doctrine, provisions restricting or prohibiting certain selling arrangements are not such as to hinder directly or indirectly, actually or potentially, trade between Member States so long as they are not shown to be discriminatory.[45] However, in *Alpine Investments* the Court considered this doctrine was not applicable to services. In the field of services, such a provision directly affects access to the market in other Member States and is thus capable of hindering intra-Community trade.[46] In the opinion of Hatzopoulos, this decision shows that a distinction between selling arrangements and all other measures is "wholly inappropriate for ensuring the free provision of services", insofar as services are by essence immaterial and their quality does not rely on its intrinsic characteristics but directly depends on the conditions under which they are delivered.[47] For Information Society services, those conditions include the selling arrangements of a service and any other aspects covered by the co-ordinated field of the Directive. None of them can be treated separately. States of destination must refrain from imposing any kind of measure on these services which would restrict their provision. However, it remains, as in any other case of freedom to provide service, possible for Member States to derogate from this principle on the grounds of the public policy clause of Article 46 EC, though, as will be analysed below, application of this clause is subject to the strict rules of Articles 3(4), (5) and (6).

Although the wording of Article 3 was supported by the ECJ case law on freedom to provide services, the initial Commission proposal attracted much discussion, which led to the introduction of several additional Paragraphs. The reason was that, unlike other legal instruments on freedom to provide services, the Directive on electronic commerce is horizontal in nature: it applies to any service that can be provided on-line. Taking this fact in conjunction with the vast scope of the co-ordinated field, the consequences of such an instrument would be enormous:[48] Member States would be forced to recognize the provision of any Information Society service coming from other Member States regardless of the legal implications deriving from it. However, the degree of integration among the Member States' legislations is not such as to enable the country of origin principle to apply generally: certain fields of

45. Joined Cases C-267/91 and 268/91, *Keck and Mithouard*, [1993] ECR I-6097, para 16.

46. Para 38. See also Cases C-34–36/95, *Konsumentombudsmannen* v. *De Agostini and others*, [1997] ECR I-3843, paras. 41–44.

47. Hatzopoulos, "Recent developments of the case law of the ECJ in the field of services", 37 CML Rev. (2000), 68.

48. According to Crabit, the Directive provides "une approche transversale en trois dimensions". Those dimensions are: the horizontal nature of the Directive, the omni-comprehensive co-ordinated field, and the regulation of all the different steps of the economic activity of the Information Society service. See Crabit, op. cit. *supra* note 12, 764 and following.

law were exempted from its application. They are included in the Annex, and Article 3(3) excludes the application of paragraphs 1 and 2 to them. The reasons reside in the impossibility to apply, in those fields, the principle of mutual recognition as set out in the ECJ case law, or in the lack of sufficient harmonization to guarantee an equivalent level of protection between Member States, or in the incompatibility with Article 3 of certain existing Directives which explicitly require supervision in the country of destination.[49]

The Annex certainly includes very important areas of law, such as intellectual and industrial property,[50] the activities of financial institutions and the issue of electronic money,[51] and the insurance sector.[52] It also includes contractual obligations concerning consumer contracts. There are already a large number of directives in this field, which have established a minimum level of consumer protection.[53] These instruments always permit Member States to adopt stricter measures in favour of consumers.[54] By definition, application of the country of origin principle is incompatible with these Directives. Finally, particular questions are listed in the Annex whose inclusion, we believe, could have been avoided or which should have been mentioned elsewhere.[55] It must be made clear that exclusion of these areas of law from the application of Article 3(1) and (2) only means that States of destination can restrict the provision of the Information Society services. The remaining provisions in the Directive are applicable in those fields – this includes, for instance, questions on the validity of consumer contracts concluded on-line, or on the liability of service providers for dissemination of contents protected under intellectual property laws.

49. See Commission Proposal, p. 32.

50. In the case of copyright and related rights, adaptation of the existing framework to the Information society has been attained in Directive 2001/29, cited *supra* note 15. It provides a harmonized solution for the adaptation and supplementation of Member States legislations so as to respond adequately to the new forms of exploitation of works of art (see Recital 5).

51. Directive 2000/46 of the European Parliament and of the Council of 18 Sept. 2000 on the taking up, pursuit and prudential supervision of the business of electronic money institutions. (O.J. 2000, L 275/39) in respect of Member States which have applied the exemptions established in Art. 8(1) of this Directive.

52. Art. 30 and Title IV of Directive 92/49/EEC (O.J. 1992, L 228/1. Last amended by Directive 95/26/EC), Title IV of Directive 92/96/EEC (O.J. 1992, L 360/1. Last amended by Directive 95/26/EC), Arts. 7 and 8 of Directive 88/357/EEC (O.J. 1988, L 172/1. Last amended by Directive 92/49/EC), and Art. 4 of Directive 90/619/EEC (O.J. 1990, L 330/50. Last amended by Directive 92/96/EC).

53. They are listed in Recital 11.

54. See Art. 6 Directive 93/13, Art. 12 Directive 97/7 and Art. 8 of Directive 99/44.

55. E.g.: freedom of the parties to choose the applicable law to their contract – in our opinion, unnecessary insofar as the Directive does not aim to modify existing rules of Private International Law (Art. 1 (4)); formal validity of contracts in real estate; the permissibility of unsolicited commercial communications by e-mail – this should have been mentioned in the precise provision dealing with these communications.

Even if the scope of application of the country of origin principle is delimited by Article 3(3), it still plays an important role insofar as the Directive applies to any kind of service provided on-line. Those services might have been the object of specific directives harmonizing the legal requirements on access to and exercise of certain professional activities in the European Community or not. In the first case, Directive 2000/31 does not substitute but complements those Directives. In the second, Member States are obliged to recognize those services as they are provided in their country of origin. Restriction of such services would contravene not only Article 3(2) of the Directive, but also Article 49 EC, which is directly applicable since the end of the transitional period.[56] There are, however, exceptional cases in which restrictive measures to the provision of Information Society services are permitted. They are listed in Article 3(4). This provision regulates the application of the general public policy clause in the field of electronic commerce by national authorities, including civil courts dealing with private law disputes.[57] Due to the vast scope of application of the Directive and the open nature of this clause – its content changes with time and from one country to another[58] – this ground might be invoked by Member States abusively and, consequently, the consolidation of the Single online market would be hindered. To avoid that, strict terms on which the clause can be invoked were established in the Directive. Paragraphs 4, 5 and 6 of Article 3 reflect the extensive ECJ case law on the application of the public policy clause and the mutual recognition principle in the field of services. First of all, restrictive measures must be justified by the need to protect one of the following objectives considered as fundamental in society:[59]

– public policy, in particular the prevention, investigation, detection and prosecution of criminal offences, including the protection of minors and the fight against any incitement to hatred on grounds of race, sex, religion or nationality, and violations of human dignity concerning individual persons;
– the protection of public health;
– public security, including the safeguarding of national security and defence;
– or the protection of consumers, including investors.

The measure may not have a general character, but must be taken in relation to a given Information Society service which prejudices one of the abovementioned objectives. It should be taken if the objective is in danger or when

56. Case 33/74, *Van Binsbergen*, [1974] ECR 1299 and Joined Cases 110 & 111/78, *Ministère Public and ASBL* v. *Van Wesemael*, [1979] ECR 35.

57. Recital 25.

58. Case 41/74, *van Duyn*, [1974] ECR 1337, para 18.

59. Cases 115, 116/81, *Adoui and Cornuaille*, [1982] ECR 1665, at 8.

there is a serious risk of prejudice.[60] The measure shall be proportionate to the objectives impaired[61] and, though it is not mentioned in the text, it shall respect the human rights of the parties concerned.[62] Also, other principles protected by the ECJ should be applied to determine the validity of the measure: it must be a measure in an area that has not already been harmonized at a Community level,[63] it may not be discriminatory to non-nationals,[64] and it may not entail a double control.[65] For instance, under this provision France is authorized to prohibit websites offering products or services promoting nazi paraphernalia such as the one that gave rise to the famous *Yahoo! Case*.[66]

On the adoption of the restrictive measure, the procedure of Article 3(4)(b), 3(5) and 3(6) must be followed. Member States authorities are required to ask the country of origin to take the appropriate measure against service providers established in their territory, and if they do not do so, or the measure is inadequate, they must notify the Commission of their intention to take their own measure. In the event of emergency, measures can be taken in advance, but they should be notified later to the Member State concerned and to the Commission, indicating the reasons why there was an emergency. The Commission decides whether the measure is compatible with Community Law and whether the Member State is allowed to continue with the measure or not.

Another legal problem around Article 3 during the adoption procedure was the relation between the country of origin principle and Private International Law rules – hereinafter referred to as PIL rules. These rules apply as soon as a cross-border relationship is at stake. As has been mentioned, by definition, Directive 2000/31 applies to Information Society services provided from one Member State to another, thus in cross-border situations. *Grosso modo*, continental lawyers conceive Private International Law as an area of law

60. Case 36/75, *Rutili*, [1975] ECR 1219, para 28, Case 30/77, *Bouchereau*, [1977] ECR 2013, para 35.

61. Case 352/85, *Bond van Adverteerders*, [1985] ECR 2124, para 36. Case C-260/89, ERT, [1989] ECR 2951, para 24.

62. Case 260/89, *ERT*, [1991] ECR 2951; Case C-159/90, *The Society for the Protection of Unborn Children Ireland Ltd* v. *Stephen Grogan*, [1990] ECR 4733, para 31, and Case C-177/94, *Perfili*, [1994] ECR I-161, para 20.

63. Case 815/79, *Cremonini* v. *Vrankovic*, [1979] ECR 3607, para 6.

64. *Dennemeyer*, para 15.

65. Case C-55/94, *Gebhard*, [1995] ECR I-4165, para 38. Meaning that the State of destination must verify that the general interest the measure tries to safeguard is not already safeguarded by a measure taken in the country of origin. See Martín y Pérez de Nanclares, "El derecho de establecimiento", in Lopez Escudero and Martín y Perez (Eds.), *Derecho Comunitario material* (MacGrawHill, Madrid, 2000), p. 117.

66. See Ordonnances de référé du Tribunal de Grande Instance de Paris de 22 mai 2000, 11 Aug. 2000 and 20 Nov. 2000, *UEJF et Licra c/ Yahoo! Inc.* Available at http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.htm

dealing with three topics; these can be represented by three questions whose answers are given by three kind of rules:
– which State's courts have jurisdiction when a dispute arises in a cross-border relationship? These are rules on jurisdiction;
– which law is applicable to the dispute? These are conflict of laws rules;
– how can a foreign decision be enforced in a given State? These are rules on recognition and enforcement of foreign decisions.[67]

Many people have assumed that Article 3(1) establishes the law of origin as the conflict of law rule applicable to e-commerce, meaning that any relationship taking place over the Internet would be governed by the law of the State where the service provider is established.[68] In our opinion, this is a misconception of the Directive. Article 1(4) and Recital 23 clearly state that it is not the purpose of the Directive to establish additional rules on private international law. Cross-border relationships on electronic commerce are governed by existing PIL rules either at Community level or national level. However, the relation of these rules with the country of origin principle is certainly complicated and it may entail various legal implications, because of the broad scope of the co-ordinated field and the horizontal nature of the Directive.

First of all, the Directive does not have any provision on jurisdiction: the country of origin principle does not confer jurisdiction over any question arising from the provision of an Information Society service to the courts of the State of origin. In the event a dispute arises in an international relationship on the Internet, as far as it relates to patrimonial matters, the Brussels Convention on jurisdiction and enforcement of judgments in civil and commercial matters will determine which courts have jurisdiction over the dispute.[69] As the Brussels Convention governs a different issue – jurisdiction of the courts –

67. See e.g. Fernandez Rozas and Sanchez Lorenzo, *Derecho internacional privado* (Madrid, Civitas, 1999), pp. 43–46; Audit, *Droit international privé*, 3rd ed. (Economica, Paris, 2000), pp. 4–15. Also, in the Common Law literature, North and Fawcett, *Chesire and North's Private international law*, 13th. ed. (Butterworth, London, 1999), pp. 7–8.

68. See e.g. Julia Barcelo et al., "La Proposition de Directive Europeénne sur le commerce electronique: questions choisies", in *Commerce Electronique: les temps des certitudes* (Bruylant, Bruxelles, 2000), p. 29, or Palacio Vallelerdundi, "Le commerce électronique, le juge, le consommateur, l'entreprise et le Marché intérieur: nouvelle équation pour le droit communautaire", (2001) *Revue du Droit de l'Union Européenne*, p. 8; also Crabit, op. cit. *supra* note 12, 759–762, 798–807.

69. See consolidated version in O.J. 1998, C 27/1. The Convention will be substituted from March 2002 by the already adopted Regulation 44/2001 on jurisdiction, recognition and enforcement of judgments in civil and commercial matters (O.J. 2001, L 12/1). Art. 1 in both texts states: "This Convention/Regulation shall apply in civil and commercial matters whatever the nature of the court or tribunal. It shall not extend, in particular, to revenue, customs or administrative matters. The Convention shall not apply to: 1. the status or legal capacity of natural persons, rights in property arising out of a matrimonial relationship, wills and succession; 2. bankruptcy, proceedings relating to the winding-up of insolvent companies

from that of Article 3 of the Electronic commerce Directive – applicable law – they cannot conflict.

That is not the case with conflict of law rules. On the determination of the law applicable to a cross-border situation, Article 3 and conflict of law rules certainly may conflict. Electronic commerce cross-border situations may be of two kinds: contractual obligations (e.g. a contractual relationship to receive Information Society services such as electronic access to a data base, a contract concluded in a web-site to acquire goods); or non-contractual obligations (e.g. liability arising from infringement of intellectual property rights by a website owner, liability arising from defamations, liability for spreading a virus through Internet, misleading advertising, passing off, processing of personal data, etc).

In the first case, there is a Community instrument – the Rome Convention[70] – which must be applied by judges of every Member State in order to determine the law applicable. It basically establishes that the parties can choose the law applicable to the contract[71] and, in the absence of a choice, the law of the country most closely connected will govern the contract.[72] There is a presumption that that law is the one of the country where the person who performs the characteristic obligation is established.[73] However, the application of those laws cannot prevent the courts from applying the mandatory rules of their national laws.[74] That is to say rules from which there can be no contractual derogation insofar as they safeguard a general interest. In the case of consumer contracts, the law chosen by the parties will apply as far as it does not provide a lower level of protection than that provided by the consumer's residence State law.[75] In the absence of choice, the law of the consumer's State of residence shall be considered as the law most closely connected to the contract.[76]

or other legal persons. judicial arrangements, compositions and analogous proceedings; 3. social security; 4. arbitration". For a general overview of the application of these instruments to Internet see Katz, "Jurisdiction and E-Commerce Disputes", 3 *Journal of World Intellectual Property* (2000), 289–307.

70. Rome Convention of 1980 on the law applicable to contractual obligations, O.J. 1998, C 27/34. For further information on the Rome Convention see Lagarde, "Le nouveau droit international privé des contrats aprés l'entrée en vigueur de la Convention de Rome du 19 juin 1980", (1991) *Revue Critique de Droit international privé* (hereafter: Rev. crit. d.i.p.), 287–340 and Giuliano and Lagarde, *Report on the Convention on the Law Applicable to Contractual Obligations* in O.J. 1980, C 282/1–50.

71. Art. 3.

72. Art. 4 (1).

73. Art. 4 (2).

74. Art. 7(2).

75. Art. 5(2).

76. Art. 5(3). There is a Proposal of the European Working Group of Private International Law recommending the amendment of Arts. 5 and 7 of the Convention to promote a proper

In the second case, there is no Community instrument yet. At present, in order to determine the law applicable to a non-contractual cross-border situation, Member States courts apply the conflict of law rules of their national systems or those international conventions ratified by their Parliaments. Due to the broad variety of factual situations which can give rise to a non-contractual obligation, those rules are numerous and divergent. The European Commission is working on a Proposal for a Rome II Regulation to give uniform conflict of law rules applicable to non-contractual matters in the EC. However, there are many interests at stake and discussions are delaying the issue of a Green Paper on the subject. In fact, most problems arise from the application of those rules to electronic commerce. Therefore, national conflict of law rules of the Member State will continue to apply for some time.

If we take a look at the co-ordinated field of Directive 2000/31, it may be observed that, according to Article 3, aspects such as "requirements applicable to contracts" or "requirements concerning the liability of service providers" are subject to the country of origin principle. Thus, at first sight, this principle appears to apply to aspects of both contractual and non-contractual obligations. But, at the same, time, Article 1(4) states that the Directive does not establish additional PIL rules. Are these provisions compatible? In our opinion, they are, because the country of origin principle is not a conflict of law rule. It is an imperative rule of Community law imposing an obligation on the Member States.[77] That is to say, it does not impose the law of origin as the law applicable to electronic commerce. Otherwise, it would create a different legal treatment of on-line legal situations from that provided for off-line situations. The Rome Convention would apply to traditional commerce but not to electronic commerce. Another reason for this assertion is that the law of origin does not need to be applied to electronic commerce because it is not needed for the purpose of the Directive. Most of the aspects covered by the *lex contractus*[78] and the law applicable to the non-contractual obliga-

functioning of the Internal market to the detriment of other public policy interests. See the text of the Proposal at (2000) Rev. crit. d.i.p., 929–933; also Quiñones Escamez, "Globalización, regionalización y nuevas tecnologías en el DIP de los contratos de consumo (mercado interior y Convenio de Roma)", *XIX Jornadas de la Asociación Española de Profesores de Derecho internacional*, available at www.jornadas-aepdiri.com (last visited, October 2001).

77. In this sense, Desantes Real, op cit. *supra* note 18, 335–336 and also Crabit, op. cit. *supra* note 12, 801, although the latter reaches a different conclusion. We accept that he makes an excellent argument to defend his point of view, though we understand the Community mandatory rule of the country of origin principle in a different way.

78. Art. 10 of the Rome Convention establishes as the scope of the applicable law: "(1) The law applicable to a contract by virtue of Articles 3 to 6 and 12 of this Convention shall govern in particular:
(a) interpretation;
(b) performance;
(c) within the limits of the powers conferred on the court by its procedural law, the consequences

tion[79] do not affect the provision of Information Society services. Finally, application of the law of origin to non-contractual aspects of electronic commerce is incompatible with the principles informing the regulation of cross-border non-contractual situations: protection of the affected market, protection of the victims, protection of the general interest, etc.

Article 3(1) and 3(2) must be read in conjunction in order to understand the mandatory rule of Community law imposed on the Member States. According to the latter, States of destination are obliged not to restrict Information Society services coming from other Member States. They are obliged to admit such services under the mutual recognition principle. This obligation is justified by the fact that the provision of the service is lawful to the extent it has been authorized in the country of origin or is in accordance with the law of that country. This does not imply that any contractual or non-contractual relation deriving from the provision of the service is governed by the law of origin. The legal regime applicable to such service is determined by the PIL rules of the State concerned, however if that legal regime includes a rule that restricts the provision of the service, a court is obliged to refrain from applying it and to apply the country of origin rule instead. The Member State is not oblige to disregard the law applicable as a whole in favour of the law of origin, but only the concrete norm restricting the provision of the service.[80] For the other aspects of the Information Society service, the former law continues to apply. That is also so when the judge applies a mandatory rule under Article 7 of the Rome Convention. Competent authorities may only derogate from this principle where the restrictive measure is grounded in one of the objectives of Article 3(4), as will be the case with many, but not all, mandatory rules.[81]

In practice, for contractual obligations, Article 3(2) should not apply very often insofar as the law of the contract will usually coincide with the law of the country of origin. That is because the Rome Convention allows the choice of the applicable law – standard terms of electronic contracts often establish the law of the service provider's establishment as the law applicable to the

of breach, including the assessment of damages in so far as it is governed by rules of law;
(d) the various ways of extinguishing obligations, and prescription and limitation of actions;
(e) the consequences of nullity of the contract.
(2) In relation to the manner of performance and the steps to be taken in the event of defective performance regard shall be had to the law of the country in which performance takes place."

79. The scope of the norm depends on the particular non-contractual obligation at stake: existence of the harm, type of liability, limits, legitimate persons to receive compensation, etc., see Fernandez Rozas and Sanchez Lorenzo, op. cit. *supra* note 67, p. 567.

80. Case C-126/1991, *Yves Rocher*, [1991] ECR I-2361.

81. Joined Cases C-396/96 and C-397/96, *Arblade*, [1999] ECR 8498. The Court held that "the fact that national rules are categorised as public-order legislation does not mean that they are exempt from compliance with the provisions of the Treaty; if it did, the primacy and uniform application of Community law would be undermined". See paras. 31–39. See also note by Fallon in (2000) Rev. crit. d.i.p., 728–737.

contract –, and because in the absence of a choice the country most closely connected is that where the service provider is established – the provider implements the characteristic performance of the contract, thus the law of his State of residence applies under Article 4(2). This will not be the case for consumer contracts or when mandatory rules from legal systems other than that of the country of origin are applicable on the basis of Article 7. In the first case, it must be recalled that obligations concerning consumer contracts are excluded from Article 3 of the Directive. In the second case, mandatory rules will only apply if they are justified by one of the objectives of Article 3(4), otherwise rules of the country of origin will prevail. Fortunately, thanks to the harmonization in the Directive of certain aspects of electronic contracts, situations in which Article 3(2) will be applicable should become fewer.

For non-contractual matters, the mutual recognition obligation is more likely to provoke legal conflicts. Until recently, it was not thought that regulation of PIL rules on these matters needed to take into consideration the possibility of hampering the freedoms. Adoption of these rules was inspired by other general interests. It was not conceived that they might hinder the completion of the Internal market, since it was considered that non-contractual rules do not affect the content of such services and do not stop a person from providing it.[82] However, at present many Information Society services are affected by these rules: if someone administers or hosts services (e.g. websites or usenet groups) in which a variety of information can be stored, such information may infringe rules on Intellectual property, law of defamation, or even criminal law. Although the Directive harmonizes certain aspects on the liability of service providers, the rest remains subject to the laws of the Member States.[83] As has been said, conflict of law rules on non-contractual matters are various and lead to varying solutions. In some situations, the law applicable to the dispute will be that of the country where the "victim" resides; in others, the law of the country where the harmful event occurred; in others, the law of the country where the effects of the harmful event were felt; and, finally, in some situations the victim or the competent authority may choose between different options.[84] Insofar as websites are accessible from any place in the Community, the rule applicable may be any of several. Since the law applicable to the dispute will seldom coincide with that of the country

82. Radicati di Brozolo, "L'influence sur les conflits de lois des principes de droit communautaire en matière de liberté de circulation", (1993) Rev. crit. d.i.p., 419–421.

83. See Chapter V.

84. For further explanation, see Boele-Woelki and Kessedjian (Eds.), *Internet. Which court decides? Which law applies? Quel tribunal décide? Quel droit s'applique?* (Kluwer Law International, The Hague, 1998); Carrascosa Gonzalez and Calvo Caravaca, *Conflictos de leyes y conflictos de jurisdicción en Internet* (Colex, Madrid, 2001); de Miguel Asensio, *Derecho privado de Internet*, 2nd ed. (Civitas, Madrid, 2001), pp. 171–177, 278–283, 505–513.

of origin, it is more likely that Article 3(2) of the Directive on electronic commerce will apply, thus Member States should refrain from applying those non-contractual rules restricting the provision of the service. Only if those rules are justified under one of the objectives of Article 3(4) will they remain applicable.

Although the obligation imposed in Article 3(2) clearly benefits the pursuing of Information Society services, it does not remove the legal uncertainty service providers are subject to in the field of non-contractual obligations. They can be sued in the courts of any Member State under the terms of the Brussels Convention and the Brussels Regulation – according to the interpretation of the ECJ, Article 5(3) grants jurisdiction to the Courts of the different places where the harmful event occurred or to the courts of the place of the event giving rise to it.[85] The conflict of law rules for non-contractual matters may lead to different solutions depending on where the complaint was brought. Although Article 3(2) obliges Member States not to restrict the provision of the service, the possibility of justifying the measures under Article 3(4) is always present. The enactment of a body of uniform rules on conflict of law for non-contractual matters will reduce such legal uncertainty. A Rome II Regulation will benefit the functioning of the Internal Market and will avoid so-called "forum-shopping": in those situations where many countries have potential jurisdiction, the plaintiff sues the defendant in the State whose conflict of law rules and national laws benefit him the most. As with the Rome Convention, service providers will know what conflict of law rules are applicable to non-contractual matters, regardless of the country where they are sued. However, there should be a careful examination of what principle(s) and objective(s) should inspire such a body of uniform rules. Certainly, application of the law of origin of the service will benefit the completion of the single online market. However, rules on non-contractual obligations also aim to promote other objectives. These objectives are not uniform for all the fields of non-contractual obligations and many of them are incompatible with the free movement of services – for instance, protection of consumers against misleading advertising or protection of the victim of an act of defamation. The appropriate solution would be one combining both objectives, but this is extremely difficult to attain. Furthermore, another aspect making the adoption of the Rome II Regulation even more difficult is the need to decide whether it will be an instrument of a universal character – like the Rome Convention – or one whose scope is limited to intra-Community relationships. In the first case, the need to respect internal market principles is weaker, insofar as it

85. Case 21/76, *Mines de Potasse d'Alsace*, [1976] ECR 1735, and Case C-68/93, *Fiona Shevill* v. *Press Alliance*, [1995] ECR I-415.

does not only apply in an Internal Market but also in other situations where there is no obligation to protect a freedom of movement.

2.3. *Principle excluding prior authorization*

According to Article 4, Member States must refrain from making the provision of an Information society service subject to prior authorization or to any other requirement having a similar effect. This provision concerns the freedom of establishment as a prerequisite for the provision of Information Society services. It aims to facilitate access to the supply of services in the Internet by removing any formality which may obstruct the freedom of establishment of service providers in any Member State. As the Commission Proposal states, it establishes a sort of "right to a site" which can be exercised by any operator, company or self-employed person deciding to use the Internet to provide a service.[86] The provision does not prevent Member States from establishing registers for service providers, but this should not be subject to any condition that would obstruct the provision of the service. In this sense, registers might be established for the sole purpose of publicity.[87]

However, as has already been mentioned, there is a wide range of activities that can be provided by electronic means. Some of those activities which are not specifically targeted at services provided on-line, may be subject to authorization or legal requirements. For example, if legislation requires professional qualifications or authorization by a professional body, it will continue to apply in full to any operator wishing to carry on such activities on-line.[88] In Spain, distance-selling retailers are obliged to register at a Public Registry[89] prior to exercising their commercial activities. Registering will still be required if they provide their services over the Internet. In particular, Article 4(2) mentions the licence authorization regime established by Directive 97/13[90] in the field of electronic communications.[91]

86. P. 22.

87. That is the case of Art. 10 of the Proposal for a Law on electronic commerce in Spain, see latest text of 30 April 2001. Available at http://www.sgc.mfom.es/.

88. See Commission Proposal, p. 22.

89. See Real Decreto 1133/1997, de 11 Julio implementing Art. 38.2 de la Ley 7/1996 sobre el comercio minorista, BOE n° 117, de 25 de julio de 1997.

90. O.J. 1997, L 117/15.

91. An important package of Directives has been proposed by the Commission in order to modify the complete regulatory framework of the newly called "electronic communications". See Doc COM(2000) 384 final, 385 final, 385 final, 392 final, 393 final, 394 final of 12 July 2000, O.J. 2000, C 365 E.

2.4. *Transparency obligation*

Although setting up an Information Society service is not subject to prior authorization, Article 5 imposes a transparency obligation on service providers. Paragraph 1 establishes a list of minimum information they have to make accessible to the general public about themselves and their activities. Such information includes:
– the name of the service provider;
– the geographical 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 corresponding VAT identification number.

In addition, according to Article 5(2), where Information Society services refer to prices, they must be clearly and unambiguously indicated, and it must be made clear whether they are inclusive of tax and delivery costs.

Imposition of such a burdensome transparency regime on service providers is justified by reason of the specific nature of the media through which they develop their activities. Because of the global nature of Internet, a recipient of a service can be dealing with a service provider established in an unexpected country, whose regulation concerning the service can be completely unknown. Furthermore, providers may abuse the possibility of hiding their identity and geographical location to defraud consumers or to commit other unlawful activities. The requirements of Article 5 concerning geographical locations and professional qualifications of service providers are essential in order to ensure transparency and consumers' confidence in the on-line service.[92] Another reason for such obligations is that, in comparison with other media, Internet provides an easy way to render the information required by Article 5 "easily, directly and permanently accessible": it should be enough to provide

92. Julia Barcelo et al., op. cit. *supra* note 68, p. 6.

a "link" in the website to access a specific page where all the information is displayed.

For many service providers the information requirements are higher. As was said above, Directive 2000/31 complements existing legislation. Therefore, depending on the activity they develop, service providers must comply with additional Community and/or national legislation. That is the case for service providers concluding consumer contracts at a distance covered by Directive 97/7 and the Amended Proposal for a Directive concerning the distance marketing of consumer financial services.[93] They apply to "contracts concerning goods or services concluded between a supplier and a consumer under an organized distance sales or service-provision scheme run by the supplier, who, for the purpose of the contract, makes exclusive use of one or more means of distance communication up to and including the moment at which the contract is concluded".[94] Therefore, when contracts are concluded with merchants, general information under Article 5 must be provided. When they are concluded with consumers,[95] such information must be complemented with that required under Article 4 of Directive 97/7 and Articles 3 and 3A of the Amended Proposal for a Directive on the distance marketing of consumer financial services.

3. The promotion of Information Society services

Once a service provider is established in a Member State, complies with the general requirements for the pursuit of the service concerned and makes accessible on his website the information required in Article 5, he will promote his Information Society service. As the Internet provides a new mean for doing business, it also requires the implementation of new marketing and advertising techniques inherent to the new medium.[96] The use of commercial communications on Internet is common for profit-seeking service providers. The need to obtain customers leads companies to use very aggressive marketing techniques which can be extremely annoying, and can become a source of fraud for consumers.[97] While there is as yet no instrument at Community

93. Doc. COM(1999) 385 final.
94. See Art. 2(1) both in Directive 97/7 and the Amended Proposal.
95. For the purpose of the Directive 97/7 and the Amended Proposal of Directive, "consumer ... means any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business or profession" (Art. 2(2)).
96. Examples of these new marketing techniques are: hyperlinks, frames, metatags, deep-linking, etc.
97. Anyone with experience of Internet knows how annoying it is when you "surf" in search of a product and several windows – so-called pop-ups – are opened on the screen when you click on a hyperlink.

level governing commercial communications as a whole,[98] at national level there are various regulations covering this matter and different definitions of the concept. Article 7 of the Directive harmonizes the applicable regime to commercial communications in the Internet.

Notwithstanding this, it should be borne in mind that websites are considered as advertising[99] and, as such, they must also comply with existing Directives on the subject.[100] However, the concept of commercial communications is broader than that of advertising in Directive 84/450.[101] In Internet, such commercial communications can be found in websites, bulletin boards, Usenet groups, or they can be sent by e-mail to thousands of recipients without prior demand – so-called spamming. Since the latter receive a different treatment in the Directive they must be studied separately.

3.1. *Commercial communications*

Commercial communications are defined in Article 2(f) as "any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organization or person pursuing a commercial, industrial or craft activity or exercising a regulated profession". Although the provision

98. However, there has been extensive work on the matter by the Commission. Two Green Papers have been adopted: "Commercial communications in the Internal Market" (COM(96) 192 final) and "The follow-up to the Green Paper on Commercial Communications in the Internal Market" (COM(98) 121 final). Recently the Commission has issued a Proposal for a Regulation concerning sales promotions in the Internal Market (Doc COM(2001)546 final) aiming at uniform rules on the use of commercial communications and sale promotions at a Community level and to apply the principle of mutual recognition.

99. In France, it has already been sustained that websites constitute "advertising". See Cour d'appel de Rennes, 1ere Ch. B., Arrêt du 31 mars 2000, Compagnie Financière du Credit Mutuel de Bretagne c. Federation logement consommation et environnement d'Ille-et-Vilaine: "Un site internet est susceptible de constituer un support publicitaire: il permet la communication au public de textes et d'images, destinée éventuellement à présenter au public le consultant des marques des services et des marchandises et à inciter à la conclusion de contrats avec les consommateurs potentiels. Le fait que le site ne puisse être consulté qu'après abonnement, et au choix du site par l'usager d'internet, ne change en rien le caractère publicitaire des annonces qui peuvent y être faites. La situation est exactement identique à celle de l'acheteur d'un journal contenant des publicités. . . "

100. Council Directive 84/450/EEC of 10 Sept. 1984 relating to the approximation of the laws, regulations and administrative provisions of the Member States concerning misleading advertising (O.J. 1984, L 250/17), Directive 97/55/EC of European Parliament and of the Council of 6 Oct. 1997 amending Directive 84/450/EEC concerning misleading advertising so as to include comparative advertising (O.J. 1997, L 290/18) and Directive 98/6/EC of the European Parliament and of the Council of 16 Feb. 1998 on consumer protection in the indication of the prices of products offered to consumers (O.J. 1998, L 80/27).

101. Art. 2(1) of Dir. 450/85 states: " 'advertising' means the making of a representation in any form in connection with a trade, business, craft or profession in order to promote the supply of goods or services, including immovable property, rights and obligations."

lays down certain situations which are excluded from the concept,[102] it is a very broad concept including advertising and any kind of communication aiming to promote a product or service. Although the boundary is not always very clear, in principle information whose sole purpose is to provide objective information about a product or service will not qualify as commercial communication.

By giving such a broad definition, two objectives are sought: first, to be technology-neutral, so that any commercial communication, regardless of the communication media, is subject to the requirements of the Directive; second, to broaden the situations in which transparency and loyalty obligation are applicable, so as to enhance consumer protection.[103]

One of the objectives pursued by legislation on this issue is to safeguard the "legitimate expectations of an average consumer who is reasonably observant and circumspect".[104] In order to achieve this objective in an Internet world, stricter requirements than those in older Directives on advertising are imposed. That is because Internet provides consumers with a new way of shopping. Web navigation is more that visiting a single website, because it is usual to click on hyperlinks guiding you to other sites belonging to other providers established in different countries. Meanwhile, new windows may automatically open on the screen to offer you additional products or services related to the one initially searching for. This implies an increase in the risk of confusion for inexperienced consumers on the nature of the information and on the person announcing it. Also, it must be recalled that the characteristics of the medium make it easier to provide such information thus the burden imposed on service providers is not disproportionate.

First, Article 6(a) and (b) require the commercial communication and the person on whose behalf it is made to be clearly identifiable. The provision aims to enable recipients to distinguish commercial communications from other type of information that can be accessed or transmitted in websites, bulletin board, e-mails, or Usenet groups. Also, since commercial communications can be placed in websites owned by others – for example, with the use of banners –, it should be made clear who is advertising the product or service. In such a manner, the risk of confusion for the "reasonably observant and circumspect" consumer decreases. It is not clear how this identification should be made in practice: some authors consider that it can take several forms depending on the Internet application. For instance, they propose that

102. "information allowing direct access to the activity of the company, organization or person, in particular, a domain name or an e-mail address; or communications relating to the goods, services or image of the company, organization or person that are compiled in an independent manner, particularly when this is without financial consideration".

103. Julia Barcelo et al., op. cit. *supra* note 68, p. 8.

104. See Case C-220/98, *Estée Lauder* v. *Lancaster Group*, [2000] ECR I-117.

website owners include all commercial communications in a specific place entitled "Advertising".[105]

Second, there is a transparency obligation when the commercial communication consists of promotional offers, such as discounts, premiums and gifts, or promotional competitions or games. According to Article 6(c) and (d), conditions to qualify for the former or to participate in the latter must be made easily accessible and be presented clearly and unambiguously. Again, it suffices to include a hyperlink in the commercial communication leading to a web page displaying these conditions.

In application of the country of origin principle, it is enough for the validity of these communications if they are authorized in the State of establishment of the service provider. Thus, certain States who do not favour certain kinds of promotions will be forced to recognize their validity when they come from other Member States. However, one needs to assess the impact of the ECJ case law in the Television Broadcasting sector enabling Member States to take, on the grounds of public policy, measures against Internet advertisers. The Court held that such measures are only justified if they are proportionate and necessary to achieve mandatory requirements of public interest – and that could be transferred to Article 3(4) of the ecommerce Directive.[106] Assuming such case law applies in the Internet, those measures should focus on the commercial communications themselves and should not prevent the provision of an Information Society service as a whole.

Another troublesome aspect of the regulation of commercial communications in Directive 2000/31 may arise from its incompatibility with the Directive on Misleading Advertising insofar as the latter is a measure of minimum harmonization.[107] In order to decide whether advertising is misleading, national courts are permitted to set a higher level of protection than that provided for in the Directive. Therefore control of advertising lies on the courts of the country of destination while Article 6 of Directive 2000/31 is governed by the country of origin principle.[108] Two interpretations are possible: either the provisions complement each other in such a way that compliance with Article 6 does not preclude courts from deciding on the misleading nature of commercial communications; or Directive 2000/31 derogates from Directive 89/552. Taking into account the vast scope of the co-ordinated field

105. Julia Barcelo et al., op. cit. *supra* note 68, p. 9.

106. *De Agostini*, *supra* note 46. The case refers to the freedom to provide broadcasting services in the framework of the TV without Frontiers Directive. However, we consider that the same principles are applicable to Information Society services.

107. Art. 7: "This Directive shall not preclude Member States from retaining or adopting provisions with a view to ensuring more extensive protection for consumers, persons carrying on a trade, business, craft or profession, and the general public".

108. Dickie, *Internet and Electronic Commerce Law in the European Union* (Hart Publishing, Oxford-Portland, 1999), pp. 26 and 70.

and its purpose, in our opinion, the second interpretation should prevail. The latest Commission work on the subject seems, indeed, to indicate the adoption of the mutual recognition principle in this field.[109]

Finally, it is regrettable that the Directive 2000/31 does not include a special provision on commercial communications for the protection of minors in the same sense as Article 22 of the Television without Frontiers Directive. That provision bans TV commercials causing moral damage or inciting children, or their parents, to buy products that may cause them physical harm. Since the provision applies exclusively to TV, a new provision including all kinds of commercial communication could be a very useful tool for protecting this vulnerable group of recipients of Information Society services.[110] A recent Commission Proposal for a Regulation on sales promotions includes a provision aimed to protect minors and adolescents in Article 5. However, this problem might find a solution in other instruments of a broader scope already adopted or on which the European Institutions are working. They are intended to combat illegal and harmful content and activities, the so-called "computer-related crimes": privacy offences, content-related offences, Intellectual Property offences.[111] Among the different measures to restrict minors' access to adult-oriented websites or the like, these instruments involve innovative solutions relying on emerging technologies such as access control, authentication tools and software filters of all kinds.[112] Also some progress may be made as a result of self-regulation by the Internet industry on good business practices on commercial communications.[113]

3.2. *Unsolicited commercial communications*

Service providers can also try to reach clients by e-mail. Currently, the use of spamming is becoming quite common. It consists of sending unsolicited electronic messages in which the service provider advertises his products or services to thousands of e-mail addresses. It is the equivalent to "junk-mail"

109. See Commission Communication "The follow-up to the Green Paper...", cited *supra* note 93, p. 12 et seq. Also, the recent Commission Proposal for a Regulation on sales promotions states this in Recitals 5 and 12 and Art. 3.

110. In this sense, see *Final Report Study on Consumer Law and the Information Society* written by Pricewaterhouse Coopers, Universities of Utrecht and Tilburg for the European Commission, 17 Aug. 2001. Project number: 487986.01, Report number: 00.019.

111. See footnote 137 *infra*.

112. Communication "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime" (COM(2000)890 final),", p. 6.

113. See Chapters V and VI. See also, "General principles for generic codes of practice for the sale of goods and services to consumers on the Internet" p. 5, available at the European Commission's supported E-confidence forum website: http://econfidence.jrc.it/

in the real world. The use of computer technologies enormously facilitates the compilation, storage and organization of personal data. In countries with a very low level of personal data protection, this information is used as a commercial good whose use is licensed from one company to another so that they complete their customer databases in order to promote their products or services by sending individual offers to Internet users.[114] If the use of spam is not regulated, this technique can be extremely annoying to recipients since the capability of service providers to store e-mails is limited and receiving a vast amount of unsolicited e-mails a day can disrupt the use of the service by the recipient and the smooth functioning of interactive networks.

In order to combat unsolicited commercial communications, Article 7(1) states that they shall be clearly identifiable as such as soon as the recipient receives them. An efficient way of clearly identifying spams is by stating in the subject box of the e-mail the commercial nature of its content. In such a way, private individuals are able to easily delete or filter the message as soon as it arrives. However, this provision only solves one part of the problem. Receipt of these messages still disrupts the smooth functioning of Internet applications and it increases the cost of Internet use since more time is needed for information to be received. Article 7(2) leaves it open to the Member States to adopt the system they prefer to protect recipients from unsolicited commercial communications. They may choose between the so-called "opt-out" or "opt-in" systems.

The "opt-out" system is already in force in the field of distance selling (Art. 10 of Directive 97/7) and in the field of electronic communications (Art. 12(2) of Directive 97/66)[115] although there is a Commission Proposal to change the system in the latter.[116] According to this system, it is assumed that an Internet user implicitly agrees to receive spam – which, in any case, must comply

114. The U.S. is the best known example. Art. 25(1) of Directive 95/46 prohibits transferring of personal data from the Member States to third countries not providing an adequate level of protection. Pursuant to Art. 25(6), the Commission has signed with the U.S. Department of Commerce the so-called Safe Habour Principles Decision (Commission Decisions 2000/518, 2000/519 and 2000/520 of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in USA, Switzerland and Hungary (O.J. 2000, L 215/1). The Decision states that transfer of personal data from the Community to U.S. companies will be admitted as far as companies comply with the principles stated by the DoC – the Safe Harbour Principles – and which have been approved by the Commission. US DoC is in charge of monitoring the implementing of those principles. US companies are very slowly adhering to the Principles.

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

116. See Art. 13 of the Proposal for a Directive concerning the processing of personal data and the protection of privacy in the electronic communication sector (O.J. 2000, C 365 E/1).

with Article 7(1) – insofar as he does not oppose and register in an "opt-out" register. Natural persons – none of the Directives mention legal persons – who do not wish to receive unsolicited commercial communications form these registers.

The efficiency of this system is under consideration due to several uncertainties which have not been adequately addressed by the Commission up to now. Although Directive 2000/31 urges Member States to ensure that service providers respect and regularly consult the "opt-out" registers, it is not clear who should be in charge of their administration and monitoring. These can be the competent authorities, the service providers themselves or independent third parties. In any case, the registers should have as broad a territorial scope as possible, since Internet is transnational and clients may reside in different Member States. For this reason, some authors have underlined the need for these registers to have a Community-wide territorial scope or, if registers are organized at national level, to be interconnected in order to share the opt-out lists.[117]

Since Article 7(2) does not impose the adoption of any system, several Member States may decide to adopt the "opt-in" system.[118] The "opt-in" system obliges service providers to ask any new customer whether he wants to receive commercial communications and only those who agree are sent them. For the sole purpose of processing the required personal data to send the communications, those customers are included in "opt-in" registers. On the one hand, this system is criticized by service providers as lays on them the burden of convincing customers and of taking the necessary steps for their registration with service providers. On the other hand, adoption of this system means an increase in privacy protection. In addition, it seems easier to manage than the "opt-out" system, as service providers will do their best adequately to administer their lists of customers wishing to receive commercial communications. Therefore, the Commission idea to prohibit the use of electronic mail for the purposes of direct marketing unless subscribers have given their prior consent in its Proposal for a Directive on personal data protection in the electronic communication sector seems appropriate.[119]

117. Julia Barcelo et al., op. cit. *supra* note 68, p. 13.

118. That is the case of Spain, see Art. 21(1) of the Last Draft Proposal of the Law on Information Society Services (31 April 2001). On the other hand, France has chosen the "opt-out" system, see Art. 22 of Projet de loi sur le commerce electronique, No. 3143 déposé à l'Assemblée nationale le 14 juin 2001. Available at http://www.legifrance.gouv.fr/html/actualite/actualite_legisl ative/prepa/pli.htm (last visited, Sept. 2001)

119. Art. 13 states: "Unsolicited communications (1) The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

3.3. *Promotion of activities of regulated professions*

Thanks to the directives on regulated professions, mutual recognition of services provided by professionals from other Member States is facilitated. The Directive on electronic commerce does not preclude the application of those directives concerning access to, and exercise of, activities of the regulated professions.[120] There are other professions whose services can also be provided on-line but which have not been subject to regularization at Community level yet. This does not impede these persons in the enjoyment of their freedom to provide services directly under Article 49 EC. However, there is a problem for lawyers, accountants or other professions that the way they provide their service on Internet may be limited by their professional bodies' codes of conducts. For example, in May 1998, a German court found that an electronic guest book maintained on the homepage of a local law firm constituted an advertisement and thus it was in breach of ethical professional rules in that country. Professions are often conservative bodies who may regard the provision of on-line services as inappropriate for their members.[121]

Article 8(1) obliges the Member States to ensure that the use of commercial communications by a member of a regulated profession is permitted. According to the general country of origin principle, those commercial communications should comply with the rules governing their activities in their country of establishment. In particular, Member States must ensure that such communications comply which "professional rules regarding, in particular, the independence, dignity and honour of the profession, professional secrecy and fairness towards clients and other members of the profession". Notwithstanding the general authorization of commercial communications by members of the regulated professions, the Directive is aware of the discriminatory treatment the application of the country of origin principle can entail for the provision of services by professionals established in Member States with very rigid professional rules. For that reason, it encourages the drafting of codes of conduct for the regulated professions at the Community level in order to determine the types of information that can be provided for the purpose of commercial communications.[122] The Commission is to be involved in the drafting of those codes of conduct and should be notified of them in order to determine their compatibility with Community Law.[123]

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

(3) Paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected."

120. Art. 8(4)

121. The example is taken from Kelleher and Murray, *IT Law in the European Union* (London, Sweet and Maxwell, 1999), pp. 114–115.

4. Electronic contracts

The promotion of products or services and of the activities of professional in commercial communications will eventually lead to the conclusion of contracts with recipients of the Information Society service. Internet does not only enable this promotion but it also allows contracts to be concluded electronically and for obligations to be performed on-line. The service in itself can be an electronic agent pre-programmed to accept the ordering of a product or service on behalf of its owner: websites are designed in such a manner that customers themselves can conclude the contract with the website by filling up an application form to order the product or the service. Furthermore, they can submit the credit card number to pay the price, and the service or product can be electronically delivered instantaneously.[124] A whole contractual relation may take place in Internet in a few minutes. In other situations, two recipients may use Information Society services such as electronic mails to conclude a contract between themselves.

The Directive on electronic commerce has not tried to regulate each and every legal problem raised by the formation and performance of these contracts.[125] The contractual regime is governed by the national law of the Member States. However, the Directive has removed legal obstacles which may hinder the establishment of the single online market by harmonizing specific aspects of the contractual process. It has also established obligations on service providers to enhance transparency of online transactions and the degree of consumer protection on the grounds, once again, of the particular nature of the new media.

122. Art. 8(2)

123. Art. 8(3)

124. A distinction is made between indirect e-commerce (the electronic ordering of tangible goods, which still must be physically delivered using traditional channels such as postal services or commercial couriers) and direct e-commerce (the online ordering, payment and delivery of intangible goods and services such as computer software, entertainment content, or information services on a global scale). See Kelleher and Murray, op. cit. *supra* note 121.

125. Time and place of formation of the contract, formal requirements, remedies to defective performance of the obligation etc. For a good explanation see Bryde Andersen, "Electronic Commerce: A Challenge to Private Law?" in Centro di studi e ricerche di diritto comparato e straniero, *Saggi, conferenze e seminari* (Rome, 1998) and De Miguel Asensio, op. cit. *supra* note 84, pp. 303–385.

First of all, Article 9 obliges Member States to ensure that their legal systems do not deprive electronic contracts of legal validity on the sole ground of their having been concluded by electronic means. At present, parties can ensure the validity of their electronic contracts because Member States' civil laws recognize a great scope of action to the freedom of the parties to regulate their relations. However, there are situations where this freedom is limited in order to protect certain categories of individuals (consumers or employees) or where a public interest is at stake (immovable property, family law). In such cases, the validity of contracts may depend on the fulfilment of some formal requirements: contracts concluded "in writing", intervention of a public authority, presence of witnesses. The provision obliges Member States to remove such requirements or to reinterpret them in such a manner that their electronic equivalents are admitted.[126] This obligation will particularly affect consumer protection regulations as far as they usually require contracts to be "in writing" or confirmation in writing.[127]

This obligation should not prevent Member States from imposing or maintaining specific legal requirements for specific contracts as far as they can be fulfilled by electronic means. In particular, Member States can still require some contracts to be in "writing", as far as the concept covers electronic documents, or they can require a signature. Since electronic signatures play in electronic commerce the same function as hand-written signature in traditional commerce,[128] the formal requirement can be equally met. Regulation of electronic signatures has been harmonized at Community level in Directive 1999/93 on a Community framework for electronic signatures. Article 5 obliges Member States to give digital signatures the same legal effects as hand-written signatures provided that certain requirements are met.[129]

126. Julia Barcelo et al., op. cit. *supra* note 68, p. 18.

127. See De Bottini, "La Directive Commerce Electronique du 8 juin 2000", (2001) RMC, 368–373, particularly 371.

128. Directive 1999/93 of 13 Dec. 1999 on a Community framework for electronic signatures, O.J. 2000, L 13/12.

129. Art. 5: "Legal effects of electronic signatures. (1) Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device: satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and are admissible as evidence in legal proceedings. (2) Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is: in electronic form, or- not based upon a qualified certificate, or not based upon a qualified certificate issued by an accredited certification-service-provider, or not created by a secure signature-creation device." A distinction is made between "advanced electronic signature" – also called digital signatures – and "electronic signature". Legal equivalence to hand-written signature is attributed to the first category insofar as they fulfil certain requirements established in Directive 99/93 guaranteeing authenticity: it is uniquely linked to the signatory; it is capable of identifying the signatory; it is created using means that the signatory can maintain under his sole control; and it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable. The second category do not fulfil those requirements, but the legal validity cannot be denied on the sole basis of its electronic nature. For further details, see Sanchez Felipe, "La reglementation du commerce electronique dans l'Union Européenne", (2000) *Uniform Law Review*, 665–682, Martinez Nadal, *Comercio electrónico, firma digital y autoridades de certificación* (Madrid, Civitas, 1998); Font, *Seguridad y certificación en el Comercio electrónico* (Madrid, Biblioteca Fundación Retevisión, 2000); Caprioli, "Sécurité et confiance dans le commerce electronique (Signature numérique et autorité de certification)", (1998) *La Semaine Juridique* (I 123), 583–59.

Article 9(2) enables Member States to exclude certain contracts from this obligation. This refers to matters whose exclusion is justified by their legal nature: "(d) contracts governed by family law or by the law of succession". For the other cases, justification seems to be the fact that intervention of a public authority is required: "(a) contracts that create or transfer rights in real estate, except for rental rights; (b) contracts requiring by law the involvement of courts, public authorities or professions exercising public authority; (c) contracts of suretyship granted and on collateral securities furnished by persons acting for purposes outside their trade, business or profession". It does not seem that this justification is enough to exclude the possibility for these contracts to be concluded by electronic means insofar as the intervention of those public authorities may also be performed electronically and using mechanisms such as electronic signatures.[130] Member States are required to provide the Commission with a list of the contracts they exclude and a justification for their exclusion.

Article 10 aims to safeguard a fundamental principle of contract law: a transaction requires each party freely and clearly to manifest a motivated contractual assent. For recipients to express a motivated and conspicuous assent, they must be well-informed of the content and conditions of the contract and of the implication of their acts on Internet. In this sense, Article 10 obliges service providers "clearly, comprehensibly and unambiguously" to provide recipients with all the information concerning the content and the terms of the contract. This information encompasses the different technical steps to follow for the conclusion of the electronic contract; whether the contract will be filed in the service provider's computers and whether it will be accessible; the technical means for identifying and correcting input errors prior to the placing of the order; and the languages offered for the conclusion of the contract.[131] In addition, Article 10(3) obliges service providers to make all the contract terms and general conditions available in a way that the recipient can reproduce and store them. This is a stricter obligation than that applicable to the rest of distance contracts since Directive 97/7 does not oblige

130. Julia Barcelo et al., op. cit. *supra* note 68, p. 20.

131. Art. 10 (1).

retailers to make all contractual terms accessible prior to the conclusion of the contract. Finally, service providers must inform recipients about any Code of conduct they adhere to and information on how these codes can be consulted electronically.[132] As will be explained, the European Community promotes the use of this kind of self-regulation in the belief it will help to implement the Directive efficiently.

Again, the strictness of this transparency obligation is justified by the novelty of the medium where these transactions take place. It was considered that electronic contracts required additional guarantees to maintain the level of consumer protection. Likewise, the general information to be provided under Article 5, the use of links leading to specific web pages should be enough to make sure that certain specific points have been made accessible, they should be included in web pages the recipient must pass through to place the order. Insofar as this provision aims basically to protect consumers, Article 10(1) permits the parties to derogate from the transparency obligation in contracts between merchants when the parties so agree. Also, Article 10(4) states this obligation does not apply to contracts concluded between individuals by electronic mails or by an equivalent individual communication system. In such a way, a certain degree of flexibility is introduced for those contractual relations where the bargaining position of the parties is balanced and thus the freedom of contract can play fairly to allow them to configure the relation to their own needs.

Finally, Article 11 deals with the placing of orders directly at a website. As has been said, a whole contractual relation can take place in a website. First the customer selects and examines the product or service, then he fills a standard form with his personal data and credit card number, and finally he send the data by clicking on an "I agree" icon on the screen. This final step may have different implications in the different Member States legal orders and it gives rise to uncertainty as to the time and place of conclusion of distance contracts. This question may have important implications for the relation: it establishes the moment transmission of the risks take place, it determines the moment certain time-periods starts to count (cooling-off period for distance consumer contracts) , or the moment the right to revoke the offer expires.[133] In the initial Commission Proposal, Article 11 was deemed to give a uniform solution to this question.[134] In broad terms, certain legal systems consider that moment being when the offeror receives the acceptance by the offeree (theory of reception) while others consider that the contract is concluded

132. Art. 10(2).

133. Davies, "Contract Formation in the Internet: Shattering a Few Myths", in Edwards and Waelde (Eds.), *Law and the Internet, Regulating Cyberspace* (Hart Publishing, Oxford, 1997), pp. 97–119.

134. Doc. COM(1998) 586 final, p. 27.

when the offeree has sent the acceptance (the Postal rule on common law). The Commission Proposal set the moment when the recipient of the service has "confirmed receipt of the acknowledgement of the receipt".[135] However, it was removed from the Directive in the Council in so far as solutions in the different legal systems were very distant. For instance, there was not a uniform qualification of advertisements on websites: while certain Member States legal systems considered them as offers other qualify them as invitations to negotiate, thus it is the recipient who actually makes the offer. The question on the moment the contract is concluded remains thus subject to the national law applicable to the electronic contract. As a consequence, regulation of this aspect will vary from one situation to another.

In the final text, Article 11 exclusively establishes an obligation on service providers to acknowledge the receipt of the recipient's order without undue delay and it determines that an order or an acknowledge of receipt must be considered to be received when the parties are able to access them. Such acknowledgement of receipt may take the form of the on-line provision of the service requested by the recipient[136] – e.g. access is given to a database, downloading of an intangible product starts. In other cases, the acknowledgement is an automatic reply message. The parties are considered to be able to access a message when it has reached the recipient's service provider's computer system – that is the "mail box" – regardless of whether they have actually consulted it or not. Although with current computer technology it is possible to know whether the transmission of the message has gone well, certainly many problems may appear on the application of this provision: recipients may be unable to access their mail-box from a long time, thus they might not know whether such acknowledgement of receipt has been received; also, it is for the Member States to decide on the legal consequences for not sending such acknowledgement. Since the Directive does not provide any principle, it is for the national legislatures to decide on the best way to regulate those aspects.

5. Liability of intermediary service providers

Internet provides an excellent media for dissemination of information. Many Information Society services consist of the storage of information to allow others to access it for remuneration or for free. Its global character makes access to that information possible from any point in the planet. However, such

135. Thus four steps where needed for the formation of the electronic contract: offer, acceptance, acknowledgement of receipt of acceptance, confirmation of receipt of acknowledgement of acceptance.

136. Recital 34.

information may have an illegal or infringing character. The impact of such harmful activities is higher that in a traditional context: effects can rapidly spread throughout the Internet world. Furthermore, information technology enables these persons to hide their identity. A direct consequence of this is the great difficulty in locating the primary party responsible for illegal and harmful content in the Internet. An indirect consequence is that victims try to sue service providers as vicariously or even primarily liable for these activities to ensure the receipt of a compensation.

Drafting of Articles 12 to 15 of Directive 2000/31 was subject to great discussion between the Community institutions and the representatives of the Internet industry. These provisions are inspired by the Digital Millennium Copyright Act of the United States, though the latter exclusively applies in the field of copyright. They aim to provide a harmonized solution on the regulation of the liability of intermediate service providers for the content of the information circulating throughout their networks. Any other aspect concerning liability arising from illicit activities carried out in Internet remains subject to national substantive laws.[137]

The term "service providers" of Article 2 encompasses two categories: content providers and intermediate service providers. While the former provide the digital materials which can be accessed on Internet – either individual end users who rent space from a service provider to create their own web page or multinationals' service providers to sell their product or services –, the intermediate service providers' activities consist of the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted.[138]

137. It is recalled that the institutions are working on the adoption of the effective measures to regulate the legality of the contents provided in the Internet (See section 3.2 *supra*). Those measures focus on both substantive and procedural aspects. They include Council Recommendation 98/560 of 24 Sept. 1998 on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity (O.J. 1998, L 270/48); Decision 276/1999 of Jan. 1999 adopting an Action Plan against illegal and harmful content on the Internet (O.J. 1999, L 33/1) which co-finances awareness actions, experiments in rating and filtering of content and hot-lines; the Green Paper on the protection of minors and human dignity in audiovisual and information services (COM(96)483 final); the Communication on the illegal and harmful content on the Internet (COM(96) 487 final); the Communication "Creating a Safer Information Society ...", cited *supra* note 112; and Council Decision of 29 May 2000 to combat child pornography on the Internet (O.J. 2000, L 138/1).

138. Depending on the functional role they play, there are: network operators (providing the facilities for the transmission of data); access providers (providing access to the Internet for their clients); host service providers (providing a server computer upon which to rent space to users to host content); bulletin board operators, news groups and chat room operators (services providing space for users to read information sent by other users and to post their own messages). They can be moderated or unmoderated. Chat rooms allow direct communication in real time; information location tool providers (providing tools to Internet users for finding websites where information they seek is located). See Julià Barceló: "Liability for on-line intermediaries: a European perspective", 20 *European Intellectual Property Review* (1998), 453–463.

Depending on the content of information they transmit or make accessible on the Internet, services providers can infringe intellectual property legislation,[139] defamation law,[140] criminal laws, civil law on torts[141] or other norms. Regulation of the intermediate service providers' liability is based on two rules: they are exempted from liability for the content of the information transmitted, processed or stored as far as they remain neutral (1); and they do not have an obligation to monitor but only to co-operate with competent authorities to remove illegal or harmful content (2).

5.1. *Exemption from liability*

The general rule in the Directive is that liability falls on the person making the unlawful information accessible. In principle, as far as intermediaries have no knowledge of the content of the services being provided they are exempted from liability.[142] However, in order to benefit from this exemption, certain circumstances must be met for each intermediary activity: "mere conduit", caching and hosting.

"*Mere conduit*" refers to the transmission of information in a communication network or the provision of access to a communication network. The definition includes all technical steps necessary for the transmission of the information: the automatic, intermediate and transient storage in the service provider computer if it is not stored for any period longer than is reasonably necessary for the transmission.[143] The service provider is not liable for the content of the information transmitted, on condition that he does not initiate the transmission, does not select the receiver and does not select or modify the information contained in the transmission.[144]

Caching consists of the temporary storage of information in the service providers' computers, performed for the sole purpose of making the access

139. Infringing acts may occur when certain websites include files containing copyright material and they can be downloaded.

140. Pictures, personal data or writings of a defamatory nature posted to bulletin boards or chat rooms.

141. These categories include cases of liability for illegal and harmful content and misrepresentation.

142. See Arts. 12(1), 13(1) and 14(1).

143. Information on Internet travels from one computer to another until it reaches its destination. Every computer along the way makes a temporal copy – a transient storage – in order to transmit the information to the following computer.

144. Art. 12 (2).

to that information easier and faster for other recipients of the service.[145] The temporary character of the storage distinguishes caching from hosting. According to Article 13, such activity is exempted from liability if the service provider does not modify the information; he complies with the conditions on access to the information; he regularly updates the information in a manner widely recognized and used by the Internet industry; he does not interfere with the lawful use of technology to obtain data on the use of the information; and he undertakes to remove or disable the access to such information once he has knowledge that the information at origin has been removed from the network or has been made inaccessible either by the service provider's own decision or by a judicial or administrative order.

Hosting is the most controversial of the three activities. It consists of the permanent storage by intermediary service providers of information provided by recipients. Service providers offer space in their computers in which recipients can store websites, e-mail boxes, discussion groups, usenet groups. They are not liable for the information stored at the request of a recipient as far as they do not have actual knowledge of the illegal character of the activity or information, or they are not aware of facts or circumstances from which the illegal activity or information is apparent. At that precise moment, as part of their obligation to co-operate in the eradication of illegal and harmful content or activities, they must act expeditiously to remove or disable access to the information.[146] Member States may establish specific procedures for that purpose, in accordance with their legislation or they may encourage interested parties to develop these systems on the basis of voluntary agreements or codes of conduct.[147] Pursuant to this provision, the private sector is promoting the use of the "Notice and takedown" procedure of the US legislation. According to this, service providers remove any content residing on their networks under the request of a "designated agent" following a valid notice in which the location of the information, its illegal character, and the specific regulation infringed is proved.[148]

145. E.g. if a recipient of the service provider visits a website, the service provider would automatically make a copy of that website in his computers to make subsequent access to that website easier for that recipient and other clients.

146. Art. 14(1).

147. Art. 14(3) and Recital 40.

148. See Orts Perez, "Análisis general de la Directiva de Comercio Electrónico con especial atención a los artículos relativos a la responsabilidad de los intermediarios", available at http://v2.vlex.com/vlex2/front/asp/e-papers.asp

5.2. *No obligation to monitor but to co-operate*

Article 15(1) states that Member States may not impose on service providers a general obligation to monitor the information transmitted or stored at the request of their recipients. It is impossible for them to control the legality of all the information circulating throughout the communication networks. In addition, permanent monitoring would certainly infringe the right to privacy as it is endorsed in the Member States' constitutional laws. However, service providers have an obligation to co-operate with competent authorities on the detection and eradication of unlawful contents and activities on the Internet. In some cases, such co-operation is at the request of competent authorities (Arts. 12(3), 13(3), 14(3) or Art. 15(2)), but in other cases such co-operation consist of a duty to be vigilant and to act on their own initiative for the removal of those materials (Arts. 14(1)(b) and 15(2)).

According to the first set of provisions, although service providers are exempted from liability for the content of the information transmitted or hosted at the request of recipients, administrative authorities, in accordance with their Member States' legal systems, may require them to terminate or prevent an infringement on behalf of one of their recipients. Also, Article 15(2) states that Member States may impose on service providers an obligation to communicate to the competent authorities information enabling the identification of recipients of their service with whom they have storage agreements. These obligations on the service providers are justified on the central role they play in the functioning of the Internet. They are the best placed to help the prevention or eradication of harmful and illegal activities. These obligations should not be considered disproportionate, nor do they entail legal uncertainty for service providers insofar as, according to the provision, they act under the initiative and the instructions of a competent authority. Liability *vis-à-vis* recipients for measures infringing their right to privacy – e.g. a disproportionately long surveillance of messages sent to a bulletin board – should lie with the competent authority. Furthermore, in any case, the steps to be taken by service providers to terminate or prevent an infringement must be "in accordance with Member States' legal orders", thus the respect of citizens' rights is guaranteed.

The second set of provisions must be criticized. They impose a duty to be vigilant on service providers. As was explained above, according to Article 14(1) (a) and (b), a service provider is under the obligation to expeditiously remove or disable access to an illegal activity or information once he gets actual knowledge or he is aware of facts or circumstances from which the illegality is apparent. Furthermore, Article 15(2) allows the Member States to establish an obligation for service providers promptly to inform competent authorities of alleged illegal activities undertaken or information provided by their recipients. In these two cases, service providers must act on their

own initiative. A request from the competent authorities is not apparent. This has been highly criticized for two reasons. First, for the diffuse meaning of "actual knowledge": when can it be stated that a provider has actual knowledge of an illegal information?, and, more important, how can the providers prove before a judge that he did not have "actual knowledge" of it?[149] The second criticism arises from the fact that service providers are placed under an obligation to assess the legality or illegality of the information provided or activity undertaken by the recipient. Taking into account the vast amount of matters Information Society services affect and the difficulty the decision on the legality of a social act may entail, this obligation imposed on providers, which may submit them to a high degree of legal uncertainty on their provision of Information Society services, seems too heavy. For instance, in a case of publication of a parody of a work of art, if the service provider considers such publication illegal on the grounds of its defamatory nature and removes it from the server, he can be liable towards the recipient if a court otherwise holds that such work of art is permitted under the freedom of expression right. In other case, a service provider must be held vicariously liable for not removing a website providing access to the customers' personal data of a telephone company although he assumed customers had consented the use of that data. In many cases, procedures such as that of the "Notice and takedown" may be introduced to help in implementing these provisions. However, there are still certain legal questions these procedures raise. They basically transfer responsibility for the decision on the legal or illegal character of the information or activity to the "designated agent". It is not clear what the position of this person is towards service providers and recipients, since determination of his liability would depend on the national law applicable. Furthermore, it is doubtful whether these procedures would be effective in every field of non-contractual liability law.

6. Effective enforcement and dispute resolution systems

Chapter III of Directive 2000/31 is entitled "Implementation". It aims to provide additional mechanisms contributing to the effective enforcement of the law in the new environment. The international dimension of the Internet entails an increase in cross-border relations. In these relations, the parties are submitted to uncertainty as to the body of rules applicable and the courts with jurisdiction over a hypothetical dispute. This uncertainty is harmful for the development of electronic commerce and it may have consequences for the

149. In this sense Marín Peidro, *Los contenidos ilícitos y nocivos en Internet* (Biblioteca Fundación Retevision, Madrid, 2000), pp. 95–101.

effective control of Information Society services. Also, weak parties such as consumers may be reluctant to sue due to disproportion between the low-value of the transaction and the need to start a proceeding abroad. Furthermore, the effects of unlawful activities can expand faster and reach a broader number of countries when they are committed in the Internet.[150] For these reasons, the Directive provides a legal framework for the development of alternative regulatory and dispute resolution schemes (Arts. 16 and 17) and for the adoption of more effective and faster judicial redress mechanisms (Arts. 18 and 20). Also, the need to co-operate among Member States' authorities for an effective law enforcement on Internet is stressed in Article 19.

The alternative regulatory and dispute resolution scheme consists of the adoption of codes of conduct at Community level and the use of alternative dispute resolution systems both in business-to-business and business-to-consumer electronic commerce. In many cases, Information Society services will give rise to consumer disputes, insofar as recipients will contract Information Society services "for a purpose outside his trade or profession". They may concern the defective performance by service providers of their contractual obligations, such as an adequate Internet access, the use of personal data without consent, or the use of misleading advertising on websites, etc. Often, the consumer will be domiciled in a different Member State from that of the provider thus he will be uncertain whether such deficiencies or activities are legal or not. He may also be unsure whether to bring the case before his own courts or before the courts of the defendant's domicile State. Even more, although domestic laws and Private International Law rules always protect their interests, consumers are usually reluctant to bring their case before judicial courts. The Commission has addressed the reasons in a number of instruments:[151] a) the high costs which a judicial dispute implies (including legal consultation, representation by a lawyer before the court, and costs of experts opinions) in comparison with the small value of the claim; b) the long duration of judicial disputes due to the backlog in the courts which leads to long delays before a case is judged; c) the complexity and formalism associated with court procedures; d) reluctance to initiate proceedings in a language other than that of the consumer. The generalization of cross-border disputes and low-value transactions on the Internet demands the adoption of more flexible mechanisms so that consumers can effectively claim their rights. At the same time, the Internet industry has already addressed the fact that new service providers may be reluctant to join electronic commerce, the reason

150. Assuming a person uploads a pirate software on his website, if it is not quickly removed once another recipient downloads it, he may offer it to other user so that the copies of the pirate software multiply and it becomes impossible to stop the infringing activities.

151. See Communication on the out-of-court settlement of consumer disputes (Doc. COM(1998) 198 final of 30 March 1998).

being that as far as their websites are accessible from the territory of any Member State, according to existing PIL rules on consumer contracts, they are potentially subject to the jurisdiction of any Member State[152] and bound by the mandatory rules of each and every State where they want to trade.[153]

Article 16(1) promotes the drawing up of codes of conduct at Community level, by trade, professional and consumer associations designed to contribute to the proper implementation of the Directive, particularly in the field of the regulated professions. This provision provides the opportunity for the interested parties to implement certain provisions of the Directive themselves, without the need of a legal intervention. Since they are aware of the problems raised by electronic commerce relations, they are better placed to provide the most adequate regulation of them.[154] Also, drawing up these codes at Community level provides legal certainty: service providers would adapt their contracts with Member States' consumers to a unique body of rules, and consumers would know where to find out their rights and obligation. For this purpose, it is stated that they should be drafted in all the Community languages and should be made accessible electronically.[155] Both business and consumer associations should be involved in the drafting of these codes in order to guarantee a proper balancing of the interests' involved. The trade, professional or consumer associations are invited to submit them to the Commission in order to determine their compatibility with Community law.

Codes of conduct may play a significant role in two very important areas for the consolidation of electronic commerce: content regulation and consumer contracts. In the first case, service providers may contractually oblige recipients to comply with a code of conduct in the use of the services made available to them. In those instruments, service providers may retain powers to remove or block access to information of a recipient when it is of an illegal nature. Furthermore they can establish hot-lines where other recipients may denounce the unlawful character of certain information stored by the service provider and "notice and takedown" procedures. In the second case, codes of conduct provide legal certainty for consumers about their rights and obligations under the contract. Service providers' adherence to a code of conduct constitutes a factor of quality and consumer reliance insofar as the provider undertakes to comply with certain obligations to the benefit of consumers relating to commercial communications, information requirements on goods and services on offer, information about the contract terms, conditions and obligations, complaint handling and dispute settlements.[156] In order to show the service providers' adherence to a code of conduct they are allowed to incorporate a label or "trustmark" on their websites usually providing an hyperlink to the provisions of the code.[157]

The success of this alternative regulatory scheme relies on two factors: legitimacy and efficiency. The former requires all the parties concerned to participate in drawing up these codes as stated in Article 16(1). For one thing, if certain service providers are not represented they may be reluctant to enforce them. Also, lack of participation of consumer associations in the bodies responsible for drawing self-regulatory instruments may entail consumers' reluctance toward norms which have been drawn up without taking their interests into account. They do not feel their contractual relations are governed by the codes of conduct instead of the State legislation. The second factor requires the establishment of mechanisms for monitoring and enforcement of the self-regulatory schemes. This means that when service providers do not comply with their obligations under a code of conduct, they should be effectively sanctioned. Effectiveness requires the involvement of Member State authorities and not simply of the bodies responsible for the administration of the code of conduct, to the extent they can be influenced by the most powerful parties. Finally, effectiveness of self-regulation is hampered by the strict limits imposed by existing legislation: mandatory rules must be respected in drawing up these codes.[158] In the field of consumer contracts, due to the "de minimis" nature of consumer protection directives, those mandatory rules vary from one Member State to another. For a self-regulatory scheme to be valid in all the Community it should comply with the strictest mandatory rules of the Member States. This definitely constrains the margins for the codes of conduct to be drawn up, thus it decreases the value of this instrument as an alternative to State law enforcement mechanism.[159]

152. Arts. 13–15 of the Brussels Convention and 15–17 of Regulation 44/2001 state that consumers can sue and can only be sued in their domicile in disputes arising from contractual relations provided that the business was directing his activities, by any means, to the consumer's residence State.

153. Arts. 5 and 7(2) of the Rome Convention oblige national judges to apply the mandatory rules of the consumer's residence legislation or that of the national court. It shall also be recalled that consumer obligations are exempted from the application of the country of origin principle of Directive 2000/31.

154. See Poullet, "How to regulate Internet: new paradigms for Internet Governance. Self-regulation: Value and limits", handed out in the Eclip Workshop "Process of Internet Regulation", held in Namur (Belgium) 7 June 2000.

155. See Art. 16 (1) (c)

156. See "General principles for generic codes of practices...", *supra* note 113.

157. See e.g. the labels of WebTrader, Trustee, BBBonline, and many other at http://consumerconfidence.gbde.org/t_invent ory.html

158. See De Miguel Asensio, op. cit. *supra* note 79, pp. 70–75.

159. This problem has been addressed in the recent Green Paper on European Union Consumer Protection (Doc COM(2001)531 final). Despite the number of harmonizing Directives in the field, differences between consumer contracts regulation in the Member States hamper the consolidation of cross-border business-to-consumer transactions. This affects electronic commerce in particular. A public consultation is opened to decide on a future legal approach to be taken in order to remove these obstacles. There are two options: the specific approach,

Self-regulation is complemented with the promotion of the use of out-of-court dispute settlement systems (ADR). Consumers are reluctant to sue in court for several reasons, the most important being the disproportion between the costs of litigation and the low amount of money usually claimed in this kind of disputes. For electronic commerce disputes, reluctance may also come from the need to litigate in a foreign country or the lack of feasibility that the decision will be effective in the Member State where the service provider is established. The inexistence of effective legal redress mechanisms may lead consumers to turn their face on electronic commerce. Effective and flexible dispute resolution systems must be developed so that consumers have an alternative system to judicial courts to claim their rights. Being so, ADR have been pointed to as a possible solution. They consist in uni-personal or collective extra-judicial bodies where the parties to a contract can agree to bring their disputes, the objective being mainly to reach a settlement.[160] In order to provide a real alternative to domestic courts, ADR systems are designed to be easily accessible to consumers, at a very low cost, with a very flexible and informal procedure and where decisions are given in a relatively short period of time. Only ADR with these characteristics represent a real alternative to domestic courts.[161]

Insofar as ADR are a manifestation of the jurisdictional power, their organization and regulation is under the competence of the Member States. However, Article 17(1) obliges Member States to remove any obstacle in their legal system that may hamper the use of out-of-court schemes, available under national law, for dispute settlement in the event of disagreement between an Information Society service provider and the recipient of the service. Furthermore, they must remove any legal obstacle impeding the use of electronic means for the development of the procedure. It has already been successfully proved in the field of domain names disputes, that procedures can be entirely

consisting in enacting several instruments on those legal matters which are still to be harmonized; or the mixed approach consisting in the adoption of a framework Directive establishing some core principles and enabling Member States and self-regulatory schemes to develop those principles. If the second option is preferred (and that seems to be the Commission's choice), co-regulation may provide an effective instrument for the regulation of on-line consumer contracts.

160. ADR existed before electronic commerce. Their utility has already been assessed in the framework of the access to justice policy of the European Community in the Communication on out-of-court dispute settlement systems. In order to inform the general public about their existence and their competences, the Commission has listed them in a database accessible at the Health and Consumer Protection Directorate General's website: http://europa.eu.int/comm/consumers/policy/ developments/acce_just/acce_just04_en.html

161. For information on the different ADR systems in electronic commerce see Tilman, "Arbitrage et nouvelle technologies: alternative cyberdispute resolution", (1999) *Revue Ubiquité*, 47–64; and Kessedjian and Cahn, "Dispute Resolution On-Line", 32 *The International Lawyer* (1998), 977–990.

carried out on-line.[162] Information technologies surely favour a faster and more efficient development of ADR proceedings: they enable the electronic submission of complaints and any additional documents needed to support the case, facilitate communication between the parties and the arbitrator, and the storing of documents relevant to each specific case.[163] In such a manner, individuals do not even have to move from their home to claim their rights.

ADR can be not only of a public nature but also private. In the latter case, if all interested parties are not consulted in its constitution, it can arise that ADR are designed to benefit business interests. Article 17(2) obliges Member States to encourage bodies responsible for the ADR to operate in a way which provides adequate procedural guarantees.[164] It is to be criticized that the European Community is progressively lowering the level of procedural guarantees required in ADR.[165] For this reason, notwithstanding the benefits ADR may have, consumers must always have the possibility to bring the case before courts. Otherwise this would be in contravention of Article 6 European Convention of Human Rights.[166] Consumers will go to ADR only if they believe they will get efficient legal redress. They can never be forced to submit the dispute to ADR before starting a judicial action.

In addition to the promotion of alternative law enforcement systems, the Directive also provides mechanisms to reinforce traditional systems. Article 18(2) legitimates consumer associations to act in court to defend the interests of this sensitive group on the ground of Directive 98/27 on injunctions for the protection of consumers' interests.[167] Additionally the Directive requests

162. The WIPO Arbitration Centre and the E-Resolution Arbitration Centre deliver decisions on the legality of a title over a generic domain name within 45 days. Visit http://arbiter.wipo.int/center/index.html and http://www.eresolution.org/.

163. See Wilikens, Vahrenwald, Morris, *Out of Court Dispute Settlement systems for e-commerce*, available at http://dsa-isis.jrc.it/ADR (last visited, Sept. 2001)

164. O.J. 1998, L 115/31.

165. In Recommendation 98/257 on the principles applicable to the bodies responsible for out-of-court settlement of consumer disputes, the Commission stated ADR must comply with seven principles so that it can be considered that they provide guaranties equivalent to a judicial procedure: independence, efficiency, transparency, liberty, legality and the adversarial principle. At present, Art. 17(2) only obliges Member States to *encourage* ADR to provide adequate procedural guarantees and the recent Commission Recommendation of 4 April 2001 on the principles for out-of-court bodies involved in the consensual resolution of consumer disputes (O.J. 2001, L 109/56) exclusively talks about impartiality, transparency, efficiency and fairness.

166. Art. 6 of the European Convention of Human Rights provides that "in the determination of his civil rights and obligations everyone is entitled to a fair hearing within a reasonable time by an independent and impartial tribunal established by law". According to this access to judicial courts is a fundamental right of individuals that knows no exception. Consumers can never be deprived of this right.

167. Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 on injunctions for the protection of consumers' interests (O.J. 1998, L 166/51)

the Member States to ensure that appropriate court actions are available for consumers, including, if possible, access to judicial procedures by appropriate electronic means.[168] Furthermore, procedural laws must be adapted to allow the rapid adoption of measures designed to terminate or prevent an infringement.[169] The global nature of Internet and the facilities of computer technologies imply that the effects of a harmful activity can rapidly spread to a broader geographic extension. This requires legal systems to provide mechanisms to act rapidly against unlawful activities so that the dissemination of the effects can be blocked.[170]

7. External dimensions of EC policy on electronic commerce

The global dimension of the Internet enables electronic traders to do business in any country in the world. Distances make no sense in cyberspace. This is specially relevant for companies working with non-tangible goods, since they can be electronically delivered, and for companies providing services. The computer software industry is specially concerned. However, the European Community refrained from dealing with the external aspects of electronic commerce in Directive 2000/31. The Internal Market approach of the Directive, and in particular the application of the country of origin principle cannot be applied to the provision of Information Society service at a world-wide level[171] and, for the time being, it can not be taken as a model for possible future international negotiations. A higher degree of legal integration is needed for that purpose.

The establishment of an appropriate European regulatory framework contributes to the creation of a common and strong negotiating position in international fora in the search for a higher consensus on the regulation of electronic commerce which may eventually facilitate Information Society services to be provided at a global level. At the same time, the establishment of the regulatory framework in the Community needs to be consistent with international instruments.[172] A example of this consistency is Directive 2001/29 on the harmonization of certain aspect of copyright in the Information Society. It translates into Community Law the principles embedded in the WIPO Treaty on Copyright of 20 December 1996,[173] not yet in force. The drafting of several of the provisions in the final text were a common initiative of the EC and

168. See Recital 53.
169. Art. 18 (1).
170. See e.g. the example of the pirate software in note 150 *supra*.
171. See Commission Proposal, p. 16.
172. Recital 58.
173. Available at http://www.wipo.int/clea/en/index.html

its Member States. The Treaty will provide a minimum level of protection in every country member of the Berne Union to works of art exploited in the Internet. Like the European Community, the United States adapted their legislation to the Copyright Treaty in the Digital Millennium Copyright Act in order to implement the Treaty. Once the EU Member States ratify it, the number of ratifications needed will have been reached and it will enter into force.

UNCITRAL has already adopted a Model Law on Electronic Commerce whose scope of application is limited to the business-to-business sector. Its purpose is to guide national legislatures on the regulation on contracts concluded on-line. At present, the UN agency's Working Group on Electronic Commerce is elaborating a Model Law on electronic signatures.[174]

In the WTO, a Ministerial Declaration on global electronic commerce, of May 1998, mandated the General Council to establish a working programme to examine all trade-related issues arising from Internet. At present, debate is focused on the legal nature of certain of the products and services which can be offered in the Internet – book, computer programs, electronic communication services. The results of the discussions will affect on the WTO agreements applicable to each of them and thus the permitted restrictions.[175] Since competence in services and Intellectual property is shared by the Community and Member States, adoption of a common position is very important to gain a strong bargaining power in the debates.

The Council of Europe, after a four-year period of work, approved the Final text of the Convention on Cyber-crime.[176] It is designed to protect network and users security by regulating high-technology crimes, including unauthorized access to a network, data interference, computer-related fraud and forgery, child pornography, and digital copyright infringement. It also regulates surveillance powers of the Member States governments and the co-ordination between them. The Convention is open for the adhesion of countries other than Members of the Council of Europe, such as the United States.

The Hague Conference on Private International Law is working on a Universal Convention on Jurisdiction and Enforcement of judgments in civil and commercial matters which also covers electronic commerce. Such an instrument should deal with jurisdiction on disputes arising in international relationships and it should establish a simplified system of recognition of judgments as far as rules on jurisdiction provided in the Convention are respected. Despite the fact that it is still under discussion whether the Com-

174. Both texts are available at http://www.uncitral.org/en-index.htm
175. Information is available at http://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm
176. See the Final Draft at http://www.coe.int/

munity has now acquired external competence over judicial co-operation in civil matters and whether it can become a member of the Hague Conference, Member States has adopted a common position on the negotiation of this Convention. Such a common position is reflected in the principles embedded in the Brussels Convention on jurisdiction and enforcement of judgments in civil and commercial matters.[177] In fact, the Convention was taken as a model to draft the text of the Universal Convention.[178] However, in the last year, divergent views between USA and EU on the regulation of jurisdiction on electronic commerce has blocked the negotiations. The adoption of this important text is in danger to the extent that EC Member States are reluctant to give more concessions than those already given in order to facilitate a final agreement.

The European Community is also concerned with decisions taken at ICANN, the non-profit, private, international organization entrusted with the administration of the Internet and the management of the domain name system. The European Community follows closely most of the issues which are discussed in this forum. The Commission expressed its views on the management of the Internet in a Communication adopted during the year 2000.[179] Also it is of some interest for this organization the creation of the top level domain name. "EU"[180] as far as the compatibility of the principles guiding the management of this domain name must be determined with those sustained by ICANN for its approval.

Finally, in the framework of the OECD, the adoption of some general recommendations on the protection of consumers in electronic commerce was agreed by its more than 40 members in December 1999.[181] They set out the principles which must guide the business-to-consumer sector of electronic commerce. They are coherent with EC legislation on consumer protection and with Directive 2000/31.

177. As has already been mentioned, the Convention will be replaced by Council Regulation 44/2001 in March 2002.

178. The different versions can be accessed at http://www.hcch.net/e/workprog/jdgm.html

179. Communication from the Commission to the Council and the European Parliament on the Organization and Management of the Internet. International and European Policy Issues 1998–2000. Doc COM(2000)202 final of 7 May 2000.

180. See Commission Proposal for a Regulation for the implementation of the Internet top level domain name .EU, COM(2000)827 final.

181. OECD Guidelines for Consumer Protection in the Context of Electronic Commerce. Available at http://www.oecd.org/dsti/sti/it/consumer/prod/guidelines.htm

8. Final remarks

Directive 2000/31 constitutes the main instrument for the regulation of all aspects of electronic commerce. Any subsequent measure adopted at Community or national level will have to follow the principles and solutions embedded in the Directive. This is due to its triple dimension:[182] it applies to any kind of activity (the horizontal nature of the Directive), it covers all the legal requirements (the co-ordinated field) and it regulates all the steps of the economic activity.

It constitutes a step forward in the process of European integration, as it introduces the application of the country of origin principle for completion of the Internal Market. Although the principle was present in other Community instruments such as the TV Without Frontiers Directive, with the Directive on electronic commerce it is the first time it has a general scope of application. This principle enables persons to provide their service in the whole Community territory just by complying with the legal requirements for the access and the pursuit of the activity in their country of establishment. Therefore, it is like providing services in their home market. Member States of destination cannot restrict the provision on any ground except for those established in Article 3(4). The Directive incorporates the ECJ case law into a legal text.

The country of origin principle is a Community mandatory rule, not a conflict of law rule. It does not derogate either from the Rome convention or any national conflict of law rule on non-contractual obligations. It obliges national judges to refrain from applying certain dispositions on the law determined by those conflict of law rules when they restrict the provision of the service. In contractual matters, the principle will not usually be applied in practice insofar as the law applicable to the contract will usually coincide with the law of the country of origin; this is otherwise in non-contractual matters. In this field, a uniform body of law will certainly help to enhance legal certainty although it is extremely difficult to satisfy the Internal Market objectives and the aims non-contractual rules try to protect.

Concerning the provisions harmonizing certain aspects of Information Society services, the increase in the level of consumer protection in the field of commercial communications and contract, justified by the special nature of the new media, should be noted. As commercial communications are essential for Information Society services, recent proposals are also based on the country of origin principle. Also, harmonization in the field of electronic contracts and intermediate service providers' liability must be welcome although further implementation on behalf of the Member States is needed in certain points: time and place of the conclusion of the contract; mechanisms to

182. Crabit, *supra* note 12.

remove or disable access to illegal information once service providers have actual knowledge of its existence.

Self-regulation can play an important role in the implementation of the Directive and in the enforcement of its provisions, especially in the fields of consumer contracts and content-regulation. The participants can create mechanisms to act rapidly to avoid the dissemination of harmful information and to service providers can adhere to code of conducts with the purpose of enhancing consumer confidence on electronic commerce. As far as the proposed new regulatory framework based on a mixed approach of the business-to-consumer transactions is concerned, the need to respect the existing legal framework decreases the relevance of this regulatory system.

Finally, insofar as the Directive on electronic commerce provides the consolidation of a common approach to the regulation of Information Society, it also reinforces EC strength in International forums. In such a way, the Directive certainly puts the Community in the way to become the most competitive and dynamic economy in the world.

Common Market Law Review 38: 1385–1420, 2001.

NATIONAL DOCTRINAL STRUCTURES AND EUROPEAN COMPANY LAW

HARALD HALBHUBER*

1. Introduction

When private lawyers try to understand how Community law affects their national legal systems, they first translate the relevant rules into their domestic doctrinal terms. National doctrinal structures thus mediate the impact of Community law on the private law systems of Member States. These structures filter European legal materials and determine their reception in domestic private law discourse. Given the diversity of the legal traditions of the Member States, this mediating effect goes to the heart of the project of Community law as a uniform legal order. More concrete, the question becomes whether Community law means the same for lawyers from different Member States. Company law will serve as an example for this interplay between national doctrinal structures and Community law.

Company law has recently attracted a lot of attention in the Community context.[1] This article will not try to contribute to the ongoing debate about the future of company law harmonization. By the same token, the article remains silent on the policy issue of whether, and to what extent, regulatory competition or harmonization of company laws are desirable.

Most importantly, the article expresses no view as to whether, as a policy matter, companies should be free to choose their State of incorporation and governing corporate law. Rather, it will explore the role national doctrinal structures have played in preventing freedom of incorporation in Europe. The article will develop this analysis as a case study, focusing on the reception of European legal materials in one country, Germany. Contributions from other Member States will also be discussed, but only as background and contrast rather than as additional fields of inquiry.

* Associate, Davis Polk & Wardwell, New York. I wish to thank Klaus Heine, David Kershaw, Roy Kreitner, Thomas McGuire, Chris Peters, Carlo Piscicelli, Michael Radasztics, Dan Squires, Matteo Tonello and Petra Vospernik for their patient readings and insightful comments. All views expressed are personal. The author welcomes comments by email to harald@halbhuber.com.

1. See recently Wouters, "European Company Law: Quo Vadis?", 37 CML Rev. (2000), 257 (providing an excellent survey of the literature).