Europe and the Internet: The Old World and the New Medium

Franz C. Mayer*

Abstract

With the Internet being more or less an American affair, the question arises as to whether its regulation has also to be dominated by the US. This article explores different European attempts at regulating the Internet, taking Germany, France and the EU as examples. At least two problems emerge: regulatory fragmentation between different European states and between the EU and its Member States, and the fact that traditional legislative mechanisms probably work too slowly to cope with the development of Cyberspace. In spite of these European efforts, the US (through 'indirect unilateralism') still dominates Internet governance. It has privileged access to the level of Cyberspace regulation where the technical architecture of Cyberspace is determined, as illustrated by the domain name system saga around ICANN (Internet Corporation for Assigned Names and Numbers). The conclusion is that, so far, Europeans have failed to shift the crucial issue of regulation of technical control over the Internet on to a truly international arena. The article acknowledges that it is not clear yet what a comprehensive international law approach to Internet governance could be like, but calls on international law to take up the issue of Internet governance and to take it seriously.

From the European perspective, the Internet is an American thing. The mere terminology 'Internet'[1] and 'Cyberspace'[2] suggests this, but it is not only the predominant language used in Cyberspace that hints at a 'special relationship' between the US and Cyberspace. There is more substantial evidence: the Internet was born in the US and the whole Internet architecture still has the marks of its origins as

* Dr jur., LL.M. (Yale). Walter Hallstein-Institute of European Constitutional Law, Humboldt University, Berlin. I am grateful for the numerous comments I received on earlier versions of the article. I wish to particularly thank Ben Rader and Gordon Geiser for their helpful questions and comments.

1 The Internet can loosely be described as the non-controllable net of nets without any central authority. The Internet is a worldwide, decentralized, more or less unlimited means of communication that allows all kinds of activities in a virtual Cyberspace.

2 The notion is attributed to W. Gibson, *Neuromancer* (1984).

the US Department of Defense's Arpanet.[3] Most of the relevant software for e-mailing and WWW-browsing originates in the US, thus reflecting a general US-American predominance in computer technology and operating systems. The World Wide Web concept developed by Tim Berners Lee at the CERN (European Laboratory for Particle Physics) in Geneva merely appears to be an exception to the rule.[4]

The Internet being an American-centred phenomenon, the question arises whether the regulation of the Internet or, more broadly, 'Internet governance'[5] automatically has to be more or less an American thing, too. Europeans hesitate. Official and less official statements stress the differences in values, choices and approaches to regulation between the old world and the US in general and in the respective attitudes towards Internet regulation in particular.[6] In the words of the French Conseil d'Etat: from a European perspective, engaging in an international debate about the regulation of the Internet is about preserving some of the old world's ideals of cultural diversity and human rights driven action in the context of globalization.[7] And it is about business, too.

What I am not going to do in this article is try to establish a European theory of international Cyberspace regulation. My purpose is more modest: it is to inform about European developments and views concerning Internet regulation related to international law. I begin by exploring European attempts at regulating the Internet. I will take the German and French examples and the attempts made at the level of the European Union to illustrate the kind of Internet regulation that Europeans engage in. My view is that in spite of those more or less successful European regulatory efforts, the US still dominates Internet governance. This is what the second part of this article is about, in which I will illustrate this claim by means of the domain name system saga.

[3] Of course, today the technical protocols are established through procedures that are not that directly linked to the US any more; for the specifics of those procedures see the references in F.C. Mayer, 'Recht und Cyberspace. Eine Einführung in einige rechtliche Aspekte des Internets' *Humborolt Forum Recht* 3 (1997) at IV, *http://www.rewi.hu-berlin.de/HFR/3–1997/*

[4] But again, the success story of the WWW is explained by US American inventions such as the browsers NCSA Mosaic or Netscape and search engines such as Yahoo or Altavista, see European Parliament (ed.), *Autoroutes européennes de l'information. Vers quelles normes?*, Document de travail (Série économique) W-18, at 14. Berners Lee moved to the US in 1994.

[5] I will use 'Internet governance' or 'regulation of the Internet' as umbrella terms related to the legal resolution of cyberlaw issues such as the protection of intellectual property and copyright infringements in Cyberspace; free speech; trading on the Internet (electronic commerce) and questions of electronic consumer protection and digital signature; encryption; taxation of electronic commerce; licensing; Internet broadcasting; competition; trade marks and domain names; identity in Cyberspace (electronic citizenship). Of course, most of those subjects are closely intertwined: encryption is a major issue in the context of electronic commerce, but it is also an important aspect of the construction of a Cyberspace identity, it may become a problem when it comes to content control, which in turn has to do with free speech and copyright issues and so on.

[6] A look at recent Internet regulation in the US seems to confirm this assessment, see Morrison, 'Sex, Lies and Taxes: New Internet Law in the United States' 41 *GYIL* (1998) 84.

[7] Conseil d'Etat, *Internet et les réseaux numériques* (1998) 14. For an English version of the report see *http://www.internet.gouv.fr/francais/textesref/rapce98/accueil.htm*

1 European Efforts to Regulate the Internet

This is not the place to give a detailed description of all the efforts made by all European countries to regulate the Internet in one way or another. I shall take Germany, France and the European Union as examples of European efforts to regulate the Internet.

Internet regulation does not start from a clean slate. Most legal problems related to Cyberspace already existed in the real world long before. Thus, most of these legal issues are already subject to regulation or can be, at least theoretically, legally resolved by deduction from existing rules:[8] distributing child pornography is illicit in most legal systems[9] no matter whether the seller uses a phone or the Internet; which legal regime governs a specific transnational electronic commerce transaction can be figured out by applying traditional conflict of law rules and so on. Efforts to regulate the Internet aim at improving and/or clarifying the existing legal regime governing Internet-related activities.

A *Germany*

The example of Germany illustrates that clarifying the legal situation is not that easy. In May 1998, Germany made the headlines in the context of Internet governance with the *CompuServe* trial at the Munich Lower Court.[10] The Munich court held *CompuServe* Germany's managing director Felix Somm responsible *inter alia* for making available prohibited content (child pornography on Internet newsgroups) to users and passed a suspended sentence of two years.

One of the numerous aspects of the decision is that it raised questions about the soundness of recent German Internet legislation, since the court, setting aside those newly enacted provisions, simply applied standard German criminal law to *CompuServe*. Most commentators agree that the judge in the *CompuServe* trial simply did not apply the Internet legislation properly to the case.[11] Still, the decision illustrates the problems and maybe the limits of efforts to regulate the Internet on the national level, possibly of Internet regulation in general.

[8] This view is contested by those who doubt whether the state can regulate Cyberspace at all, see Johnson and Post, 'Law and Borders — The Rise of Law in Cyberspace', 48 *Stanford Law Review* (1998) 1367. I skip the whole debate opposing regulation sceptics and regulation supporters. For a detailed account of this debate see Goldsmith, 'Against Cyberanarchy', 65 *University of Chicago Law Review* (1998) 1199 with further references.

[9] See for France Article 227–23 of the Criminal Code; for Germany § 184 III of the Criminal Code.

[10] Amtsgericht München 8340 Ds 465 Js 173158/95, 28 May 1998, *MMR* (1998) 429 and *NJW-CoR* (1998) 356. Cf. Hoeren, 'Ist Felix Somm ein Krimineller?', *NJW* (1998) 2792 and Kühne, 'Strafbarkeit der Zugangsvermittlung von pornographischen Informationen im Internet', *NJW* (1999) 188 with further references. Other spectacular cases related to Germany include the *Zündel* case on neo-Nazi material from Canada banned in Germany but made available on numerous servers *inter alia* in the US, and the *Radikal* case on material illicit under German law, available on a Dutch server, see *MMR* (1998) 93.

[11] Ladeur, 'Monitoring and Blocking Illegal Content on the Internet — a German and Comparative Law Perspective', 41 *GYIL* (1998) 55, 76 with further references. Even the prosecution finally pleaded not guilty, considering the control of newsgroups to be neither technically possible nor reasonable. Cf. also Sieber, 'Rechtliche Verantwortlichkeit im Internet', *MMR-Beilage* 2 (1999). Ulrich Sieber advised the

The relevant German Internet legislation of 1997 comprises Federal legislation on the 'new' media — the Federal Statute on Information and Communication Services (IuKDG)[12] with a Teleservices Statute (TDG)[13] — on the one hand, and the Mediaservices-Interstate-Agreement (MDStV),[14] concluded between the States (Länder) on the other hand.[15] The Federal Electronic Signature Act (Signaturgesetz) was also part of the IuKDG and was the first digital signature law worldwide to be enacted that covered the whole territory of a state.[16]

The guiding principle of the TDG and the MDStV is full liability for one's 'own' content (§§ 5 I TDG and MDStV) in accordance with the respective standard rules of criminal law, copyright law etc.; as far as 'other' content is concerned, liability for providing such content exists only to the extent that the content provider has positive knowledge[17] about the content and that it is technically possible and reasonable for him or her to block the dissemination of that content (§§5 II TDG and MDStV). There is no liability for simply providing access (§§ 5 III TDG and MDStV). The idea behind the TDG and the MDStV is probably best captured by the image of a legal filter that has to be passed through before other, regular liability principles of private or of criminal law apply.[18]

Federal Ministry on Research and the German Parliament on §5 TDG; he was also counsel to the defendant in the *CompuServe* trial. The *CompuServe* case is settled now, as the Court of Appeal (Landgericht München I) overruled the Lower Court on 17 November 1999, stating that Somm was not responsible for the content in question.

[12] Informations und Kommunikationsdienstegesetz of 22 July 1997, I *BGBl* (1870), for an English version see *http://www.iid.de/rahmen/iukdge.html*

[13] Teledienstegesetz. This statute is laid down in Article 1 of the IuKDG. The Federal Telecommunications Statute (TKG, Telekommunikationsgesetz, 25 July (1996), I *BGBl* 1120) regulates 'classic' telecommunications, in particular their technical aspects, see § 3 Nr. 16 and 17 TKG, the TDG focuses on content.

[14] Mediendienste-Staatsvertrag of 20 January/7 February 1997, see e.g. *GVBl Berlin* (1997) 360.

[15] Both sets of rules came into force on 1 August 1997. The twofold structure is explained by a classical federal-system quarrel about legislative competencies. As the same principles apply, a clear-cut distinction between media and teleservices is neither necessary nor practicable. The distinction between tele- and mediaservices on the one hand and traditional media such as the press or broadcasting on the other hand is more difficult, though. The distinction has a significant practical importance, as broadcasting is subject to licensing, see § 20 Broadcasting-Interstate-Agreement (RStV, Rundfunkstaatsvertrag, broadcasting without a licence can be fined up to 500,000 DM, § 49 II RStV). For questions of compatibility of the TDG and the MDStV with TRIPS and EU-regulation, cf. Sieber, *supra* note 11, at 4.

[16] The experimental character of that law is emphasized by the fact that the law was planned from the beginning to be subject to evaluation after a two-year testing period. For an intermediary assessment after the first two two years, cf. Roßnagel, 'Das Signaturgesetz nach zwei Jahren', *NJW* (1999) 1591. The official German government report of June 1999 assessing the German Internet legislation of 1997 is published as Bundestagsdrucksache 14/1191. For digital signatures in general, see Dumortier, *The Legal Aspects of Digital Signatures* (1999).

[17] For the problems of further defining knowledge see Ladeur, *supra* note 11, at 69. In particular in the context of criminal law, the strategy of prosecutors of issuing 'notifications' to providers indicating that there may be a problem with material accessible through the provider in question has left providers with doubts about their responsibilities, *ibid.*, note 69. The *CompuServe* case illustrates the uncertainties of those provisions: a notification of the Munich prosecutors had led the *CompuServe* manager to have newsgroups removed from the American server which then led the Munich court to argue that this proved that there was a technical possibility of blocking access.

[18] See Sieber, *supra* note 11, at 5.

The Munich *CompuServe* case indicates that the neat distinctions suggested by the law are not that easy to put into practice. Even if it was correct that the legal mechanisms of the TDG and the MDStV have not yet been understood by those who apply the law,[19] the problem remains that the dividing-line between 'own' content and 'other' content is still difficult to draw.[20] This is illustrated by the question of liability for hyperlinks.[21] The critics emphasize that the unclear standards of liability for providers constitute an 'incentive' for not making any effort to know about content, they point to the unresolved problem of the technical feasibility of control over content[22] and they complain about a terminology 'unsuited to the complexity of the problem'.[23]

As far as encryption is concerned, the Germans have been more hesitant and there has been no specific encryption legislation so far. Initially, the Federal Ministry of the Interior repeatedly called for restrictive legislation in that field.[24] On 2 June 1999, the Federal government adopted a cabinet position on the guidelines of German government encryption policy,[25] confirming that even in future, there will be no restrictions on the development, production, commercialization and use of encryption in Germany. In addition, the government strongly encouraged the use of encryption to secure communication and commercial transactions[26] and announced that even export restrictions would be reduced. The position of the government seems to be motivated by the potential of enormous damages due to electronic eavesdropping and manipulation of computer data. Of course, the central issue of the encryption debate remains unsolved: the government offers no solution to the obvious dilemma resulting from the antagonism between user protection and law enforcement requirements to get access to information under specific circumstances. At present, data security and privacy considerations outweigh law enforcement concerns.

To sum up, it may be said that the German approach is unilateral, ambitious, systematic and fairly comprehensive, but the proof of the pudding is in the eating, and there are indications that the regulatory objective of statutes such as the IuKDG,

[19] *Supra* note 11.

[20] See Bonin and Köster, 'Internet im Lichte neuer Gesetze', *ZUM* (1997) 821 at 825 about whether to set frames around somebody else's content leads to qualify this content as 'own' content of the user setting frames.

[21] For details, see Sieber, *supra* note 11, at 13 *et seq*. For further references on the problem of links cf. Ladeur, *supra* note 11, at 67 note 47.

[22] Ladeur, *ibid.* at 69 *et seq*.

[23] *Ibid.* at 76.

[24] See 'Der Briefkasten bleibt zu', *Die Tageszeitung*, 10 June 1999, at 13. The US until recently maintained a restrictive approach and limited the exportation of strong encryption products such as PGP for national security reasons. The US Bureau of Export Administration (BXA) issued new encryption export regulations much less restrictive in January 2000, see *http://www.eff.org*

[25] See the joint press release of the Federal Ministries of the Interior and for Economic Affairs and Technology of 2 June 1999, *http://www.bmwi.de/presse/1999/0602prm1.html*

[26] The Federal Ministries of the Interior and for Economic Affairs and Technology have set up a website that contains a broad variety of information on encryption, including links to additional sources of information, *http://www.sicherheit-im-internet.de*

which is to establish legal certainty, has not been achieved. The approach adopted with regard to encryption appears to be more careful.

B *France*

France should have been well prepared for the Internet, having known since the beginning of the 1980s a mass-computer phenomenon in some ways similar to the Internet: the Minitel system, which already presented the problems of content control, copyright, identity/domain name control and all the rest.[27] The difference between the Internet and Minitel, though, is that Minitel has always been a system rooted in France and limited to French territory through its specific link to the French telephone system, very unlike the boundary transcending Internet.

Consequently, in some fields related to the Internet, the French regulatory reaction to the Internet — after a phase of passivity — was as if it was still about a traditional nationally controllable means of communication. This is particularly visible in the French approach to encryption. Initially, French encryption regulation was quite strict.[28] The French law distinguished between electronic signature functions and authentification on the one hand and confidentiality questions on the other hand. Encryption, belonging to the latter, was restricted to a key length of 40 bits. This level of encryption can be broken with several computers working simultaneously for a couple of hours.[29] Selling, importing and exporting stronger encryption (key length over 40 bits) was subject to authorization, its use was also restricted. The French have now given up this restrictive approach to encryption. In March 1999, for most operations, the unrestricted key length was raised to 128 bits,[30] and the authorization requirement was replaced by a mere declaration requirement.[31] The unrestricted use of encryption is about to follow.[32]

The restrictive encryption regulation is hardly representative of the French attitude towards Internet regulation, though. There is evidence that the French are willing to

[27] Minitel allows communication and electronic commerce, though at a — by Internet standards — ridiculously low data transmission rate. For the Minitel experience, see Rheingold, *The Virtual Community* (1983), at 220 *et seq.*

[28] The relevant law is Article 28 of the Statute 90–1170 of 29 December 1990 and the Implementation Decrees 98–101 of 24 December 1998 and 98–206 of 23 March 1998. For details, see Conseil d'Etat, *supra* note 7, at 97 *et seq.*

[29] For the specifics of key lengths and encryption problems, see Froomkin, 'The Metaphor is the Key: Cryptography, the Clipper Chip and the Constitution', 143 *University of Pennsylvania Law Review* (1995) 595; cf. also the references in Marauhn, 'Sicherheit in der Kommunikationstechnik durch legislatives Risikomanagement', *KritV* (1999) 57. For the international dimension of encryption policies, cf. also the statement of 3 December 1998 issued in the context of the Wassenaar Arrangement, *http://www.wassenaar.org/docs/docindex.html*

[30] Decree 99–200 of 17 March 1999.

[31] Decree 99–199 of 17 March 1999.

[32] See the speech of French Prime Minister Lionel Jospin in August 1999, Société de l'information: discours du Premier ministre à l'Université d'été de la communication, 26 August 1999, *http://www.premier-ministre.gouv.fr/PM/D260899.html.* For details see Féral-Schuhl, *Cyberdroit. Le droit à l'épreuve de l'internet* (1999) at 174 *et seq.*

engage in international cooperation in that respect. A distinctive element of the French approach is that there have been impressive official studies on the different options for Internet regulation: the Inter-ministerial Falque-Pierrotin report of 1996[33] and the Conseil d'Etat report of 1998[34] have brought together government and non-government expertise in order to formulate recommendations on how to regulate the Internet, they are also evidence of a realistic and open view on the Internet. Both reports emphasize to a significant extent the necessity of international regulation.

In the field of data protection, the French Conseil d'Etat, in its 1998 report, suggested the combination of elements of autoregulation with an international treaty, which would define, on a worldwide level, a minimum of data protection principles and which could provide for a cooperation among states in the prosecution of violations.[35] As far as electronic commerce and consumer protection are concerned, the Conseil d'Etat suggests a strengthening of — so far insufficient — international consumer protection standards[36] and suggests an international treaty on electronic transactions and consumer protection.[37] As to other issues that have been subject to debate not only in France, such as the taxation of electronic commerce (VAT, direct taxes and tariffs), the Conseil d'Etat concludes that any merely national effort would be doomed and recommends a concerted European/international effort in the context of the European Union (direct taxes), the OECD (indirect taxes) and the WTO (tariffs).[38] The Conseil d'Etat also recommends international cooperation (WIPO, WTO, OECD) on the issue of copyright protection.[39]

There is even more evidence of French efforts to reach international solutions to Internet-related regulatory problems: concerning the issue of content control, France suggested a charter on content at the OECD level in September 1996. This effort, considered to be 'étatiste' by some, may be viewed as being directed against a US approach, which is suspected of being too half-hearted towards any international cooperation that threatens to become mandatory.[40]

Compared to Germany, so far France has been more hesitant about engaging in large-scale national Internet legislation. One way to interpret the passive French attitude is that it is evidence of an understanding that (European) unilateral national governmental regulation will have only limited effects on the Internet and that, therefore, international cooperation is necessary. There is another explanation, of course, which is simply that France has had to accept the superiority of the Internet over Minitel and to get acquainted to the Internet.

[33] Internet. Enjeux juridiques, Rapport au ministre délégué à la Poste, aux Télécommunications et à l'Espace et au ministre de la Culture, Paris 1997. See *http://www.telecom.gouv.fr/francais.htm*

[34] *Supra* note 7. For additional studies in France, see Féral-Schuhl, *supra* note 32, at 261.

[35] See Conseil d'Etat, *supra* note 7, at 44.

[36] The Conseil d'Etat refers to the Hague Convention of 1955 and the Rome Convention of 1980 (Convention on the law applicable to contractual obligations, OJ 1980 L 266/1).

[37] See Conseil d'Etat, *supra* note 7, at 72 *et seq.*

[38] *Ibid.* at 109.

[39] *Ibid.* at 165.

[40] *Ibid.* at 206.

C *European Union*

Most of the efforts on a Europe-wide level correspond to efforts made at the level of the European Union. Again, it all started somewhere in the 1990s, when the Internet became a mass phenomenon. The standard approach at the EU level, so far, has been to regulate specific aspects of the Internet related to the mainly economic[41] fields of European integration.

The earlier regulatory efforts were not specifically aimed at the Internet but were more general efforts to regulate multimedia activity.[42] Those efforts became more and more Internet specific during the second part of the 1990s:[43] the recent draft directives on digital signature and on electronic commerce probably contain the most specific Internet rules issued by the EU and as such they are worth a closer look.

1 Digital Signature

Facing increased legislative activity in the area of digital signature and encryption,[44] the Commission detected a need for a harmonized legal framework at the European level in order to avoid the development of obstacles to the functioning of the Internal

[41] Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data (OJ 1995 L 281/31) may be a typical example. The directive states that the free movement of data is closely related to the free movement of goods and services and that data are goods requiring specific protection. The directive is closely linked to the Internet as the Internet is probably today's most important sector for data transfer. On the EDI foundations of Community activity in the field of electronic commerce see J. Dickie, *Internet and Electronic Commerce Law in the European Union* (1999) 3 *et seq.* The Commission Green Paper on 'The Protection of Minors and Human Dignity' (COM (96) 483) published in October 1996 together with a communication concerning illegal content on the Internet is one of the few documents focusing on non-economic issues. Cf. also the Council resolution of 17 February 1997, OJ 1997 C 70 and the recommendation of the Council on the protection of minors and human dignity, pointing to autoregulation, of 24 September 1998, 98/560/EC most recently the draft resolution concerning child pornography on the Internet, OJ 1999 C 362/8 *et seq.*

[42] See Directive 89/522/EEC of 3 October 1989, modified in 1997, 'Television without Frontiers' (OJ 1989 L 298/23; modified by Directive 97/36/EC, OJ 1997 L 202/60). Another example is the 1997 Bangemann report, published as a Commission Green book (COM (97) 623), dealing with the convergence of the different media. In that context, cf. also Grewlich, '"Cyberspace": Sector-specific Regulation and Competition Rules in European Telecommunications', 36 *CML Rev.* (1999) 937.

[43] For directives not directly aimed at the Internet but having strong impact on Internet governance see Directive 97/7/EC of 20 May 1997 on the protection of consumers in respect of distance contracts (OJ 1997 L 144/19) with financial services being subject to a special directive (COM (98) 468); cf. also the draft directive on copyright protection (COM (97) 628); Directive 96/9/EC of 11 March 1996 on the legal protection of databases (OJ 1996 L 77/20); Directive 98/84/EC on conditional access systems (OJ 1998 L 320/54); Directive 98/34/EC (OJ 1998 L 204/37) and Directive 98/48/EC (OJ 1998 L 217/18) aim at preventing regulatory fragmentation in the field of information society services through a mechanism that requires Member States to inform the Commission about any national regulation that concerns information society services.

[44] See *supra* the German Signaturgesetz included in the IuKDG. The Explanatory Memorandum of the Commission indicates that at the time of the Commission proposal, legislative activities related to electronic signatures existed in Austria, Belgium, Denmark, France, Finland, Germany, Italy, the Netherlands, Spain, Sweden and the United Kingdom.

Market in 1997. The approach chosen[45] included posterior authorization, voluntary accreditation schemes, a focus on the essential requirements for certification service providers, including their liability. The Commission emphasized the need to take into account ongoing developments at the international level such as the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce and subsequent work aimed at the preparation of uniform rules on digital signatures,[46] OECD work following the 1997 Guidelines for Cryptography Policy and WTO activities.

The Commission draft is an example of how Internet regulation in Europe should not work: the same month the German statute on digital signatures came into force, the Commission published its proposal for the regulation of digital signatures on the European level, suggesting a regulatory approach at least initially not fully compatible with the German approach.[47]

2 Electronic Commerce

The issue of electronic commerce[48] led to one of the most important and probably also most ambitious efforts of the European Commission to regulate the Internet. After its electronic commerce communication 'A European Initiative in Electronic Commerce' of April 1997,[49] the Commission put forward a proposal for a directive on electronic commerce in November 1998,[50] aiming at establishing 'a coherent legal framework for the development of electronic commerce within the Single Market'.[51]

The country-of-origin principle as an established principle of EC law is the leading principle of the draft directive. Generally speaking, it is applied when harmonization of rules is either not feasible or not desired. The risk of this approach is always a de facto harmonization on the regulatory level of the Member State that imposes the least restricting legal requirements on an activity.

The directive would apply only to service providers established within the EU. Services covered by the directive would be business to business and business to consumer services, services provided free of charge to the recipient, e.g. funded by advertising or sponsorship revenue and services allowing for online electronic transactions such as interactive teleshopping of goods and services and online

[45] OJ 1998 C 325/5 *et seq.*; cf. also Brisch, 'Gemeinsame Rahmenbedingungen für elektronische Signaturen', *CR* (1998) 492; Schumacher, 'Digitale Signaturen in Deutschland, Europa und den U.S.A.', *CR* (1998) 758. The directive is now adopted: Directive 1999/93/EC of 13 December 1999, OJ 2000 L 13/12 *et seq.*

[46] Draft rules on electronic signatures have been published in November 1998, see *http://www.un.or.at/uncitral/english/session/wg–ec/wp-79.htm*

[47] For details, see Roßnagel, *supra* note 16, at 1592. After some modifications the draft directive came closer to the German approach, *ibid.* at 1593. According to the German government report of June 1999 assessing the German Internet legislation of 1997, there will be no need for 'essential modifications' to the German legislation because of the directive, cf. *supra* note 17, at 20.

[48] For a general overview on electronic commerce, see Stoll and Goller, 'Electronic Commerce and the Internet', 41 *GYIL* (1998) 128.

[49] COM (97) 157.

[50] COM (98) 586, see OJ 1999 C 30/4.

[51] Press release DG XV, available at *http://www.europa.eu.int/comm/dg15/en/media/eleccomm/999.htm*

shopping malls. Examples of sectors and activities include online newspapers, online databases, online financial services, online professional services (lawyers, doctors, accountants, estate agents), online entertainment services such as video on demand, online direct marketing and advertising and services providing access to the WWW.

The draft defines the place of establishment in line with the principles established for Article 43 (ex 52) ECT[52] as the place where the operator actually pursues an economic activity through a fixed establishment, irrespective of where websites or servers are situated or where the operator may have a mail box. The aim of those provisions is to remove legal uncertainty and to ensure that operators cannot evade supervision, as they would be subject to supervision in the Member State where they are established. In addition, information service providers are obliged to make available to customers and competent authorities basic information in an easily accessible manner and in a permanent form concerning their activities (name, address, e-mail address, trade register number, professional authorization and membership of professional bodies where applicable, VAT number).

The draft requires Member States to adjust national legislation with a view to removing any prohibitions or restrictions on the use of electronic media for concluding contracts. As far as service providers who transmit or store information from third parties are concerned ('intermediaries'), the draft directive wants to establish legal certainty through an exemption from liability for intermediaries who only play a passive role as 'mere conduits' for information from third parties. It also limits liability for 'intermediary' activities such as the storage of information.

Control in the country of origin being the guiding principle, the proposed directive would still allow Member States, on a case-by-case basis, to impose restrictions, if necessary to protect the public interest on a number of specified enumerated grounds, in following a specific procedure.

The European Parliament called on the Commission to alter its proposal and suggested a number of amendments to the proposal in May 1999.[53] The Commission issued a revised draft on 1 September 1999,[54] incorporating most of the amendments suggested by the European Parliament without giving up the main orientations of the proposal.

The critiques of the Commission proposal are too numerous to be explored here in detail.[55] They concern the overly narrow definitions of the draft directive: excluding

[52] See Case C-221/89, *Factortame* [1991] ECR I-3905.

[53] See European Parliament Legislative resolution of 6 May 1999, A-4–0248/99.

[54] COM (1999) 427 final.

[55] See for example the German debate about the e-commerce draft directive: Waldenberger, 'Electronic Commerce: der Richtlinienvorschlag der EG-Kommission', *EuZW* (1999) 296; Brisch, 'EU-Richtlinienvorschlag zum elektronischen Geschäftsverkehr', *CR* (1999) 235; Hoeren, 'Vorschlag für eine EU-Richtlinie über E-Commerce', *MMR* (1999) 192; Lehmann, 'Rechtsgeschäftliche Verantwortlichkeit im Netz — Der Richtlinienvorschlag der EU-Kommission', *ZUM* (1999) 180; Maennel, 'Elektronischer Geschäftsverkehr ohne Grenzen — der Richtlinienvorschlag der Europäischen Kommission', *MMR* (1999) 187; Spindler, 'Verantwortlichkeit von Diensteanbietern nach dem Vorschlag einer E-commerce-Richtlinie', *MMR* (1999) 199. Cf. also Dickie, *supra* note 41, at 101 *et seq.*

Internet radios and push-services;[56] the silence on the hotly debated liability for hyperlinks and search engines;[57] the unclear reach of the country of origin principle[58] and the role of the Rome Convention: the reference to the legal situation in the country of origin is considered unclear insofar as the draft directive is silent on whether this implies the respective municipal conflict-of-law rules, which could bring an activity under a different legal regime than the one of the country of origin.[59] Some German authors are unhappy about the range-of-liability exemptions, which go beyond the German legislation:[60] this concerns caching and hosting, where the notion of knowledge applies not only to the content but also to the illegality of the content, privileging providers who do not care about the content; it also goes for the fact that the draft directive does not limit reduced liability to 'other' content as German legislation does. A more general German critique concerns the 'American-style' legislation technique.[61] It has also been pointed out that the transparency requirements do not specify in what language information has to be provided;[62] this touches one of the core problems of Internet regulation. Finally, as is also true of the German TDG,[63] incompatibilities with Article 45 TRIPS could occur as far as liability for copyright infringements is concerned, if Article 45 I TRIPS imposes liability for mere negligence, since the draft directive links liability to positive knowledge.[64]

A more general critique is that the approach taken contributes to the number and complexity of EU instruments applicable to electronic commerce instead of assembling the relevant EC provisions into one code.[65] Although the directive has a sound basis of legislative competence in Article 47 (ex 57), 55 (ex 66) and 95 (ex 100a) ECT, its adoption and implementation may encounter fierce resistance beyond the current debate because of its arguably unprecedented effects on core Member State law such as criminal and contract law.[66]

The amended proposal for a directive has to be adopted by the European Parliament and the Council of Ministers under the co-decision procedure. Observers are sceptical

[56] Waldenberger, *ibid.* at 296.

[57] Spindler, *ibid.* at 204.

[58] Waldenberger, *supra* note 55, at 298.

[59] For a more elaborate reflection on this weak point of the draft directive see Hoeren, *supra* note 55, at 195.

[60] Spindler, *supra* note 55, at 202.

[61] Waldenberger, *supra* note 55, at 302.

[62] Hoeren, *supra* note 55, at 197.

[63] Lehmann, 'Unvereinbarkeit des §5 Teledienstegesetz mit Völkerrecht und Europarecht', *CR* (1998) 232, at 233 *et seq.*

[64] Spindler, *supra* note 55, at 205 with further references.

[65] Dickie, *supra* note 41, *passim*. For Commission efforts to reduce the number of relevant instruments, see the new framework for electronic communications suggested by the Commission in a Communication issued in November 1999, *http://europa.eu.int/comm/dg13/electrocomm.htm* at 6.

[66] See Spindler, *supra* note 55, at 200, for a more detailed analysis of the implications for Member State criminal law. The Commission proposals for determining the moment of conclusion of an electronic contract appear incoherent from a German private law perspective. For the issue of *ultra vires* acts in the European Union in general, see F.C. Mayer, 'Kompetenzüberschreitung und Letztentscheidung', forthcoming.

whether an agreement on e-commerce legislation will be reached in the near future.[67] Such a delay would support those critics who consider the legislative procedures at the EU level to be too slow for the pace of change in the electronic marketplace.[68]

What is of particular relevance in the present context is the fact that the draft directive poses a serious problem for the German legislator, as huge parts of the IuKDG and the MDStV would have to be rewritten if the draft came into force:[69] this concerns the country-of-origin principle, the transparency and information requirements and the provisions dealing with electronic contracts as well as the German distinction between media and teleservices, which are not part of the EU draft.

D *Conclusions*

Of course, a rough sketch of the German, French and EU efforts can barely give a full picture of the broad variety of efforts dealing with numerous issues linked to Cyberspace governance in Europe. From what I have outlined, one might get the impression that European regulatory efforts resemble a system of trial and error, that they are too isolated, limited to an economic rationale and that they show inconsistencies with the respective higher legal provisions. The German and the EU experience may also support the claim that a traditional legislation machinery with parliaments and bureaucracies works too slowly to capture the development of Cyberspace.

A more optimistic assessment would emphasize the efforts to reach legal certainty, the willingness of Europeans to engage in international cooperation where necessary and to attribute a role in Internet governance to the private sector.[70] The optimistic view would not attribute deficiencies of unilateral Internet regulation to structural obstacles to regulate the Internet unilaterally, but to incompetent judges, unclear wording and similar 'technical' problems of legislation. It would underline that at this initial stage of Internet regulation, legislation is not about a perfect and 'future-proof'[71] legal framework, but rather about exploring the ground.

However, even without going further into the details of the regulatory efforts that I have just mentioned or which exist in other European countries, it seems fair to say — here I get back to my initial question of whether Internet governance is American-

[67] Chapman, 'No Deal in Sight on E-commerce: Rulebook to Drag On', *European Voice*, 9 September 1999, *http://www.european-voice.com*. The Council has reached a common position on 7 December 1999, see *http://www.europa.eu.int/comm/dg15/en/medie/eleccomm/99-952.htm*

[68] See Dickie, *supra* note 41, *passim*. As directives must be implemented into Member-State law, the relevant law will remain fragmented (between the European level and the Member-State level), anyway.

[69] Hoeren, *supra* note 55, at 199. The German government report of June 1999 assessing the German Internet legislation of 1997, *supra* note 16, at 28, is less pessimistic, but admits that changes to the German legislation will be necessary, *ibid.*, at 32.

[70] For this aspect of Cyberspace governance see Article 16 of the EU draft directive on electronic commerce, *supra* note 50. For the view of the industries concerned see Bertelsmann Foundation (ed.), *Self-regulation of Internet Content* (1999), *http://www.stiftung.bertelsmann.de/internetcontent/*

[71] This notion is used by Dickie, *supra* note 41, at 40, note 20.

centred — that Europeans do not seem to leave Internet regulation entirely to the US. They are trying on their own.

2 Internet Governance in Fact Is an American Thing

The US participates, of course, in international negotiations about Internet governance. Still, Europeans suspect that public and private interests in the US are aiming at structuring the use of and the behaviour in the digital networks along American lines, which is associated with a purely economic rationale.[72] This may be true and some elements of the regulatory approach taken by the US seem to confirm this assessment.

Let me explain. One way to illustrate the regulatory approach taken by the US is to think of Cyberspace as a road system, very much in line with the notorious 'information super highway' metaphor. Now, if we want to prevent, say, heavy trucks from circulating on our roads, there are basically two options: we can set up traffic signs, prohibiting heavy trucks from using those roads, or we can build roads or bridges too narrow for heavy trucks, which will also prevent trucks from using our roads. The European regulatory efforts that I outlined correspond to the traffic sign approach. We find this type of regulation in the US as well; recent examples include the Communications Decency Act of 1996[73] or the Digital Millennium Copyright Act of 1998.[74] The difference between the US and Europe is that the US also has privileged access to the other level of regulation of Cyberspace, the 'road-construction level' where the technical preconditions of Cyberspace are laid down.

Unlike most other regulatory situations in the real world, Cyberspace is a merely technical construct. This is illustrated by the fact that censors have turned to technical means to control net access in most of the 45 countries[75] that restrict access to the Internet: there, technical control can mean no access to the Internet at all (e.g. North Korea, Iraq, Libya[76]), a combination of government monopoly over servers and the use of filter technologies (e.g. Belarus, Sudan[77]) or hardware control through the mandatory registration of Internet computers (China[78]).

Without the technical norms 'creating' the Internet, there would be no Cyberspace. Hence the technical standards are crucial, and they imply policy choices. There is a widespread misunderstanding that, basically, the Internet is not subject to any regulation at all and that it constitutes some kind of 'cyber-anarchy'. This image is wrong.[79] Not only do all kinds of informal (netiquette) and formal rules (provider

[72] See Conseil d'Etat, *supra* note 7, at 13 *et seq.*

[73] 47 USC § 223; cf. *Reno v. American Civil Liberties Union*, 521 US 844, 117 S.Ct 2329 (1997) for the invalidation of parts of the CDA.

[74] 112 Stat. 2860.

[75] I refer to a survey issued by Reporters sans frontières, 'Les Vingt Ennemis d'Internet', Communiqué de presse, 9 August 1999, *http://www.rsf.fr/alaune/ennemisweb.html*

[76] *Ibid.*

[77] *Ibid.*

[78] *Ibid.*

[79] For a more detailed account, cf. F.C. Mayer, 'Recht und Cyberspace', *NJW* (1996) 1782, at 1789 *et seq.*

contracts) impose a particular way of behaviour in Cyberspace. What is more important is that there are numerous protocols and standards that lay down the technical elements of the Internet which structure and limit one's 'experience of Cyberspace':[80] to begin with, it is the technical architecture of Cyberspace that can be used to control access to Cyberspace or at least to specific Cyberspace communities.[81] I believe, however, that the 'road-construction-level' of Internet regulation is not limited to an access/no access dichotomy. Specific encryption, electronic signature, firewall and filtering programmes for newsgroups, e-mail and web-pages may or may not be supported by the technical architecture of Cyberspace, which allows a wide range of regulatory options to implement policy choices.[82]

In addition, technical standards mirror cultural preferences: only think of the language standards of the Internet which are founded on the ISO 8859 standard, a polycultural approach which has no equivalent in the monocultural American TCP/IP world.[83]

So the crucial question is: who is to set those technical standards? There is the Internet Society (ISOC), hosting the organizations responsible for the Internet infrastructure; the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB).[84] ISOC has individual and organizational members from all over the world and is based in the US. One of the missions of ISOC is to promote an 'Internet culture' that fosters effective self-governance based on broad consensus.[85] And, since 1998, there is an entity called Internet Corporation for Assigned Names and Numbers which has been attributed the responsibility for the domain name system (DNS). Nobody will get far in Cyberspace without the proper Cyberspace identity, the domain name, to begin with. Attributing a Cyberspace identity is, in some ways, like attributing citizenship. Thus, the quarrel about the control over Internet domain names, which I will use to illustrate my point about US control over the Internet, has to do with crucial issues of Internet governance.

Domain names (the easy-to-remember names for Internet addresses such as *www.ejil.org*) and the corresponding unique Internet Protocol numbers of each Internet computer (e.g. 141.20.18.6) serving as routing addresses on the Internet are required for transmission of information via the Internet.[86] The domain name system

[80] Goldsmith, *supra* note 8, at 1213. See Lessig, *Code and Other Laws of Cyberspace* (1999), on how the architecture of Cyberspace is shaped by interests.

[81] *Ibid.*, cf. also the examples given in the RSF report, *supra* note 75.

[82] Allegations published in September 1999 that Microsoft's encryption framework in the Windows operating system contains a 'backdoor' key for the US National Security Agency (see *http://www.cryptonym.com/hottopics/msft-nsa.html*) illustrate how technical architecture, in that case on the level of an operating system, could support policy choices.

[83] European Parliament (ed.), *supra* note 4, at 38. For the effects of the current Internet language standards on the German language, see Dougherty, 'Sprechen Sie Internet Deutsch?', *WiredNews*, *http://www.wired.com/news/news/culture/story/21752.html*; Runkehl *et al.*, *Sprache und Kommunikation im Internet* (1998).

[84] *http://www.ietf.org* and *http://www.iab.org*

[85] *http://www.isoc.org/isoc/mission/*

[86] For details, see *RFC* 1034 and *RFC* 1035 with further references, *http://www.rfc-editor.org/rfc.html*

is divided into top-level domains (TLDs) and second level domains. Besides the country-code TLDs (ccTLDs) such as .de (Germany) or .fr (France), there is a small set of generic top level domains (gTLDs) without any national identifier but denoting a specific activity: .com for commercial users, .org for non-profit organizations, .net for network service providers etc.

In the early days of Cyberspace, the list of all hostnames was managed by one person, Jon Postel, then at the UCLA. Later, it was the Internet Assigned Numbers Authority (IANA),[87] headed by the same Jon Postel, under contract with the US government agency DARPA,[88] that allocated blocks of numerical addresses to regional IP registries such as RIPE in Europe. As of 1992, the registration, subject to a fee, of gTLDs .com, .org and .net was performed by Network Solutions, Inc. (NSI), a Virginia-based company under contract with NSF.[89] That contract expired on 30 September 1998.

Following a Presidential directive,[90] the US government issued a Green Paper under the title 'A Proposal to Improve Technical Management of Internet Names and Addresses' in January 1998.[91] The government estimated that there was a need for change for a couple of reasons, including widespread dissatisfaction about the absence of competition in domain name registration; a lack of mechanisms for resolving conflicts between trademark holders and domain name holders; the call of commercial interests for a more formal and robust structure of the domain name system; an increasing percentage of Internet users outside the US claiming a larger voice in Internet coordination and the transformation of the Internet into a more commercial medium for which the funding of US research agencies such as NSF and DARPA was considered inappropriate.

The proposal outlined in the Green Paper was to set up a private non-profit corporation incorporated under US law, responsible for the coordinated maintenance and dissemination of the protocol parameters for Internet addressing. The response to the Green Paper by the European Commission and the Council[92] dated 16 March 1998,[93] addressed to the US government on behalf of the European Community and its Member States, outlined the concerns of the Europeans: according to this letter, the future management of the Internet should take into consideration the fact that it is

[87] *http://www.iana.org*

[88] Defense Advanced Research Projects Agency.

[89] National Science Foundation.

[90] Presidential Memorandum on Electronic Commerce, 33 *Weekly Comp. Presidential Documents* 1006, 1 July 1997. The initiative to issue this directive is attributed to Presidential advisor Ira Magaziner, see 'Clinton Guru Ira Magaziner is Making D.C. Net-Savy', *Time*, 28 September 1998, at 48 and Siegele, 'Verfassungsvater des Cyberspace', *Die Zeit*, 13 August 1998, at 8.

[91] *http://www.ntia.doc.gov/ntiahome/domainname/dnsdrft.htm*

[92] At that point, the European Commission called for an international instrument defining the powers and responsibilities of international self-regulatory bodies and codifying the conditions under which public authorities would refrain from corresponding activities, see International Policy Issues Related to Internet Governance, Communication to the Council from the Commission, 20 February 1998, *http://www.ispo.cec.be/eif/policy/governance.html*

[93] *http://www.ispo.cec.be/eif/policy/govreply.html*

already a global communications medium and thus the subject of 'valid international interest'. The EU requested to be admitted to enter into full consultations with the US before certain features of the US proposals are implemented, as agreed upon in a joint EU–US statement on electronic commerce dated 5 December 1997. The Europeans expressed their belief that the future of the Internet has to be agreed upon within an international framework. They pointed to the fact that the proposal has the potential for consolidating permanent US jurisdiction over the Internet as a whole, including dispute resolution and trademarks used on the Internet. The position of the Europeans was that the European Union and its Member States and the rest of the world should be allowed to participate fully in the decisions that will determine the 'future international governance of the Internet'. They recommended that the US government limit its direct regulatory intervention in the Internet only to those relationships which fall clearly under existing contracts between US government agencies and their contractors and that all other decisions be referred to 'an appropriate internationally constituted and representative body'.

On 5 June 1998, the US government issued the revised version of the Green Paper as a White Paper entitled 'Management of Internet Names and Addresses'.[94] The core elements of the Green Paper remained unchanged. This time, the European reaction was less clear. The European Commission found that the White Paper did respond to a large extent to the comments and criticisms put forward by the EU and others and recommended that the EU should fully participate in the organization and management of the Internet that has been launched by the White Paper.[95] The Commission stated that the US White Paper recognizes that an US-centric approach is 'increasingly' outdated and stressed that 'there is now an opportunity for European and other international interests to take up the challenge to participate fully in the next phase of Internet development'. It admitted, though, that the effect of incorporating the new Corporation under US law has yet to be assessed[96] and several times emphasized the need for a multilateral process.

The French position seems to be an example of a more manifest European rejection of the White Paper. The French[97] favour the approach on the domain name issue formulated by an International Ad Hoc Committee (IAHC) in a report of February 1997.[98] The IAHC was set up by the IANA and the ISOC and included institutions such as the International Telecommunications Union (ITU) and the WIPO. In its report, the IAHC adopted the view that the Internet top level domain space was a public resource, subject to the public trust, and that any administration, use and/or evolution of the Internet TLD space constituted a public policy issue. The proposal of

[94] 63 Fed. Reg. 31741 (1998), *http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm*

[95] Internet Governance, Management of Internet Names and Addresses, Analysis and Assessment from the European Commission of the United States Department of Commerce White Paper, Communication from the European Commission to the European Parliament and to the Council, 29 July 1998, COM (1998) 476, *http://158.169.51.200/eif/dns/com98476.html*

[96] *Ibid.*, point 3.

[97] I refer to the French Conseil d'Etat's 1998 report, *supra* note 7.

[98] *http://www.iahc.org/txt/draft-iahc-recommend-00.txt*

the IAHC attributed a significant role to international organizations such as the ITU and the WIPO.

In October 1998, during what has been referred to as the 'constitutional convention of the Internet',[99] the creation of the Internet Corporation for Assigned Names and Numbers (ICANN)[100] constituted the first step towards an implementation of the White Paper.[101]

ICANN is a private non-profit organization, incorporated under Californian law. No government officials or officials of a multinational entity or treaty organization may serve on the ICANN board.[102] ICANN is responsible for the control of the domain name system, the distribution of the IP addresses, the development of new standards for Internet protocols and the organization of the root-server-system of the Internet.[103] That ICANN will also have the final say over the ccTLDs may be of particular interest for international lawyers.[104] What is crucial to understand is that ICANN's scope of action is not limited to domain name issues, it also reaches into the realm of general technical standards and protocols of the Internet.

The first steps of ICANN were far from successful: in June 1999, ICANN triggered harsh criticism which led to US House of Representatives hearings over the charge of levying an illegal Internet tax by suggesting a fee for domain name and IP address registrations, intended to cover the non profit ICANN's costs.[105] From a European perspective, the main problem[106] with ICANN is not really its private character or a US

[99] Kaplan, 'A Kind of Constitutional Convention for the Internet', *New York Times, Cyber Law Journal*, 23 October 1998, the notion of 'constitutional convention of the Internet' is attributed to Professor David Post.

[100] *http://www.icann.org*

[101] It was only after some alterations of the initial bylaws, though, that the US Department of Commerce finally accepted ICANN as the company that will help to shift the management of the DNS to the private sector as outlined in the White Paper, following the principles of stability, competition, private bottom-up coordination and representation. See the Memorandum of Understanding between the US Department of Commerce and Internet Corporation for Assigned Names and Numbers of 25 November 1998 at *http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm*

[102] Art. VII s. 5 of the bylaws.

[103] There are 13 root servers around the world, half of which belong to agencies or research partners of the US government. Nine root servers are located in the US. In Europe, there are two root servers (London and in Stockholm). The databases of those root servers are synchronized with NCI's master root server database.

[104] Think of the admission of a ccTLD for, say, Kosovo or for other territories that claim independence. For most country names, the IANA referred to the ISO 3166 standard, see *http://www.din.de/gremien/nas/nabd/iso3166ma/internet.html*

[105] See McCullagh, 'Domain Players Face the Music', *Wired News*, 24 July 1999, *http://www.wired.com/news/news/politics/story/20887.html*

[106] For general criticism of ICANN, see *http://www.icannwatch.com*

domination of the board.[107] It is one of ICANN's tasks to represent the interests of the worldwide Internet community. Thus, ICANN is internationally oriented. The bylaws provide for geographic diversity of the members of the board,[108] although the geographic regions as defined in the bylaws — Europe; Asia/Australia/Pacific; Latin America/Caribbean Islands; Africa; North America — appear somewhat arbitrary: which group will Russia, for example belong to? ICANN's work will also be decentralized; the bylaws provide that there will be supporting organizations for addressing, for protocols and for name registration.

The real problem is that ICANN is incorporated under Californian law and remains under the shadow of US jurisdiction. In the categories of multilateralism and unilateralism, this configuration could be called indirect unilateralism. It has been pointed out, though, that this arrangement is not that unusual and may find an analogy in the internationalization of satellite communication, where functions of the private US corporation COMSAT were complemented by an intergovernmental body (INTELSAT).[109] I doubt whether satellite regulation and internet regulation can really be compared, especially when it comes to the value-related aspects of governance.

The possible problems arising out of the US jurisdiction, especially the jurisdiction to enforce, are too numerous to explore here. But what if US Congress or the California legislature pass a law that requires ICANN to act in a specific way? What about court orders from a US court or a Californian court? What about competition issues? What if governments or courts of another country claim jurisdiction on actions of ICANN board members from that country? Can an individual claim that ICANN violated her fundamental rights?[110]

By now, the Europeans have two options: to comply with the US arrangement that is being implemented with ICANN or to enter into conflict with the US. The worst case scenario, open conflict and the development of separate technical standards in Europe and in the US is no technical impossibility, but it is not likely to happen. Although the survival of the metric system proves that separate technical standards in the US and in Europe can be maintained,[111] the cost of the separation of Internet standards and European cyber-independence would be too high: the cost would be the end of the

[107] Of course, those who try to maintain a traditional image of what 'der Staat' is about will not feel comfortable at all with a private entity such as ICANN. Arguably, the digital age will not see the 'state of the information society' ('Staat der Informationsgesellschaft') (see Ernst Forsthoff's influential book, *Der Staat der Industriegesellschaft* (1971), for the previous shift of paradigms) which will in part be due to the decoupling of the information society from 'the' state. For the effects of the digital age on 'the state', see also Schoch, 'Verantwortungsteilung in einer staatlich zu regelnden Informationsordnung', in Schuppert (ed.), *Jenseits von Privatisierung und 'schlankem' Staat* (1999), at 221 *et seq.*

[108] Art. V s. 6 of the bylaws.

[109] Stoll and Goller, *supra* note 48, at 144.

[110] See Grote, 'Kommunikative Selbstbestimmung im Internet und Grundrechtsordnung', *KritV* (1999) 27 on the issue of fundamental rights and the Internet.

[111] European Parliament (ed.), *supra* note 4, at 26.

unity of the Internet system, which is part of the key to its success, and very probably also the end of worldwide interconnectivity.[112]

Still, the question remains of how the relationship between ICANN and international law will develop. The World Intellectual Property Organization (WIPO) came forward with a paper on domain names in early 1999.[113] The aim of this plan is, *inter alia*, to fight 'cybersquatters' who register domain names of 'famous' trademarks in order to resell them. The WIPO report suggests special rights for owners of famous brands, thus preventing a registration of that name by anyone else. The paper has been transmitted to ICANN, which currently has the final authority on those matters.

The only way to detach ICANN from its specific geographical link to the US would be to establish ICANN under a multilateral treaty. Then, as a structure of non-statal, 'indirect' multilateralism, ICANN would be an interesting animal in the zoo of public international law, for the ICANN structure privileges the participation of individuals and groups rather than of states. Extending the current ICANN solution — indirect unilateralism — to other, less technical and more value-driven issues of Cyberspace governance such as content control is — from a European perspective — not a realistic option, as this would submit these value issues to US jurisdiction. The US–EU conflict about the EU Data Protection Directive[114] touches on such a value-driven issue and points to the potential for conflict between the US and Europe that those matters contain: the directive requires any country that trades in personal information with a EU Member State to embrace Europe's strict standards of privacy protection.[115] Article 25 of the directive prohibits the transmission of personal information to countries that do not observe sufficient standards of privacy, as is the case with the US. The directive is related to the issue of Internet regulation as it concerns websites that use cookies or profiling systems. Those value-driven issues will either lead to open conflict or to more traditional ways of international cooperation, which means no US jurisdiction over the governance structures. An entity that resembles ICANN may play a role, if it is rooted in international law.

Generally speaking, thinking of the formation of ICANN as a constitutional convention[116] may be not that far from what ICANN is all about. ICANN could indeed

[112] In the DNS context, a separation of standards already exists as there have been alternate root servers since 1996, offering additional gTLDs, until now without much success though. For more details see Diamond, 'Whose Internet Is It Anyway?', *Wired*, 6 April 1998, *http://www.wired.com/wired/archive/6.04*

[113] See *http://wipo2.wipo.int/process/eng/processhome.html* for more details. Cf. also the position of the European Community and its Member States on the WIPO efforts, *http://www.ispo.cec.be/eif/dns/wiporfc2.html*

[114] Directive 95/46/EC of 24 October 1995 on the protection of individuals with regards to the processing of personal data and the free movement of such data, OJ 1995 L 281/31.

[115] For more details on this subject, see Davies, 'Europe to U.S.: No Privacy, No Trade', *Wired*, 6 May 1998, *http://www.wired.com/wired/archive/6.05*

[116] See *supra* note 99.

be the beginning of a specific Cyberspace governance structure that 'constitutionalized' Cyberspace.[117] With the ongoing project of European integration, Europeans have some experience of governance that no longer depends on the authority of a state. They know that there can be international governance under a constitution without a state.[118] This European experience may be useful in assessing chances and risks of future efforts to establish Internet governance structures rooted in international law. From the European experience also arise the crucial questions concerning non-governmental governance that will sooner or later hit Internet governance structures like ICANN as well: the issues of accountability, democracy and transparency.

3 Summary

The European approach to Internet regulation amounts to more or less successful unilateral national or unilateral European regulation, combined with a realistic assessment of the necessity to cooperate on the international level to some extent. However, the Europeans have failed to shift the crucial issue of regulation of technical control over the Internet on to to a truly international arena.

But what does 'international arena' actually mean? In spite of the increasing number of references to Internet regulation on 'the international' level, it is not really clear yet what a comprehensive international law approach to Internet governance would be like.[119] There is a wide range of options from legally non-binding soft law[120] to the participation of internationalized non-governmental entities like ICANN, to a World Internet Organization[121] or to a combination of those options.

Nevertheless, the arguments in favour of trying Internet governance on the international level are compelling enough even without a blueprint of international Internet governance at hand: one argument in favour of shifting Internet regulation

[117] ICANN seems to fear this responsibility, see the interview statement 'We don't want to be a government' by ICANN Interim chairman Esther Dyson, 'Wir wollen keine Regierung sein', *Die Tageszeitung*, 15 July 1999, at 13.

[118] For a detailed account of constitutionalism within EU governance, see Pernice, 'Multilevel Constitutionalism and the Treaty of Amsterdam: European Constitution-Making Revisited?', 36 *CMLR* (1999) 703.

[119] One novel approach to the regulation of the Internet from an international law perspective has been the suggestion to treat Cyberspace as an international space outside national territorial reach resembling the Antarctic: Menthe, 'A Theory of International Spaces', 4 *Michigan Telecommunications & Technology Law Review* (1998) 3. However, unlike the Antarctic, Cyberspace simply is not a distinct space somewhere else, it is right with us. For an overview of public international rules related to the Internet see Patrick Mayer, *Das Internet im öffentlichen Recht*, (1999), at 111 *et seq.*

[120] See the European Commission and European Parliament proposals of October 1998 for a legally non-binding 'Internet Charter', setting out principles in areas such as liability, jurisdiction and data protection, European Parliament Legislative resolution of 1 January 1999, A-4–0366/98 and *http://www.ispo.cec.be/eif/dns/ip98114.html*

[121] The standard procedure for solving international legal problems, which consists in submitting the issue to the ILC, then to convene an international conference and then finally to set up an international organization is not likely to be followed though as this would probably take too long.

on to the forum of an international organization with a universal reach is that this could enhance access by developing countries, which have been more or less left out so far, to the new technologies.[122] More generally, international Internet governance could help open up the predominant economic rationale of the debate on Internet governance to the human rights dimension of Internet regulation. This concerns human rights guarantees of access to information that can be linked to Article 10(1) ECHR and Articles 19 of the Human Rights Declaration and the CCPR on the guarantee of privacy as a human right, which may support requests for unlimited strong encryption.

And, of course, international Internet governance — multilateralism — is the only way for Europeans to effectively reduce the indirect unilateral US dominance of Internet regulation outlined above. Getting back to the image illustrating the two approaches to Internet regulation: (European) traffic sign regulation is useless if there are no roads at all or if the roads are not where the traffic signs are set up; coordination between the regulatory level where the parameters of the road system are laid down and the traffic sign level is a precondition for meaningful traffic sign regulation.

Finally, there may be a link between the effects of Cyberspace on legal thinking[123] and international law: Cyberspace with its fractured, nonlinear structure, conditioning behaviours such as 'surfing' and 'zapping' seems to fit in with a world where, at least for the younger generations, 'zapping' and 'surfing' have become regular ways of taking up information, thus opening up a new approach to learning and thinking in general. Our concept of law will not remain unaffected either.[124] Probably, the way future generations of lawyers will think will be more and more fractured, less linear, less driven by the need to have an overarching legal reference system related to the territory of a particular state. Their way of thinking will probably be closer to that of international lawyers.

[122] See K.-H. Standke, *Vereinte Nationem*, Wissen ist Macht — mehr denn je. Auswirkungen der neuen Informations und Kommunikationstechnologien im Zuge der Globalisierung (1998) 53, at 56, pointing out the role telecommunications and development have played at the UN level since the 1960s.

[123] For an original contribution on the subject see Viktor Mayer-Schönberger's essay on the way Cyberspace affects, perhaps even transforms the authority of law: 'On the Net, No One Knows You Are a Dog! The Authority of Law in Times of Cyberspace', *Vienna Working Papers in Legal Theory, Political Philosophy, and Applied Ethics No. 6, http://www.univie.ac.at/juridicum/forschung/wp06.pdf* Cf. also Lévy, *Cyberculture,* Rapport au Conseil de l'Europe, Paris (1997).

[124] Of course, this also applies to international law, see Gamble, 'International Law and the Information Age', 17 *Michigan Journal of International Law* (1996) 747.