ROBERT SCHUMAN CENTRE FOR ADVANCED STUDIES

EUI Working Papers

RSCAS 2011/24
ROBERT SCHUMAN CENTRE FOR ADVANCED STUDIES
Global Governance Programme-04

INTERNET LAW IN THE ERA OF TRANSNATIONAL LAW

Oreste Pollicino and Marco Bassini

EUROPEAN UNIVERSITY INSTITUTE, FLORENCE

ROBERT SCHUMAN CENTRE FOR ADVANCED STUDIES

GLOBAL GOVERNANCE PROGRAMME

Internet Law in the Era of Transnational Law

ORESTE POLLICINO AND MARCO BASSINI

EUI Working Paper **RSCAS** 2011/24

ISSN 1028-3625

Printed in Italy, April 2011
European University Institute
Badia Fiesolana
I – 50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu/RSCAS/Publications/
www.eui.eu
cadmus.eui.eu

Robert Schuman Centre for Advanced Studies

The Robert Schuman Centre for Advanced Studies (RSCAS), created in 1992 and directed by Stefano Bartolini since September 2006, aims to develop inter-disciplinary and comparative research and to promote work on the major issues facing the process of integration and European society.

The Centre is home to a large post-doctoral programme and hosts major research programmes and projects, and a range of working groups and ad hoc initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration and the expanding membership of the European Union.

Details of the research of the Centre can be found on:
http://www.eui.eu/RSCAS/Research/

Research publications take the form of Working Papers, Policy Papers, Distinguished Lectures and books. Most of these are also available on the RSCAS website:
http://www.eui.eu/RSCAS/Publications/

The Global Governance Programme at the EUI

The Global Governance Programme (GGP) aims to share knowledge, and develop new ideas on issues of global governance, serve as a bridge between research and policy-making, and contribute the European perspective to the global governance debate.

The GGP comprises three core dimensions: training, research and policy. The Academy of Global Governance is a unique executive *training* programme which combines EUI's top-level academic environment with some of the world's leading experts in the field of global governance and is targeted to young executives and policy-makers, public sector officials, private sector professionals, junior academics, and diplomats. Diverse global governance issues are investigated in *research* strands and projects coordinated by senior scholars, both from the EUI and from internationally recognized top institutions. The *policy* dimension is developed throughout the programme, but is highlighted in the GGP High-Level Policy Seminars, which bring together policy-makers and academics at the highest level to discuss issues of current global importance.

For more information:

www.globalgovernanceprogramme.eu

Abstract

Since its birth, the Internet has usually been considered as a threat to the traditional conception of sovereignty as power of a state to regulate the interactions taking place within its territory. The extra-territorial nature of the Internet has definitely contributed to the globalization of legal orders, by requiring them to develop a shared framework to address the problems arising from the relationships occurring on the Internet across various states. In the era of transnationalism, just some of the areas of law have been affected by the adoption of common legal standards, while others, closer to the national identity. Thus, almost paradoxically, the law of the Internet demonstrates that the advent of the era of transnationalism does not imply the end of the role of national law, but only implies it has to be rethought in the broader context of globalization of legal systems.

Keywords

Internet, transnationalism, globalization, sovereignty

Introduction*

If under the label of "globalisation" it is possible to identify, in the words of Habermas,[1] all those trends capable of modifying that historical constellation which has been characterised, since the post-Westphalia era, by the convergence, within the same national borders, of state, society and economy, then the Internet could be seen as the pioneer of the new post-national constellation.[2]

It is difficult, in fact, to find in the history any expression of a compression of time and space[3] more profound than that which characterises social interaction in cyberspace. With particular reference to the space –the territorial element-, our main research question is whether this compression has been so extreme as to create a borderless world, "allergic" to any attempt to regulate it at national and even supranational and transnational level.

If the answer is positive, then the anarchic nature of the Internet would imply that Internet law has benefited only from the *pars destruens* of the post-Westphalian legal context (globalisation as denationalisation), which has determined the crisis of the national legal order as self-contained and self-sufficient normative whole.[4] In that hypothesis, the rise of cyberspace would instead be completely immune to the *costruens* part (globalisation as multilevel supranational governance). This is also encapsulated in the progressive lack of centrality of municipal law caused by the advent of the new season of transnational law, a law which, as Kaarlo Touri[5] has recently reminded us, does not entirely fit between within the dichotomy between municipal law and international law.[6]

If, by contrast, the answer to our first question is negative, and consequently we can see combined in Internet law both the *destruens* and the *costruens* parts emerging after the crisis of the post-Westphalian legal order, then it might be interesting to explore to what extent and especially at what level of governance a regulatory approach could play its role in cyberspace.

---

* Paper presented at the workshop "*Transnational Law – Rethinking Law and Legal Thinking*", European University Institute, Florence, 10-11 March 2011. Oreste Pollicino authored 'Introduction', First part Subsection a), Second Part Subsection a) and Conclusions. Marco Bassini authored First Part Subsection b) and Second Part Subsection b).

1 JÜRGEN HABERMAS, THE POSTNATIONAL CONSTELLATION (Polity Press 2001).

2 As Thomas Fredman, in 1999, has stated that "The Internet is going to be like a huge vie that takes the globalitation system, and keeps tightening the system around everyone, in ways that will only make the world smaller and faster and faster with each day passing". See THOMAS. L. FRIEDMAN, THE LEXUS AND THE OLIVE TREE: UNDERSTANDING GLOBALISATION 141 (Farrar, Straus & Giroux 2000). More recently, and more broadly, Andrea Hamann and Helene Ruiz Fabri have underlined as "technologies spread on a global scale and grow more complex, social problems, formerly addressed internally by state organs are increasingly transferred to the transnational sphere, where governing becomes a matter of international cooperation". *See* Andrea Hamann & Helene Ruiz Fabri, *Transnational Network and Constitutionalism*, 5 INT'L J. CONST. L. 481, 482 (2008).

3 At the basis of the well known definition of globalisation given by DAVID HARVEY, THE CONDITION OF POSTMODERNITY: AN INQUIRY INTO THE ORIGINS OF CULTURAL CHANGE (Blackwell 1989).

4 The *destruens part* of the process of globalisation finds, in other words, its concretisation in the end of black-box model which was premised, as prof. Tuori has noted, on the "Coexistence of territorially differentiated nation-state legal orders, each of them claiming exclusive jurisdiction within their respective territorially defined social spaces, and international law, confined to regulating external relations between sovereign state". *See* Kaarlo Tuori, *Towards a Theory of Transnational Law* (a very first draft, Helsinki, August 26, 2010).

5 Id.

6 According to Gralf Pieter Calliess, "Transnational Law identifies a third category of autonomous legal orders beyond the traditional categories of national and international law. Transnational law is created and developed by the law creating powers of global society, it is bases in general principles of law and their concretisation in social practice, its application, interpretation and development are, at least primarily, the responsibility of private dispute resolution providers, and it is codified – if at all, in general catalogues of principles and rules, standardised contract forms of codes of conduct which are set up by private rule-making bodies". *See* Gralf P. Calliess, *Transnationales Verbraucherventragsrecht*, 68 RABELSZ 244, 254 (2004).

In particular, it is important to understand whether the post-national nature of the Internet has really left behind any state ambition to regulate it or, by contrast, whether in a process of *europeisation* and *internationalisation* of many fields of law, Internet law should represent a partial exception, because of "its national" fatal attraction.

If the latter hypothesis were to be confirmed, then a very paradoxical scenario would emerge, a scenario in which the area of Internet law, for years considered the most emblematic expression of the limits of national law in facing the challenges of globalisation, would, by contrast, prove to be one of the few fields of law still encapsulated in national law, in which not only a global approach, but also a transnational one are likely to prove not quite appropriate.

In the attempt to find reasonable answers to said research questions, the paper is divided into two parts, each one of which is composed of two subsections. The first part of the paper will investigate the initial scholarly analysis of the main characteristics of the law of the Internet (subsection A), and how that analysis has influenced, even though only partially, the original case law of the national courts regarding the identification of the relevant jurisdiction (subsection B).

In the second part of the paper, we will highlight how, after some years, the first, radical, arguments relating to the presumed anarchic nature of the Internet have started to show their weakness. Consequently, the relevant question is no longer whether it is possible to regulate the Net, but, very differently, how to do it. In particular, in the present second season of cyber law, the issue at the core of the current academic, judicial and legislative debate is how to determine and choose the best level to regulate what, some years earlier, was considered, by definition, to be an a-national phenomena.

In this respect we will try to bring to light the weakest points of the cyber-anarchic approach (subsection A). We will then underline, providing an overview of the most important case law (subsection B), how, far from being an a-national or post-national issue, the problem related to enforcement jurisdiction on the world wide web is very often at the heart of a state's national identity.

The concluding remarks have a twofold aim. First we will explore whether and, if so, how, the future evolution of Internet law could find its place in the new transnational law era, in particular dealing with the relationship between law and technology. Secondly, a special emphasis will be given to the rise of a new fundamental right in the new season of the transnational law: the right to have access to the Internet.

First part

A. The Origins: The debate over the feasibility of the Internet regulation: The characteristics that make the Internet an atypical environment for legal interactions:

Despite the engineering of the Internet at the outset responded to a very internal and state-centric priority, that of national security,[7] according to the earliest legal scholarship[8] which focused on the topic, the Internet would present an entirely new dimension to the problem of squeezing transnational activities into the national context. In particular, according to the said authors, while law and regulation had always been organised on the assumption that activities are on the whole geographically delimited, the peculiar character of the world wide web would result in its borderless

[7] *See* Saskia Sassen, *The Impact of the Internet on Sovereignty: Unfounded and Real Worries, in* 42 LAW AND ECONOMICS OF INTERNATIONAL TELECOMMUNICATIONS 195 (Christoph Engel & Kenneth Heller eds., Baden-Baden, Nomos, 2000).

[8] *See* David R. Johnson & David G. Post, *Law and Borders-The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

nature. Thus the Internet, by undermining the criteria of territoriality as a basis for common regulation, would chip away at the state itself.

More precisely, some authors have described the Internet as a self-regulating platform able to develop its own code,[9] whereas others argued that a regulation based on geographical boundaries was unfeasible and applying national laws to the Internet was therefore impossible. In particular, David Johnson and David Post, two champions of this anarchic approach to the web, stated that "events on the Net occur everywhere but nowhere in particular, no physical jurisdiction has a more compelling claim than any other to subject events exclusively to its laws. Efforts to determine where the events in question occur are decidedly misguided".[10]

According to the cyber-anarchic approach, the rise of Internet law would have caused the disintegration of state sovereignty with regard to cyberspace. Said disintegration would have implied the impossibility to apply to the field under investigation any tool based on the theory of transnational law. How would it be possible to share either horizontally or vertically a sovereignty which does not exist any more? [11]

How did the above mentioned approach influence the first judicial attempts to assess the new kinds of conflicts emerging on the Internet?

B. How case law has addressed attempts to emancipate the Internet from legal regulation

The approach of U.S. courts to the problems raised by the seemingly borderless nature of the Internet has moved from a reconsideration of the criteria they had set forth over time to determine the power of a court to settle disputes affecting, directly or indirectly, two or more legal orders. With regard to the most critical matters addressed, such as the exercise of freedom of speech, the U.S. case law has established the limits of personal jurisdiction in cross-border disputes on the grounds of the Due Process of Law clause contained in the Fourteenth Amendment.

It is worthwhile to take a look at these criteria in order to figure out how problems arising from the nature of the Internet have found solutions pretty much consistent with former rulings. In *Pennoyer v. Neff*[12] the Supreme Court held that "the authority of every tribunal is necessarily restricted by the territorial limits of the State in which it is established. Any attempt to exercise authority beyond those limits would be deemed in every other forum […] an illegitimate assumption of power, and be resisted as mere abuse".[13] According to the *Pennoyer* court, each state has jurisdiction "over persons and property within its territory".[14]

---

9 *See* PAUL BARAN, COMMUNICATIONS, COMPUTERS AND PEOPLE (The RAND Corporation, 1965), who forecasted that new technology would not have required law because it would have had the power to self-regulating all its relevant consequences and LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (Basic Books, 1999), who argued that the technology would have produced a "code" more effective than the law to regulate its functioning and consequences.

10 *See* Johnson & Post, *supra* note 8.

11 It is indeed quite paradoxical that one of the most famous and drastic assumption of the new alleged a-national borderless dimension of cyberspace has used, to assert its claim, the constitutional, (and then consequently national) rhetoric of the constitutional fathers. According infact to the notorious Barlow's cyberspace declaration of independence, "Government of the Industrial word, you weary giants of flesh and steel.., the global space we are building to be naturally independent of the Tyrannies you seek to impose on us. You have no moral rights to rule us, nor do you possess any method of enforcement we have true reason **to** fear"- *See* John P. Barlow, *A Declaration of the Independence of Cyberspace* (February 8, 1996), *available at* https://projects.eff.org/~barlow/Declaration-Final.html.

12 95 U.S. 714 (1878).

13 *Id*., at 720.

14 *Id*.

This decision reflected a concept of jurisdiction based exclusively on territorial borders, where the power of national courts to adjudicate lawsuits rests upon a contact between the forum state and the defendant or its property.

This approach turned out to be inappropriate as the growth of interstate commerce implied increases in litigation, and new technologies facilitated the circulation of people and goods. Thus, a harm could be inflicted and suffered in a certain state though neither the wrongdoer nor the injured party were physically present there.

Therefore, in *International Shoe Co. v. Washington*[15] the Supreme Court, even if not explicitly, overruled *Pennoyer* and worked out a more flexible test requiring the achievement of a minimum contact between the defendant and the forum state. In particular, the court specified that in any case jurisdiction must not "offend traditional notions of fair play and substantial justice"[16]. The minimum contact test did not provide a fixed rule, but resulted in a specific and in-depth factual inquiry in every case where jurisdiction over the defendant was at issue.

Additionally, in *Hanson v. Denckla*,[17] the Supreme Court further developed the minimum contact test, by requiring from the defendant an act that constituted a "purposeful availment" of the benefits and protections of the forum state.[18]

An important application of these criteria in the field of tort law occurred in *Calder v. Jones*,[19] where the court developed the "effects test". The plaintiff had filed suit in California against two reporters, living and working in Florida, who had authored an allegedly defamatory article published in a newspaper that circulated in California. The Supreme Court found that California had jurisdiction, since

> under the circumstances, petitioners must 'reasonably anticipate being ha[u]led into court there' to answer for the truth of the statements made in their article. An individual injured in California need not to go to Florida to seek redress from persons who, though remaining in Florida, knowingly cause the injury in California.[20]

More in detail, the Supreme Court set forth a three-prong test, pointing to the awareness of the defendant about three circumstances: first, the allegedly defamatory article circulated in California; second, the plaintiff resided there; finally, the allegedly defamatory statements would have harmed the reputation of the plaintiff there.

How did such test impact on the increase of relationships on the Internet? Adjudicating jurisdiction began to be felt as a key issue, since the development of the Internet implied that interactions seemed to take place anywhere and nowhere.[21]

What the American courts did in reaction to the development of legal relationships on the Internet was striving to adapt the principles expressed in the case law to such a new, apparently borderless, environment. Some important "refinements" were needed.[22] In so doing, the judges distanced

---

15 326 U.S. 310 (1945).

16 *Id*., at 326.

17 357 U.S. 235 (1958).

18 *Id*., at 253.

19 465 U.S. 783 (1984).

20 *Id*., at 790.

21 *See* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV., 1199.

22 UTA KOHL, JURISDICTION AND THE INTERNET. REGULATORY COMPETENCE OVER ONLINE ACTIVITY 82 (Cambridge University Press 2007).

themselves from the approach of those who had sustained that the Internet could not be subject to legal regulation.[23]

These efforts were carried out through a series of cases where courts tackled the dilemma of whether websites should be considered either foreign entities attempting to enter into national borders or foreign territories that can be visited once users have access to them. Depending on the answer, it could be said that a website is anywhere instead of nowhere, but this seems just a formalistic exercise. Rather, courts took account of the type of contact required by the case law to assert jurisdiction over operators of websites given the transnational character of the Internet. In this light, they mainly focused on whether the activities carried out on the Internet by defendants constituted a "purposeful availment" of the benefits and protections offered by the state claiming jurisdiction and thus met the minimum contact test.[24]

A first attempt to refine the criteria developed in the foregoing decisions was made in 1997 in the landmark case of *Zippo Manufacturing Co. v. Zippo Dot Com, Inc*.[25] In *Zippo*, the District Court for the Western District of Pennsylvania worked out the famous "sliding scale test", by distinguishing websites according to three levels of interactivity: according to *Zippo*'s court, "the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of the commercial activity that an entity conducts over the internet".[26]

At the outset, the court focused on subjects operating websites with the purpose of doing business: in such cases, "if the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper".[27] Second, the court pointed out that passive websites, unlike the "active" ones, are operated with the sole purpose of supplying information and making it available (also) in other countries, so that such kind of activity does not constitute a sound basis for personal jurisdiction. Last, the court held that "the middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the web site."[28].

On such grounds the District Court concluded that Zippo Dot Com, a Californian corporation, had entered into contact via its website with Pennsylvania residents with the purpose of doing business.

---

[23] It is worth quoting the concurring opinion delivered by Justice Thomas is *Ashcroft v. American Civil Liberties Union* 535 U.S. 564 (2002). In that case it was at issue which "community standards" contents published on websites had to comply with in order not to be prohibited under a national statute. Justice Thomas concluded that: "If a publisher chooses to send its material into a particular community, this Court's jurisprudence teaches that it is the publisher's responsibility to abide by that community's standard. The publisher's burden does not change simply because it decides to distribute its material to every community in the Nation. Nor does it change because the publisher may wish to speak only to those in a community where avant garde culture is the norm, but nonetheless utilizes a medium that transmits its speech from coast to coast. If a publisher wishes for its material to be judged only by the standards of particular communities, then it need only take the simple step of utilizing a medium that enables it to target the release of its material into those communities" 535 U.S. 583.

[24] *Ex multis*, in *CompuServe, Inc. v. Patterson*, 89 F.3d 1257 (6th Cir. 1996) the Court ruled that the defendant, a Texas resident, purposefully availed himself of the privilege of doing business in Ohio by electronically transmitting shareware softwares files to CompuServe, which, in turn, advertised and distributed them to its subscribers over the Internet. *Contra* the Second Circuit of Appeals in *Bensusan Restaurant Corp. v. King*, 126 F.3d 25 (2nd Cir. 1997) held that the simple creation of a passive website did not constitute a purposeful availment, since it only permitted users located everywhere in the world to access it. *See also Maritz Inc. v. CyberGold Inc.*, 947 F. Supp. 1328 (E.D. Mo. 1996) and *Humphrey v. Granite Gate Resorts, Inc*. 568 N.W. 2nd 715 (Minn. 1997).

[25] 952 F. Supp. 1119 (W.D. Pa. 1997).

[26] *Id*., at 1124.

[27] *Id*.

[28] *Id*.

Such "purposeful availment" was enough to meet the minimum contact test; thus, the court had jurisdiction and could reject Zippo Dot Com's motion to dismiss the case.

The sliding scale test has been strongly criticised, however. Among others, Kohl noted:

> One may even question why the interactive nature of a site should be at all relevant to whether a court does or does not have jurisdiction over a defendant. Assuming its validity, a site which is highly interactive in its design would appear to subject its provider to the personal jurisdiction of every court, and those which are not, of no court at all.[29]

Hörnle is on the same wavelength as Kohl:

> The Zippo sliding-scale test is only a frequently cited test established by a US District Court. It cannot overrule or replace the minimum contacts test. In fact it could be argued that the distinction between passive and active websites as a determinative factor is now technologically obsolete, as very few websites are merely passive showcases of information.[30]

Indeed, just in a few cases courts referred to *Zippo*. In *ALS Scan, Inc. v. Digital Service Consultants, Inc.*[31] the Fourth Circuit of Appeals applied both *Zippo* and *Calder* tests in a suit for copyright infringement caused by the posting of copyrighted materials over the Internet. The court ruled that the infringer could not be subject to the jurisdiction of Maryland (where the plaintiff had filed suit) since its website was at most passive and had not established any contact with the forum state.

Likewise, in *Cybersell Inc. v. Cybersell, Inc.*[32] the United States Court of Appeals for the Ninth Circuit found that the posting on the website of Cybersell, incorporated in California, of an allegedly infringing service mark for which an homonymous Arizona company had filled out an application did not support personal jurisdiction in Arizona, as the passive nature of the website (that only advertised the owner's services) did not qualify as purposeful availment of the benefits and protections of Arizona.

On the contrary, the District Court for the Western District of Wisconsin declined to adopt the sliding scale test in *Hy Cite Corporation v. BadBusinessBureau.com*[33] because

> Even a "passive" website may support a finding of jurisdiction if the defendant used its website intentionally to harm the plaintiff in the forum state […] Similarly, an "interactive" or commercial website may not be sufficient to support jurisdiction if it is not aimed at residents in the forum state.[34]

Additionally, Justice Crabb pointed out that rejecting *Zippo*'s sliding scale test

> does not mean that a website's level of interactivity is irrelevant in deciding whether the exercise of jurisdiction is appropriate. The website's level of interactivity may be one component of a determination whether a defendant has availed itself purposefully of the benefits or privileges of the forum state.[35]

In the area of tort law, in *Amway Corp. v. The Procter & Gamble Company, The Procter & Gamble Distributing Company, Sidney Schwartz and Kenneth Lowndes,*[36] the plaintiff, incorporated in Michigan, brought a claim, among others, against the owner of a website that had posted defamatory

---

29 Kohl, *supra* note 22, at 86.

30 Julia Hörnle, *The Jurisdictional Challenge of the Internet, in* LAW AND THE INTERNET 121, 147 (Lilian Edwards & Charlotte Waelde eds., Hart Publishing 2009).

31 293 F.3d 7907 (4th Cir. 2002).

32 130 F.3d 414 (9th Cir. 1997).

33 2004 WL 42641 (W.D. Wis. Jan. 8, 2004).

34 *Id*., at 11.

35 *Id*., at 12.

36 2000 WL 33725105 (W.D. Mich. Jan. 6, 2000).

information about the company's reputation. The District Court for the Western District of Michigan applied the *Calder* effects test to determine whether it had jurisdiction over the defendant Schwartz, who resided in Oregon. First, it ascertained that the defendant had committed an intentional tort, which constitutes the first prong of the *Calder* test. Second, the court acknowledged that the brunt of the harm had been felt by the plaintiff in the forum state, so that it could be said to be "the focal point of the harm" suffered by the company. Third, the plaintiff had proved that the defendant inflicted the tortious action knowing that the brunt of the harm would have been suffered in Michigan. Therefore, the court ruled that it had jurisdiction over the defendant.[37]

Not only American courts have faced problems of jurisdiction over the Internet. Another landmark case regarding a claim for online defamation was addressed in 2002 by the High Court of Australia. In *Dow Jones & Company, Inc. v. Gutnick*[38] the plaintiff filed a complaint for defamation against a financial information firm, due to an article that appeared in its online newspaper. Few of its subscribers were located in Australia, but the High Court adjudicated the case, holding that

> [i]f people wish to do business in, or indeed travel to, or live in, or utilise the infrastructure of different countries, they can hardly expect to be absolved from compliance with the laws of those countries. The fact that publication might occur everywhere does not mean that it occurs nowhere.[39]

It is worth comparing the arguments used by the Australian High Court with the above-mentioned criteria set forth in the U.S. case law. First, the Australian court found that "harm to reputation is done when a defamatory publication is comprehended by the reader, the listener, or the observer. Until then, no harm is done by it".[40] Accordingly, it held that:

> Defamation is to be located at the place where the damage to reputation occurs. […] It is only when the material is in comprehensible form that the damage to reputation is done [...] In the case of material on the World Wide Web, it is not available in comprehensible form until downloaded on to the computer of a person who has used a web browser to pull the material from the web server. It is where that person downloads the material that the damage to reputation may be done. Ordinarily then, that will be the place where the tort of defamation is committed.[41]

Similarly a British court heard a defamation case brought by an American citizen against the authors of some articles posted on a website based in California. In *Lewis v. King*[42] the England and Wales Court of Appeal addressed what should be deemed as an attempt of "forum shopping", very similar to the idea of "regulatory arbitrage".[43] Both the plaintiff and the defendant resided in the U.S., and the website where defamation occurred was "located" in California. Nonetheless, the plaintiff brought the suit before a British court, assuming that the defamatory content could be accessed in Great Britain and thus caused harm to his reputation there. U.S. and British law regulate the burden of proof differently in such cases. Under U.S. law, the plaintiff has to prove that the defamatory statements are false, while under British law it is incumbent on the defendant to prove that such statements are true. Anyway, the court did not care about the forum-shopping argument raised by the defendant and found that it had jurisdiction because defamation, according to British law, occurs when a libellous statement is posted on the Web and becomes accessible in Great Britain. Accordingly, since the plaintiff had a

---

37 On the contrary, in the abovementioned case *Cybersell, Inc. v. Cybersell, Inc.* the Court of Appeals for the Ninth Circuit refused to apply the Calder test, as it found that the test does not apply with the same force as it would to an individual, because a corporation does not suffer harm in a particular geographic location in the same sense that an individual does.

38 [2002] HCA 56.

39 *Id*., at § 186.

40 *Id*., at § 26.

41 *Id*., at § 44.

42 [2004] EWCA Civi 1329.

43 Micheal A. Froomkin, *The Internet as a Source of Regulatory Arbitrage, in* BORDERS IN CYBERSPACE 129 (Brian Kahin & Charles Nesson eds., MIT Press, 1997).

reputation there, the harmful event was felt in Great Britain and the domestic court jurisdiction was proper.[44]

Another remarkable judgement arouse out of the criminal case *R v. Perrin,*[45] where a French operator of a website who resided in the U.K was convicted for having posted contents prohibited under the Obscene Publication Act 1959. He contended that the British court lacked jurisdiction since the server hosting the website was located outside of the U.K. and thus the British law was not applicable; however the court rejected this argument, pointing out that, otherwise, if domestic laws were applicable exclusively to content posted from the country of origin, operators would be encouraged to forum shopping, as also noted by Uta Kohl.[46]

Courts also asserted jurisdiction over online gambling operators targeting users in other states. Gambling regulation considerably varies from state to state, since it hinges on a number of factors such as morality, culture and religion as well. As many States outlawed or the practice of gambling, the Internet allowed providers to overcome such "regulatory barriers" and thus target users where gambling was illegal. Several rulings were delivered by both national and supranational courts on the matter.

Particularly, the European Court of Justice case law, that will be investigated below (in the Second part, subsection b), sought to strike a balance between the economic freedoms guaranteed by the European Union Treaty and the power of states to forbid or limit (online) gambling for the safeguarding of public order or other protected values. On the other hand, national courts sought to assert their jurisdiction over the owners of websites that provided internet gambling without being legally-licensed in the country of destination of their services.

These efforts are illustrated by two leading cases. First, in *People v. World Interactive Gaming Corp.*[47] the court enjoined two companies headquartered in Antigua and legally licensed in said State from offering gambling to Internet users in New York, where games of chance were prohibited. The respondents contented that the New York court lacked both personal and subject matter jurisdiction. The court rejected, saying that "what makes Internet transactions shed their novelty for jurisdictional purposes is that similar to their traditional counterparts, they are all executed by and between individuals or corporate entities which are subject to a court's jurisdiction".[48]

At the outset, the court found it had personal jurisdiction on the grounds that both the *International Shoe* minimum contact and the "purposeful availment" requirements were met since the respondents were clearly doing business in New York. Then, in response to respondents' argument that New York law did not apply to companies incorporated in Antigua, the court pointed out that "the act of entering the bet and transmitting the information from New York via the Internet is adequate to constitute gambling activity within the New York state".[49] Furthermore, the Court said that

> Wide range implications would arise if this Court adopted respondents' argument that activities or transactions which may be targeted at New York residents are beyond the state's jurisdiction. Not only would such an approach severely undermine this state's deep-rooted policy against unauthorized gambling, it also would immunize from liability anyone who engages in any activity

---

44 As specifically regards England, for more details *see* Amit Sachdeva, *International Jurisdiction in Cyberspace: a Comparative Perspective*, C.T.L.R. 245 252 (2007).

45 [2002] EWCA Crim 747.

46 Kohl, *supra* note 22, at 98.

47 714 NYS 2d 844 (1999).

48 *Id.*, at 849.

49 *Id.*

> over the Internet which is otherwise illegal in this state. A computer server cannot be permitted to function as a shield against liability.[50]

Therefore the New York Supreme Court found that the respondents had violated both the domestic law of the State of New York prohibiting gambling and some federal statutes aimed at ensuring the enforcement of local laws against gambling with respect to the use of the Internet.

Similarly, the United States Court of Appeals for the Second Circuit affirmed the judgment delivered by the district court in *United States v. Cohen*.[51] The defendant had been convicted of violations under a federal statute which prevented operators involved in the business of betting or wagering from using wire communications facilities (such as the Internet or the phone) for the transmission in interstate or foreign commerce of bets or wagers. Like in *People v. World Interactive Gaming Corp.*, the company was legally licensed in Antigua, where it had been incorporated, but also targeted U.S residents via the Internet. It was not at issue the violation of the law of the State of New York but rather the compliance with the provision of the Wire Wager Act that forbids using the Internet to bypass the prohibitions concerning land-based activities provided by national laws.

***

Some important remarks arise from the quoted case law on jurisdiction over the Internet. As Reidenberg highlighted:

> The maturation of the analysis reflects an evolution from a somewhat naïve view of the Internet to a rejection of the Internet activists' simple denial of law. The Internet became popular precisely because of the promise of a global audience. But, this promise could not absolve online activities of legal responsibility. While online technologies were initially designed for geographically indifferent access, nothing fixed the technology in stone. Commercial pressures and the dynamic nature of the Internet have resulted in geolocation and the re-creation of geographic origin and destination.[52]

All the cases examined above, as well as many others that would likewise deserve to be mentioned, clearly pose at least two types of problems for anyone who deals with the legal implications of the Internet. These problems stem in large part from the lack of a common framework of standards that could be shared between states. Especially when we are dealing with values such as freedom of speech, the level and the extent of protection guaranteed by national constitutions significantly vary from state to state; so that an expression deemed defamatory or contrary to public moral standards in a given state could be, on the contrary, protected under the law of another.

First, if the Internet makes websites accessible anywhere and proper jurisdiction in any state where a harm occurs due to their contents, two paths are feasible: either the contents must comply with all the relevant jurisdictions where the website can be accessed, or access to such contents may be limited to those countries which has not outlawed them.[53] Both these solutions are merely hypothetical: the first one would entail that the law of the most restrictive state becomes, at least potentially, the applicable law for every form of speech due to the simple fact that Internet makes it accessible anywhere. It would be paradoxical that a national law regulates interaction outside national borders. This point was highlighted in *American Civil Liberties Union v. Reno*,[54] where it was held:

---

50 *Id.* at 850.

51 260 F.3d 68 (2d Cir 2001).

52 Joel Reidenberg, *Technology and Internet Jurisdiction*, 153 U. PA. L. REV. 1951, 1956 (2005).

53 *See also* the case CompuServe occurred in Germany in 1995. The service provider blocked the access to 200 chat groups in order to avoid prosecutions under the Bavarian obscenity law. It was unable to ban the access only to local costumers, so it suspended the groups worldwide. In so doing, it applied the moral standard of Germany in all the countries where the website could be accessed. Further details in LAWRENCE LESSIG, CODE 2.0 39 (New York 2006).

54 217 F.3d 162 (3rd Cir. 2000).

> Web publishers cannot prevent Internet users in certain geographic locales from accessing their site; and in fact the Web publisher will not even know the geographic location of visitors to its site. Similarly, a Web publisher cannot modify the content of its site so as to restrict different geographic communities to access of only certain portions of their site. Thus, once published on the Web, existing technology does not permit the published materials to be restricted to particular states or jurisdictions […] In gravitating toward an effects doctrine, sovereign states promoted submission to the rule of law rather than capitulation to an Internet attack.[55]

The second solution, which would lead to an opposite result, has long been challenged by operators that dispute the existence of technical instruments to target users according to their place of origin. Additionally, it would not ensure an effective protection of constitutional values, since technological barriers also could be overcome, under certain conditions.

The second problem is directly connected with the first one. If websites can be accessed anywhere, then their contents may cause harm beyond the borders of the country of origin where the website or the operator that maintains it are localised. Thus, foreign jurisdictions have the power to adjudicate disputes arising out of online activities, but it has to be questioned how the judgments delivered in said cases could effectively be enforced.

Both the issues above were evidently at stake in the case *Yahoo! v. Licra*, which is relevant with respect to both enforcement issues and the difficult balance to strike between freedom of speech and the protection of other fundamental rights on the Internet. The analysis of this case is provided under subsection (b) of the second part of this paper. Yet, some remarks can be noticed in advance. Yahoo! hosted a website where auctions for the sale of Nazi memorabilia took place. Two French antiracist organisations sought an order enjoining Yahoo! to disable the website in France, since the sales of those memorabilia is prohibited under the French Penal Code. In the first case, brought before the Tribunal de Grande Instance de Paris, it was at issue whether technical devices could allow operators to monitor and block access to websites depending on the place of origin of the users. Relying on the feasibility of such a system of control, the court required Yahoo! to take all the necessary measures to prevent the website from being visited in France. Yahoo! had contented that no technical device allowed such monitoring but the court ruled in favour of the petitioners since the offending material was accessed (also) in France and, accordingly, the harm was felt there.[56]

A common denominator can be found amongst the cases described above: they all show that as long as websites do not target nor produce harm to certain individuals or entities, a domestic jurisdiction cannot be asserted on the sole ground that website contents do not comply with the laws of that state. In the *Yahoo!* saga the point at issue was definitely whether a French court had the power to issue an order directed to the foreign operator who maintained the website due to the violation of the French Penal Code.

***

The assignment of domain names on the Internet constitutes another crucial issue that it is useful to examine through the lenses of transnationalism. ICANN (Internet Corporation of Assigned Names and Numbers) is the private, non-profit, Californian company that is responsible for the administration of the Domain Name System. It was incorporated in 1998 with the purpose of enhancing participation of the Internet community in the governance of the domain names, regarded as crucial issue for the

---

55 *Id*., at 169.

56 As noted by Matthew Fagin, *Regulating Speech Across Borders: Technology vs. Values*, 9 MICH. TELECOMM. TECH. L. REV. 395, 429 (2003): "The central mechanisme of the French decision is the application of an effects-based analysis for international Internet jurisdiction, employed as a means of imposing the social cost of global Internet communications on content providers".

progress of the Internet. As it has been noted, "the reconciliation of effective global governance and participatory democracy is the promise behind the ICANN experiment".[57]

Although ICANN members are private stakeholders, the U.S. government have maintained an important control over the Domain Name System, since ICANN and the Department of Commerce have signed a memorandum of understanding[58] recognising that ICANN is the body in charge of managing the transition toward privatisation of domain names.

Before ICANN was established, IANA (Internet Assigned Numbers Authorities) had created a *de facto* monopoly for the registration of generic Top-Level Domains (gTLD, such as .com, .net and .org), so that the U.S. had a strategic control on the development of the Internet. Registration of domain names followed the rule "first-come, first-served".

As the Internet grew and the number of websites increased, some critical issues arouse. Most notably, a practice known as cybersquatting spread. It occurs when a "cybersquatter" registers in bad faith a domain name containing a trademark with the deliberate purpose of reselling the right to use that domain name to the owner of the trademark in order to get money.[59] In 1999 the U.S. enacted specific legislation to outlaw such conduct, the Anticybersquatting Consumer Protection Act.[60]

The protection of trademarks against cybersquatting raises no problem when the holder of the trademark and the cybersquatter are both subject to the same national law. However, the issue becomes complex when the cybersquatter and the owner of the trademark are located in different countries. As in the paragraphs above, a matter of jurisdiction is at stake – a matter of jurisdiction made harder by the impact of the Internet.

The Anticybersquatting Consumer Protection Act entitles the owner of a trademark to bring a civil action against the domain name registrant who (a) is in bad faith, and (b) registers, traffics or uses a domain name which either (i) is identical or confusingly similar to a distinctive mark, or (ii) is identical or confusingly similar to or dilutive of a famous mark, or (iii) is a trademark under U.S. law. Additionally, the Act allows the owner to file an *in rem* civil action against a domain name in the judicial district in which the domain name registrar, domain name registry, or other domain name authority that registered or assigned the domain name is located, provided that the the court finds that the owner was not able, also through due diligence, to obtain *in personam* jurisdiction over a person who would have been a defendant in a civil action *in personam*. Using this approach, the Act grants a strengthened protection to holders of trademarks against the risk of cybersquatting.

Notwithstanding these measures, problems could still arise, especially in those states which had not enacted anticybersqyatting legislations. It is worth noting the case of *GlobalSantaFe Corp v. Globalsantafe.com*[61]. The plaintiff filed suit under the Anticybersquatting Consumer Protection Act against a Korean citizen who had registered with the local registrar Hangang the domain name globalsantafe.com as soon as Global Marine and Santa Fe announced their merger. The action was brought in Virginia, where the registry authority which had the control over the .com Top-Level Domains, VeriSign, was headquartered, since the plaintiff sought a judicial order directing the Korean and the American authorities to transfer the domain name.

---

57 Jochen Von Bernstoff, *The Structural Limitations of Network Governance: Icann as a Case in Point, in* TRANSNATIONAL GOVERNANCE AND CONSTITUTIONALISM 257, 259 (Christian Joerges, Inger-Johanne Sand & Gunther Teubner eds., Hart Publishing 2004).

58 The text of the MoU is *available at* http://www.icann.org/general/icann-mou-25nov98.htm

59 One of the first cases of cybersquatting was *Panavision Int'l v. Toeppen*, 131 F.3d 1316 (9th Cir. 1998).

60 15 U.S.C. § 1125(d).

61 250 F. Supp. 2d 610 (E.D. Va. 2003).

The court first ordered Hangang and VeriSign to take all the necessary steps to transfer the domain name but Hangang did not comply because in the meantime the cybersquatter had obtained an injunction from the District Court of Seoul that enjoined the registrar from transferring the domain name due to the U.S. court lacking jurisdiction. Thus, the plaintiff asked the Virginian court for a new order directing VeriSign to cancel the infringing domain name until it was transferred. The court found that the requirements provided under the Anticybersquatting Consumer Protection Act were met, so it could direct the registrar to cancel the domain name. First, it held that:

> The physical location of the ".com" registry within this district is quite significant, for it is the location of the registry here which establishes the situs of the power to transfer or cancel the domain name within this district, pursuant to the ACPA, even if the registrar has not submitted a registrar certificate granting the court authority over the disputed domain name […] if the infringing domain name were registered in a top-level domain whose registry was outside the United States, jurisdiction in the United States might be avoided entirely, provided the registrar is also foreign and the individual registrant lacks sufficient contacts with the forum to meet the due process requirements for personal jurisdiction. In other words, there is a significant gap in the ACPA's trademark enforcement regime for domain names registered under top-level domain names, such as the foreign country code domain names, whose registry is located outside the United States[62].

Additionally, the court said that:

> An aggressive assertion of United States jurisdiction and control over the domain name system based on its essentially arbitrary physical geography may have the unintended consequence of causing a segmentation of the domain name system as other countries seek to assert their own control over the Internet by establishing competing and conflicting systems physically located outside the United States Even absent such segmentation, a desire to avoid United States jurisdiction may cause foreign registrants to choose to use domain names within their respective country code top-level domains, whose registries are located in and operated by the foreign countries, rather than the currently popular "generic" domain names such as ".com" and ".net." The result may be an increasing number of domain names registered out of the reach of United States jurisdiction, but accessible to United States users through the universal domain name system, which in turn will pose a serious challenge to the enforcement of United States trademark rights on the Internet[63].

Thus, the court asserted its jurisdiction, having no important international comity concerns regarding *in rem* jurisdiction.[64]

Given that the registries for the generic top-level domains such as .com, .org and .org are located in the U.S., disputes arising out of trademark infringements can be adjudicated under the Anticybersquatting Consumer Protection Act by U.S. courts. Further details on the matter will be highlighted, however, under section (b) of the Second part.

---

62 *Id*., at 623.

63 *Id*., at 623-624.

64 The Court applied the first-in-time rule, according to which "the first court seized of jurisdiction over property, or asserting jurisdiction in a case requiring jurisdiction over property, may exercise that jurisdiction to the exclusion of any other court" *Sec. and Exch. Comm'n v. Banner Fund Int'l*. 211 F.3d 602, 611 (D.C. Circ. 2000). As regards judicial comity, more in-depth remarks will be provided in the analysis of the Yahoo! case. However, it is worth reporting the definition of the concept of judicial comity given by the U.S. Supreme Court:

"Comity, in the legal sense, is neither a matter of absolute obligation, nor of mere courtesy and good will. It is a recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or other persons who are under the protection of its laws. The comity thus extended to other nations is no impeachment of sovereignty. It is the voluntary act of the nation by which it is offered, and is inadmissible when contrary to its policy, or prejudicial to its interests". *See Hilton v. Guyot*, 159 U.S.113, 163-164 (1895).

Second part

A. The Achilles' heel(s) of the "futility" argument: three points overlooked by the anarchic approach.

As the above analysis based on case law demonstrates, since the advent of the new millennium national courts have started to reject the so-called "futility argument", according to which laws based on geographic borders are not feasible on the Internet, and they have begun to require website operators to manipulate the architecture of the websites so as to make them recognise or take account of territorial boundaries. In other words, the analysis shows how, even for the most revolutionary global communication technologies, geography and governmental coercion retain fundamental importance.[65]

There are at least three arguments which seem to have been undervalued by the cyber-anarchic approach when, as we have seen at the beginning, it has been said that "cyberspace really undermines the relationship between legally significant phenomena and physical location".[66] The first argument is related to the identification of the relevant conception of sovereignty. The second has to do with the paradoxical effect of the evolution of technology. The third is instead connected to the many faces in which the notion of jurisdiction can be concretised.

First of all, with respect to the conception of sovereignty taken as a point of reference by this approach, it considers relevant a granitic and static notion that was already old fashioned at beginning of the 1990s, when the Internet acquired a commercial dimension, and it is even more today. It is a conception according to which a nation has plenary enforcement jurisdiction over persons and property within its border but little, if any, beyond.[67]

More precisely, this conception could have been perhaps considered actual and still valid more than 100 years ago, when, in 1895, in the case *Carrick v. Hancock*, Lord Russel of Killowen CJ famously declared that "the jurisdiction of a court was based upon the principle of territorial dominion, and that all the persons within territorial dominion owe their allegiance to its sovereign power and obedience to all its laws and to the lawful jurisdiction of its courts".[68]

Since then, many things have changed. First of all such an absolutist concept of sovereignity and the assumptions related to the supposed exclusivity of the control of the sovereign state on everything present in its territory have started to show their lack of adequacy. This happened much earlier than the rise of the Internet, with the development of technology, the growth of international trade and a resultant increase in cross-border movement of persons, goods, capital and services.

In particular, even before the advent of the Internet, problems related to the regulation of telephone, television, financial services and pollution, for instance, had brought to light the need of a shared sovereignty, or at least, of a shared agreement between the country of origin and the country of destination of the trans-border content at stake.

In this light, Internet law does not seem to raise new problems in qualitative terms if compared to the regulation of the other transnational activities, but rather in quantitative terms, by the exploitation of two elements which play a crucial role in the theoretical framework of transnational law: space and time.

---

65 Jack L. Goldsmith & Tim Wu, *Preface to the second edition of* WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD (Oxford University Press, 2008).

66 *See* Johnson & Post, *supra* note 8, 1367.

67 *See* Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty,* 5 IND. J. GLOBAL LEGAL STUD. 475 (1998).

68 *Carryck v. Hancock* (1895) 12 T.L.R. 59.

With regard to the territorial dimension, the real jurisdictional novelty of cyber law seems to be, on the one hand, that it will give rise to more frequent circumstances in which effects are felt in multiple territories at once,[69] and, on the other hand, that it makes it very easy and inexpensive for individuals outside the regulating jurisdiction to send harmful content into the regulating jurisdiction.[70]

With regard to the temporal dimension, one of the most peculiar characteristics of the Internet is that it does not seem to raise new legal issues, but it is instead able to rebut the factual assumptions underlying certain already well known legal regimes.

The law of copyright, for example, "relied upon the factual assumptions that reproduction will lead to a loss of quality and that the marginal cost of reproduction and distribution will outweigh the benefits achieved by infringement. However in the digital age, an unlimited number of perfect copies can be made and distributed at minimal cost" [71] and a drastic compression of time. The compression of time in the world wide web is clearly underlined by the High Court of Australia, in the *Dow Jones* case, where it was stated that "in the past *The Times* newspaper would have gone to every colony in Australia. It might have got there rather late, but it could have gone... throughout the whole of that part of the world which was coloured red. I do not see the internet as introducing anything particularly novel, you just get it more quickly".[72]

In relation to the sovereignty conundrum at the heart of the Internet regulation, the only certainty is that there is not a univocal vision of the impact of Internet law on state sovereignty. It could be said the Internet is seriously able to undermine the sovereignty of the state and, at the same time, especially in dictatorial regimes, that it represents a privileged tool to enforce the sovereignty of the people against the regime. Is it not the case that, for the very recent events in Egypt, one of the key words has been Internet Revolution.[73]

With regard to the second element named above, which undermines the claims of a "borderless" Internet, the process of innovation in information technology deserves particular attention. This process if, on the one hand, is at the basis of the claims advocated by the cyber-anarchic school of thought in order to challenge the state jurisdiction, on the other hand, seems, in a paradoxical way, to have empowered sovereign states to assert their rules on Internet activities.[74]

As in fact we have seen, in the analysis of the case law, the major concerns about multi-jurisdictional regulatory exposure have been based on the idea that a content provider or Internet service provider with a multi-jurisdictional presence cannot monitor or control the geographical flow of information on the Internet. As it has been correctly stated,[75] this assumption has become steadily weaker with the evolution of digital technology, and especially with the ever more recurrent use of tools of geo-localisation allowing geographical content discrimination.

---

69 Joel P. Trachtman, *Cyberspace, Sovereignty, Jurisdiction and Modernism*, 5 IND. J. GLOBAL LEGAL STUD. 561, 569 (1998).

70 For example, in relation to defamation, it has been said that: "there is nothing very new (about on line defamation)....but the problems of traditional publishing and defamation are so multiplied when applied to a forum as large, as cheap, as transnational as the internet, that is not hard to see why there is a perception that the law of libel has been transformed by its application to new electronic highway". *See* Lilian Edwards, *Defamation and the Internet*, *in* LAW AND INTERNET-REGULATING CYBERSPACE 183, 184 (Lilian Edwards & Charlotte Waelde eds., Hart Publishing, 1997).

71 Kohl, *supra* note 22, at 38.

72 [2002] HCA 56.

73 *See* http://internetsgovernance.blogspot.com/2011/02/egypt-crisis-and-internet-revolution-20.html.

74 *See* Reidenberg, *supra* note 52, at 1956.

75 Jack L. Goldsmith, *Unilateral Regulation of the Internet: a Modest Defence*, 11 E.J.I.L. 135, 159 (2000).

Against this background, the relevant question today is no longer if content discrimination is technically feasible, but, as Jack Goldsmith[76] has noted in this respect, how much it costs and what is the desired degree of its effectiveness. In other words, ironically, the technological infrastructure, which has been at the heart of some authors' assault on national jurisdiction, has revealed itself to be one of the most powerful engines to make the Internet "less transnational".

In relation to the third element above mentioned, an important difference, too often overlooked by the cyber-anarchic approach, is that between prospective jurisdiction and enforcement jurisdiction. With regard to the former, it finds its expression in the power of state to make its law applicable to a particular transaction. It is evident as, in the said context, national law continues to play a crucial role, even if the content source is beyond the reach of the territorial government. The inability of government to stop the harmful effects of this content at the border does not mean that the source is beyond local regulation.

If it is not possible to intercept the content at the border, a nation can take many steps within its territory to regulate indirectly content transmitted from abroad. Generally, this happens through the adoption of legal sanctions against the foreign content provider's local assets or agents. This has always worked, for example, with unwanted radio and television content broadcasted from one nation into another and, as will be seen in the case of *Google v. Vivi Down*, it applies to Internet content as well.

As it has been correctly stated, "the medium by which the harm is transmitted into the regulating jurisdiction – be it economic interdependence, postal mail, wind current or the internet – is not relevant to the justification for regulating it"[77].

If, in the light of the notion of prospective jurisdiction, the very right of sovereign states to establish rules for online activity is undeniable, it seems more problematic for the same state, moving on to the enforcement jurisdiction, to enforce all the regulatory claims it is entitled to assert under its prospective jurisdiction. If, in fact, the territorial constraint does not occupy a decisive position, with regard to the former, by contrast, as we have seen in the analysis of case law, the said constraint instead acquires a crucial role, because a state can enforce jurisdiction only against persons or entities with a presence or assets within its territory.

In this context, the dynamics which characterise the interaction between interconnected legal orders in the era of transnational law become pivotal in order to successfully settle the conflicts of law emerging in cyberspace. In particular, the central claim of this section is that in the field of the Internet regulation, where state intervention is forced to acknowledge its structural limits, the national law cannot be replaced, even if some scholars advocate it,[78] and in certain fields this has already been done, by ex-ante "pre-packed" rules like those enacted in the area of international public law or even of European law.

By contrast, the only practicable solution in this regard seems to be a case by case approach which takes place in the *no man's land* between municipal law and international law, in accordance with the rules at the heart of a pluralistic vision of transnational law. This view, in its normative terms, and in the words of Kaarlo Tuori, "advocates discursive treatment of conflicts of authority, search for compatible solutions to such conflicts, mutual learning process and inclusion of relevant foreign legal orders perspective in coherence-seeking reconstructions of law".[79]

---

[76] See id.

[77] Goldsmith, *supra* note 67, at. 479.

[78] *See* Henry H. Perritt JR, *The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance*, 5 IND. J. GLOBAL LEGAL STUD. 423 (1998).

[79] *See* Tuori, *supra* note 4.

On the other hand, a hierarchical approach encapsulated in an attempt at a top-down harmonisation stemming from international public law or European hard law does not seem a feasible option with respect to Internet regulation because, as the following analysis of the case law will prove, it needs to face the unconquerable challenge of the nature of the state interests involved in the transnational regulatory issues. Very often, even paradoxically, in the light of the supposed a-national character of the world wide web, this harmonisation overlaps with the hard core of state values at the heart of its national identity.

A combination of interests and values, those relevant in this context, is then at the basis of the constituent power of the nation and is by definition excluded by any process of top-down harmonisation, whether judicial or legislative, as shown in the dialectic between the Constitutional Courts of the EU Member States and the European Court of Justice.

B. How case law addressed the challenge of the world wide web to regulatory barriers

General principles of public policy, protection of morality, human dignity, privacy concerns are only a few of the fundamental values inspiring the legislations enacted in almost all the legal systems. Nevertheless, some of these values are subject to different levels of protection depending on the specific standards shared in each community. For example, the protection of values such as freedom of speech and privacy largely differs, from a quantitative and qualitative point of view, from state to state, due to its close link to the cultural, moral and religious background. Since the digital era has changed the natural environment where interactions take place, the protection of fundamental values has become more and more critical. The following cases will demonstrate that moving from an exclusive national perspective in regulating legal interactions, as most of them take place on the Internet, would result in a failure; thus, that only a wider approach constitutes a "workable solution", even without an exclusion of the national level, which still constitutes an essential stage for the choice of law. Four groups of cases are addressed below in the light of these remarks.[80]

B.1 Hate speech

In the first episode of the Yahoo!-Licra saga,[81] Yahoo! was brought before the Tribunal de Grande Instance de Paris by two antiracist organisations seeking a judgment that ordered Yahoo! to disable a website where auctions of Nazi memorabilia took place due to the violation of the French Criminal Code. On May 2000, the Court issued an order directing Yahoo! to take, within three months, "all necessary measures to dissuade and render impossible any access via Yahoo.com to the Nazi artefact auction service and to any other site or service that may be construed as constituting an apology for Nazism or a contesting of Nazi crimes"[82]. The court of Paris, looking at the effects caused by the website, found that the exercise of jurisdiction was proper, since the harm was suffered in France as consequence of the visualization of the auction on the Internet. By the criminal law barring the merchandise of Nazi paraphernalia, France had enacted a legislation aimed at protecting the "its own internal public order and the dignity of its citizens".[83]

---

80 Particularly, the first case that will be examined, *Yahoo! v. Licra et al.*, demonstrated the growing of the Internet and its emancipation from the U.S. control in the aftermath. Most notably, as argued by Reidenberg, "the positive impact of the Yahoo! decision is that Internet actors will have to recognize varying public values across national borders. The Yahoo! decision begins to force the technical elites developing the Internet to respect democratically chosen values and the rule of law". *See* Joel Reidenberg, *The Yahoo! Case and the International Democratization of the Internet*, Fordham University School of Law, Research Paper 11, April 2001, 3, *available at* http://papers.ssrn.com/paper.taf?abstract_id=267148.

81 *La Ligue Contre le Racisme et l'Antisémitisme v. Yahoo!, Inc*., Tribunal de Grande Instance de Paris, May 22, 2000.

82 *Id*.

83 *See* Fagin, *supra* note 56, at 422.

In response to this order, Yahoo! first argued the lack of jurisdiction of the French court; additionally, alleged that the order issued by the court was unenforceable[84] because no technical means could allow the Internet service providers to control and select users having access to a certain website depending on their country of origin. Also, Yahoo! contended that, should it had been forced to comply with French law, the website would have to be removed altogether, to the detriment of those living in jurisdictions where the merchandising of Nazi memorabilia had not been unlawful.[85] On November 2000[86] the Tribunal rejected the defences raised by Yahoo! and thus upheld the order issued on May. In response to this judgment, Yahoo! did nothing but display on the home page the warning that the website was in violation of the French Criminal Code.

Next, before the U.S. District Court for the Northern District of California, Yahoo! sought a declaratory judgment that the French Tribunal lacked jurisdiction. Yahoo's argument was that the court order violated the First Amendment and was therefore unenforceable. It looks to have been a quite paradoxical approach, as Yahoo!, before the French court, had seemingly supported the regulation sceptics' theories and then looked at the First Amendment as a shield ensuring an absolute protection.[87] The U.S. Court held:

> What is at issue here is whether it is consistent with the Constitution and laws of the United States for another nation to regulate speech by a United States resident within the United States on the basis that such speech can be accessed by Internet users in that nation.[88]

The Court found that the order issued by the Tribunal conflicted with the First Amendment of the U.S. Constitution: it would have been inconsistent had an U.S. court issued it, all the more so it was against the Constitution. Despite the order was a legitimate exercise of the France's sovereignty, the District court "rejected the possibility of enforcement on First Amendment grounds".[89] Neither international comity concerns were taken into account by the court, that articulated the discretionary character of comity as envisaged in *Hilton*. The court said:

> Absent a body of law that establishes international standards with respect to speech on the Internet and an appropriate treaty or legislation addressing enforcement of such standards to speech originating within the United States, the principle of comity is outweighed by the Court's obligation to uphold the First Amendment.[90]

Protection of public order and human dignity in France on one hand and protection of freedom of speech in the United States on the other one were therefore at stake.[91] The case has showed as a difference in the degree of the protection of general principles of public policy, due to the lacking of a common legal framework at supranational level, can result in conflicts between jurisdictions and problems of enforcement.

---

84 With respect to this point, it should be noted that, in response to Yahoo!'s claim that no technical device allowed filtering the users accessing a website, appointed a panel of experts to ascertain whether it was technically feasible for Yahoo! to determine the origin of cybersurfers.

85 Many commentators looked at the order of the French court "as a threat to the exercise of the freedom of speech on the Internet, as a misguided attempt to impose national regulations on the Internet, or as a exercise in futility because of the global nature of the Internet". *See* Reidenberg, *supra* note 80, at 1.

86 T.G.I. Paris, November 22nd, 2000.

87 *See* Fagin, *supra* note 56, at 426.

88 169 F. Supp. 2d 1181 (N.D.Cal.2001).

89 Fagin, *supra* note 56, at 426.

90 169 F. Supp. 2d 1181, 1193 (N.D. Cal. 2001).

91 "The American allegiance to the First Amendment is as central to the American perception of free speech as the moral imperative and commitment to 'personal dignity' that underlies the French hate speech statute. This variance in approach does not detract from the fact that both are legitimate policies of sovereign democratic political systems. However, in the end, neither the technology of the Internet nor the system of international law gives one a greater claim to legitimacy than the other". *See* Fagin, *supra* note 56, at. 438.

However, the defendants appealed the decision, raising in turn the lack of jurisdiction of the District Court. In 2004 the Ninth Circuit of Appeals[92] reversed the decision, finding that:

> France is within its rights as a sovereign nation to enact hate speech laws against the distribution of Nazi propaganda in response to its terrible experience with Nazi forces during World War II. Similarly, LICRA and UEJF are within their rights to bring suit in France against Yahoo! for violation of French speech law. The only adverse consequence experienced by Yahoo! as a result of the acts with which we are concerned is that Yahoo! must wait for LICRA and UEJF to come to the United States to enforce the French judgment before it is able to raise its First Amendment claim. However, it was not wrongful for the French organizations to place Yahoo! in this position.[93]

Notably, the U.S. District Court lacked personal jurisdiction, since the antiracist organizations had not availed themselves of the benefits and protections of California and the "old-fashioned" minimum contact test, applied to the Internet environment, was not met.

In brief, the point at issue in the *Yahoo!* case was twofold. On the one hand, the power to enforce a judgment issued by a foreign court was at stake; in this light, it should be noted as the role of judicial comity was significantly undermined in the decision of the District Court grounding on the discretionary character of that principle. On the other hand, the case clearly illustrates the difficult dialogue between legal orders when courts' decisions affect the protection of constitutional values. In this field, national courts feel it is legitimate to overcome national boundaries in order to ensure the highest degree of protection to values such as free speech, human dignity or public order. The reasons why this dialogue is still troublesome today lie with the differences between the values and the connected degree of protection under national constitutions. Different ways of thinking of freedom of speech as well as public order result, at the final step, in problems of recognition (as the *Yahoo!* case bears testimony) of judgments issued by foreign courts, that is, their enforcement. If neither state is willing to step back, only mutual recognition of such differences in a supranational perspective could reconcile the transnational character of the Internet and the national "fatal attraction" of legal regulation.

In the light of above, it seems that Reidenberg's words got the point

> The Yahoo! decision can […] be seen as both an ordinary case that the French court judged according to basic jurisdictional principles that are also recognized in American law and as an extraordinary case that creates a principle of international democracy and the respect of non-commercial values for the technological infrastructure of the Internet.[94]

B.2 Gambling

In the first part, subsection b), a part of the case law regarding online gambling has been reported to point out how the Internet apparently allows users and operators to overcome territorial boundaries for carrying out activities that could be prohibited under the laws of certain states because of their strong connection with different moral, cultural and religious backgrounds. Notably, said cases showed as some forum shopping attempts failed because of the U.S. courts' power to adjudicate cases where the minimum contact requirements had been met.

On the same matter, the European Court of Justice has addressed issues that go far beyond the sole jurisdictional challenge relating to online gambling. In most of the judgments delivered by the court indeed it was at stake whether values protected by national constitutions, such as the public order and consumer protection, can be undermined due to the prevailing of supranational principles, such as the

---

92 379 F.3d 1120 (9th Cir.2004).

93 *Id*., at 1123.

94 Reidenberg, *supra* note 80, at. 4.

fundamental freedoms of the European Union. The decisions issued by the court made clear that the most critical points stem from differences in the way of thinking and protecting said constitutional values. In other words, the largest part of the conflicts between national laws and fundamental principles addressed by the European Court of Justice arouse because of the different price states are willing to pay to give up or undermine their protection.

Over the last decade online gambling has provided a privileged perspective to look at the relationship between law,[95] intended to be the safeguard of constitutional values, and technology, intended to make available a borderless environment where many interactions take place. So, one could suppose that harmonisation of substantial rules constitutes the best way to achieve a working legal framework in the transnational context. Harmonisation usually is reached through international treaties and presupposes a transfer of sovereignty over supranational entities from national ones.[96]

However, as the *Yahoo!* case has brought to light, not all the parts of different legal orders are suitable to be subject to harmonisation, since they reflect the qualitative and quantitative degree of protection required for certain values by each legal order. Harmonisation has proved effective for the construction of a common legal framework as long as it has been employed to regulate activities that are universally condemned or endorsed. As Uta Kohl points out, the real problems start when we go beyond this core of activities.[97]

> When it comes to gambling, banking, trading in securities or other economic activity, or hate, political, religious, pornographic, privacy-encroaching or reputation-damaging 'speech' – there is much diversity in how States deal with these activities legally. Regulation that would be in the eyes of one State an undue encroachment on the freedom to communicate is in the eyes of another a legitimate curb on that freedom. Substantive harmonisation has not occurred even where the difference of opinion seems rather slight, which is by no means unusual. Most States agree in principle that consumers deserve some protection in their dealing with business or that children should be shielded from pornographic material. But variations in the detail of how much protection there should be and how it should be implemented, and perhaps an inherent resistance to making an external legal commitment, have prevented States from finding a common denominator.[98]

In the European context, measures affecting the cross-border provision of online gambling were intertwined with concerns relating to the fundamental economic freedoms guaranteed by the European Union Treaty. It should be noted that online gambling regulation, unlike the more general area of e-commerce regulation, has not been subject to harmonisation, since Directive 2000/31/EC expressly left gambling out of its field of application. It goes without saying that gambling fits within the group of activities which are regarded differently across states according to their different moral, cultural and religious standards.

The leading case on the matter was addressed by the European Court of Justice in 2003. In *Gambelli*[99] a prejudicial question had been raised in the course of the criminal proceedings against some intermediaries who had established an illegal network of agencies collecting bets on behalf of a British company lacking the license required by law to operate in Italy.[100] The Italian case law had

---

95 *See also* Bernhard Maier, *How Has the Law Attempted to Tackle the Borderless Nature of the Internet ?*, 18 IJL&IT 2010, 142 (2010).

96 Furthermore, harmonisation can occur "by deregulation". *See* Kohl, *supra* note 22, at. 262.

97 *Id*., at 264.

98 *Id*., at 264-265.

99 Case C-243/01, Criminal proceedings against Piergiorgio Gambelli and Others, 2003 ECR I-13031.

100 More in detail, Article 4 of Law 13 December 1989, no. 401, published in Gazz. Uff., December 18, no. 294, establishes criminal penalties for any person who, also via the Internet, provides gambling without having been awarded a license. However, Italian Administration had limited the number of licences and had set forth requirements for the applicants that could not be fulfilled by many companies operating in other European countries and there legally-licensed. Absent any

always justified the restrictions provided by domestic regulation, allegedly conflicting with the E.U. fundamental principles, on the grounds of the safeguarding of public order and consumer protection.

The Court held that "restrictions based on such grounds […] must also be suitable for achieving those objectives, inasmuch as they must serve to limit betting activities in a consistent and systematic manner". In so doing the Court worked out the "hypocrisy test": it held it was for the national courts to determine whether Italian law met such criteria; however it suggested the answer by pointing out that:

> In so far as the authorities of a Member State incite and encourage consumers to participate in lotteries, games of chance and betting to the financial benefit of the public purse, the authorities of that State cannot invoke public order concerns relating to the need to reduce opportunities for betting in order to justify measures such as those at issue in the main proceedings.[101]

The subsequent ruling of the European Court of Justice in *Placanica*[102] seemed to have marked a point of no return, since it found that Italian law was not in compliance with the European Union principles in so far as it established criminal penalties for operators collecting bets online that had not been awarded the license prescribed by law. The Court said: "that blanket exclusion goes beyond what is necessary in order to achieve the objective of preventing operators active in the betting and gaming sector from being involved in criminal or fraudulent activities".

In other words, by addressing these cases the European Court of Justice pointed to public order concerns and consumer protection as the only actual reasons that might justify limitations to the fundamental freedoms of the European Union such as those provided by Italian law, and thereby the control on the activities carried out over the Internet by the unauthorized operators.[103] These measures, in any case, had to pass the "hypocrisy test" described in *Gambelli*.

The Internet in fact was used in the attempt of striking down the regulatory barriers raised by Italy, but it became clear a) that the restrictions provided by Italian law were essentially driven by protectionist policies and would have not passed the *Gambelli* test, b) that the desired level of internal protection could be achieved also without curbing the economic fundamental freedoms, since in most cases operators' countries of origin enact themselves proper systems of protection.

However, a decision[104] delivered in 2009 in response to another prejudicial question seems to have reopened the debate on the issue. In *Liga Portuguesa de Futebol Profissional v. Bwin*, the European Court of Justice found that Portuguese law, which had created a monopoly in the market of gambling (no matter whether over the Internet or not) complied with the European Union law. In more detail, the Court held that the monopoly, even though curbed the freedom to provide services, was justified on the grounds of maintaining public order and consumer protection, especially in the light of the higher risks caused by the use of the Internet for gambling.[105] The fact that other states had enacted

(Contd.)

form of harmonisation, foreign operators, such as the British bookmakers, were unable to target the Italian market and thus complained Italian regulation was in conflict with the freedom to provide services guaranteed by the European Union Treaty. In this context, the Internet became the way to overcome such regulatory barriers, either by targeting Italian users via websites, or establishing a network of agencies operating in Italy which transmitted via the Internet the stakes placed by players.

[101] *Id.*

[102] Joined Cases C-338, C-359 & C-360/04, Placanica and Others, 2007 ECR I-1891.

[103] Italian law also required Internet Service Providers blocking the access to websites providing gambling on behalf of non-licensed companies.

[104] Case C-42/07, Liga Portuguesa de Futebol Profissional and Bwin International Ltd v. Departamento de Jogos da Santa Casa da Misericórdia de Lisboa, 2009 ECR I-7633.

[105] In his opinion, the Advocate General pointed out that the use of the Internet had significantly increased the critical issues connected with gambling: "The extension of the Santa Casa's exclusive right to lotteries and off-course betting on the internet seems to me all the more justified in that the risks to consumers and to public order are, in my opinion, potentially greater with regard to on-line games than in relation to games offered in the traditional way. So far as dangers to consumers are concerned, it is generally accepted that the risks of excessive spending and a real addiction to gaming

less restrictive regulations of gambling had no importance in the Court's opinion, since every state has the right, in the absence of any form of harmonisation, to enact the legislation that best reaches the desired degree of protection. In *Liga Portuguesa*, Bwin, a famous operator incorporated in Gibraltar, provided gambling services on sporting events over the Internet targeting Portuguese users; in so doing, violated the monopoly, thus it was fined.

Two similar judgments were delivered on July 2010 with regard to the Dutch regulation of gambling. In these cases, too, the European Court of Justice found that maintaining public order and consumer protection could justify restrictive measures affecting the provision of gambling services, such as the exclusive rights granted to certain operators for every category of games[106].

The cases above-detailed provides an overview on various attempts to strike down the "regulatory barriers" raised by states with the purpose of strengthening the internal protection of constitutional values. As the *Yahoo!-Licra* saga has brought to light, the most critical issues arise when different ways of thinking and protecting general principles of public policy confront each other. The Internet, given its transnational character, is the natural environment for these conflicts to come out and in areas of law where any state has the power to set out a certain degree of protection, these conflicts give rise to the problems focused on in the former paragraph. In the cases addressed by the Court of Justice it was at issue to what extent states could limit the reach of supranational principles such as the European Unione. fundamental freedoms by enacting rules allegedly aimed at the safeguarding of public order and consumer protection. Therefore, only harmonisation of substantial rules seems to be a sound remedy but without a common denominator for concepts such as public order, everything will be more difficult…

B.3 Privacy

In *Google-Vivi Down*,[107] a criminal proceeding brought before the Court of Milan, four Google executives were charged with defamation and violation of privacy.[108] The trial arouse out of a case where a user posted on the UGC platform run by Google a short video where a teenager with Down syndrome was taunted by his classmates. One of the main points at issue was whether the jurisdiction

(Contd.)

are generally aggravated by the following circumstances, namely the permanent availability of the opportunity to play, the frequency of wins, their enticing or attractive nature, the possibility of staking large sums, the availability of credit in order to play, the location of games at places where people can play on an impulse and, finally, the fact that there is no information campaign regarding the risks of gaming. It must be observed that the offer of games on the internet combines several of these risk factors. First, the offer may be available at any moment and the player can have access to it without moving away from where he is. There is no barrier of space or time between the consumer and the offer of gaming or gambling. In addition, the internet enables the act of playing to be carried out in a context where the player is completely isolated. Secondly, the internet enables the player to have access technically to all the providers of on-line gaming services. Furthermore, on-line games do not require the production of material goods, so that the range of games offered may be very extensive. Consequently the range of internet games is much greater than that of traditional games. Likewise operators can offer on the internet bets or lotto games the results of which can be made known immediately, so that consumers can play many times in a short period of time. In addition, internet relationships do not permit the on-line service provider to check the identity of the consumer in the same way as in the case of a sale between natural persons. Prohibition measures for the protection of minors or vulnerable persons can be circumvented much more easily. Internet relationships are anonymous. Finally, players may be offered credit in order to play on line and payments can be made very easily by internet. The combination of these different factors shows, in my view, that internet gaming potentially represents a higher risk for consumers, particularly minors and the weaker consumers who cannot overcome their gaming habit. Games of chance and gambling by internet may also present significant risks to public order". *See* Opinion of Advocate General Bot delivered on 14 October 2008.

[106] Case C-203/08, Sporting Exchange v. Minster van Justitie 2010 ECR I-0000 (nyp) and Case C-258/08, Ladbrokes Betting & Gaming Ltd, Ladbrokes International Ltd v. Stichting de Nationale Sporttotalisator, 2010 ECR I-0000 (nyp).

[107] Trib. Milan, February 24th 2010, *in* Foro it. 2010, 5, II, 279.

[108] For further information on the case, *see* GUIDO CAMERA & ORESTE POLLICINO, LA LEGGE È UGUALE ANCHE SUL WEB (Milan 2010).

of the Italian court was proper, in the light of the principles regulating data protection in Europe. Article 5 of the Italian Privacy Code provides:

> The present Code regulates the processing of personal data, including those held in foreign countries, performed by a controller established in Italy or in a territory however subject to Italian sovereignty.

Also, it applies to controllers from outside the European Union processing personal data that use an equipment located within the Italian territory.[109]

On the grounds of the second paragraph of Article 5, Google Italy argued that the Italian Privacy Code was not applicable, since the technical infrastructure (i.e., the server) where the video had been stored was located in the U.S., thereby no processing of personal data had taken place in Italy. The Court rejected Google's argument, pointing out that no correspondence between the place where the server is located and the place where personal data are processed is required by law.

Some important rationales seem to be underlying the court's opinion:

First, the processing of personal data was seen as a process that is anything but instantaneous, so that it had taken place *also* in the United States, but not exclusively there.

Second, the Court relied on a comprehensive definition of "processing", including a long chain of activities (from the input through the broadcasting of the video).

Third, an extensive interpretation of "equipment", in the second paragraph of Article 5 was given: there were technical infrastructures other than the server where the video was stored that made possible its broadcasting in Italy; in this way the processing of personal data occurred (also) outside the United States.

The crucial issue was: did the Italian court have the power to adjudicate the case? In 2006 an Italian citizen had threatened an action against Google Italy for violation of the Privacy Code. In that case, Google had failed to remove from its cache outdated contents, which kept on being displayed among the search results. Google Italy objected that Italian law was not applicable and contended that the only subject responsible for the processing of personal data was Google Inc., which had the exclusive control of the server and the search engines, as well. The Italian Data Protection Commission found that the activities connected with the management of the search engines were carried out only by Google Inc., so that Italian court lacked jurisdiction over Google Italy.

Moreover, the case law of the European Court of Justice provides that companies operating their business via the Internet have to be deemed established in the place where their activities are actually performed. At the same time, in the European context some clarifications were felt more and more necessary with respect to cases where the controller of the processing of personal data was established in a country outside the European Union.

The "*Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites*"[110] was adopted in 2002 by the Article 29 – Data Protection Working Party. It seemed to include in the notion of "equipment" for the processing of personal data all the infrastructures used to perform operations such as the collection, working out and diffusion of personal data. In this way, the field of application of the Directive 95/46/EC would have been significantly extended.

---

[109] Article 5, Legislative Decree no. 196, 30 June 2003, published in Gazz. Uff. 29 July 2003, no. 174 - Ordinary Supplement No. 123/L.

[110] Article 29 Working Party document 5035/01/EN/Final, WP 56, adopted on 30 May 2005, *available at* http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2002_en.htm.

Another important document, the Data Protection Working Party's Opinion 1/2008,[111] especially focused on the search engines. The opinion made clear that, in case a company that runs a search engine is located outside the Economic European Space, the European Directive may apply under the condition that at least one of the offices of the controller takes part to the processing of personal data within a Member State and the processing is performed in the context of the activities carried out by such office.[112]

The Court of Milan found that this requirement was met in *Google – Vivi Down*, thus asserted it had jurisdiction. But this was just the first stage…

B.4 ICANN revisited

Further interesting remarks can be noticed with respect to the Domain Name System and its evolution.

In the wake of the U.S. Anticybersquatting Act, ICANN has implemented a Uniform Dispute Resolution Policy (UDRP),[113] The purpose underlying this policy is to provide "trademark holders with a quasi-legal procedure for the resolution of domain name disputes".[114] Also, it "constitutes an experiment in the globalisation and private enforcement of intellectual property rights".[115]

It has to be noted, however, that the Dispute Resolution Panel only addresses disputes concerning abusive registration of generic Top Level Domain (gTLD), such as, for instance, .com, .edu or .org.

Section 4 of the UDRP lays down three requirements that cases have to meet to be adjudicated by the Panel. First, the domain name has to be identical or confusingly similar to a trademark or service mark in which the complainant has rights. Second, the respondent has not to hold any rights or legitimate interests in respect of the domain name. Third, the domain name has to be registered and has to be used in bad faith.

---

111 Article 29 Working Party Opinion 1/2008 on data protection issues related to search engines, 00737/EN WP 148, adopted on 4 April 2008, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf.

112 *Id*., at 10: "The combined effect of Articles 4 (1) (a) and 4 (1) (c) of the Data Protection Directive is that its provisions apply to the processing of personal data by search engine providers in many cases, even when their headquarters are outside the EEA. Which national law applies in a certain case, is a matter of further analysis of the facts of that case. The Working Party expects the search engine providers to contribute to this analysis by providing adequate clarification of their role and activities in the EEA.

In the case of multinational search engine providers:

-a Member State in which the search engine provider is established, shall apply its national data protection law to the processing, according to Article 4 (1) (a);

-if the search engine provider is not established in any Member State, a Member State shall apply its national data protection law to the processing, according to Article 4 (1) (c), if the company makes use of equipment, automated or otherwise, on the territory of that Member State14, for the purposes of processing personal data (for example, the use of a cookie).

In certain cases, a multinational search engine provider will have to comply with multiple data protection laws as a result of the rules regarding the applicable law and the transnational nature of its personal data processing:

-a Member State shall apply its national law to a search engine established outside the EEA if it makes use of equipment;

-a Member State cannot apply its national law to a search engine established in the EEA, in another jurisdiction, even if the search engine makes use of equipment.

In such cases, the national law of the Member State in which the search engine is established is applicable".

113 *See* http://www.udrplaw.net.

114 Von Bernstoff, *supra* note 57, at 270.

115 *Id.*

In the light of above, some questions arise: how should the ICANN policy be regarded? Has it given rise to an autonomous legal order based on its own rules?[116]

Vaios Karavas and Gunther Teubner[117] attempted to answer such questions after having considered a very interesting case adjudicated by the ICANN Panel in 2001. [118] They addressed the contentious issue relating to the nature of the ICANN law, moving from the view of fundamental rights (such as freedom of speech) taken into account in some' decisions of the Panel. They compared three theories. The first is the theory that ICANN panels are merely administrative *fora*, whose decisions can be electronically enforced by accredited dispute resolution providers.[119] Notwithstanding that national courts can be involved in such disputes, ICANN panels, as Karavas and Teubner note, "often refer to US law"[120] and particularly to norms such as the First Amendment. Therefore, the UDRP would result in the extraterritorial application of U.S. law in the field of domain name disputes. The second theory is grounded on the principle that "the relevant national law that the panel determines to be appropriate in the light of all the relevant circumstances […] might prevail".[121] The third way is the most interesting: "Are we seeing the development of an autonomous *lex digitalis*, analogous to the *lex mercatoria*, with its own autonomous *ordre public transnational*, in line with which courts of arbitration would be required to develop internet-specific decisions on fundamental rights and their horizontal effects within the Internet?".[122]

In easier terms, the point at issue is whether the UDRP created an autonomous, transnational legal order, based on its own rules or a simple intergovernmental forum to adjudicate disputes involving problems of choice of law. If every state applied national law, there would be a serious risk of fragmentation of the Internet law regarding generic domain names.

It is useful to quote a valuable remark of Von Bernstoff: "Usually, intergovernmental *fora* based on treaties are not regarded as being capable of providing regulatory decisions with the necessary legitimation, both in terms of public participation and in terms of efficiency and flexibility"[123]. The UDRP established by ICANN is perhaps not immune from these flaws; however, it has proved "a highly efficient form of global private adjudication, even though the judgments given can be appealed or challenged before national courts […] Without any meaningful international public participation, new substantive global private rights have been created by ICANN".

Maybe this is not (yet) a transnational and autonomous legal order, however it does not seem so far away…

---

116 Vaios Karavas & Gunther Teubner, *http://www.CompanyNameSucks.com: The Horizontal Effect of Fundamental Rights on 'Private Parties' within Autonomous Internet Law*, 12 G.L.J. 1335, 1343 (2003).

117 *Id.*, at 1341.

118 BGH, Nov. 22, 2001, BGHZ 149, 191 – shell.de.

119 Karavas & Teubner, *supra* note 116, at 1341.

120 *Id.*

121 *Id.*, at 1342.

122 *Id.*

123 Von Bernstoff, *supra* note 57, at 259.

Concluding remarks

A. First concluding remark: the unavoidable need of a common ground of values shared among states: which future of constitutional law in the transnational governance?

Beginning the final remarks by reference to the very first assumption of this paper, it seems to us that the process of globalisation has neither led to a world in which borders are irrelevant, nor, as it has been argued,[124] to a world in which decisions on how borders are relevant are increasingly made outside of the national domestic process. In order to give effectiveness to the said decisions, the said process seems instead to have made crucial the existence of a common shared legal and value ground among the states which are involved in those decisions.

The key question in this regard is how to achieve the necessary minimum common ground. It seems evident that a process of hard harmonisation stemming from European law or international law is the least suitable method to achieve said goal. It is in fact obvious that, due to the high degree of vertical transfer of sovereignty required by every process of top-down harmonization, nation states will be more reluctant to accept a direct limitation of their sovereign powers in exactly those areas that are more connected, as the above case law analysis shows, to their national identity.

By contrast, it is not surprising that a preference for mutual recognition of the national values at stake in the Internet regulation appears to be the instrument of political and economic integration which is more respectful of diversity and a state's autonomy.[125] More precisely, in the era of transnational law, on the one hand it becomes crucial the degree of the cooperative attitude of each state to a mutual voluntary recognition of the values characterizing the single national legal order, on the other hand, it acquires a very important role the relationship between the regulatory consequences of mutual recognition and its conception as a form of governance.[126]

Ironically, as it has been correctly noted, the recognition of diversity entailed in mutual recognition actually depends on a certain degree of common identity, as only the latter can provide the basis for the mutual trust necessary to implement mutual recognition.[127] This appears even more true, as the above case law clearly shows, in the field of Internet law. The most problematic and irreconcilable issues have arisen when there were overwhelming distances between the very essence at the heart of the notions of public order belonging to the different legal orders involved in a single judicial dispute.

There are still two further challenges faced by the process of mutual recognition in order to prove the most effective tool to achieve a feasible model of governance in relation to Internet law. First of all, as has been underlined,[128] the process of mutual recognition is not immune from a necessary, even if partial, limitation of the state sovereignty that finds its concretisation in the exercise of public choice.

Secondly, one of the limits of mutual recognition that makes its application to the field of Internet law more problematic is that, until now, it has served to create a more homogeneous (or at least a less

---

[124] Mattias Kumm, The Legitimacy of International Law: a Constitutionalist Framework of Analysis, 15 E.J.I.L. 907, 913 (2004).

[125] Kalypso Nicolaıdis, 'Trusting the Poles? Constructing Europe through mutual recognition', 14 J. EUR. PUB. POL'Y 682 (2007).

[126] *See* Miguel P. Maduro, *So Close and yet So Far: the Paradoxes of Mutual Recognition*, J. EUR. PUB. POL'Y 814, 817 (2007), where the Author observes as "only a clear assumption of mutual recognition as a form of governance can highlight the institutional dimension associated with it, in terms of the mechanisms of participation and representation that it embodies and their importance in both explaining and modeling its regulatory impact".

[127] *Id*., at 814.

[128] *Id*.

heterogeneous) internal market within the European Union. As we have seen above, instead one of the most crucial issues is the clash between the European and the U.S. visions of Internet regulation.

Against this background, a process of mutual recognition of the underpinning national values at the heart of the single-state regulation can really become the privileged instrument to achieve an effective framework of transnational Internet governance only if the soft and discretional judicial comity approach[129] (which we have seen at the stake in the *Yahoo* case) is empowered by an "injection of legal pluralism", in the terms advocated by Miguel Poiares Maduro's contrapunctual logic[130] at the heart of the interaction between legal orders and by Kaarlo Tuori's theory of transnational law.

In particular, the judicial comity attitude should be strengthened by a legal pluralism approach seen in its normative terms. As Tuori has clarified, this advocates discursive treatment of conflicts of authority, the search for compatible solutions to such conflicts,[131] value systems and reciprocal commitments between legislative and judicial powers. States are hard pressed to realise their regulatory objectives by mutual cooperation, but they can no longer pretend to be regulatory islands.

Before moving on to the second concluding remark, it remains to underline three final points. The first has to do with the notion of the so-called "judicial dialogue", which has also characterised the dynamics of our case law-based analysis; the second is connected with the relationship between state public choice, technology and the role of constitutional law; the third is related to a new kind of collision between interacting legal orders.

With regard to the first element underlined, the analysis of case law could be useful to clarify a stereotype which unavoidably appears every time the judicial globalisation discourse[132] comes close, in the light of the theory of transnational law, to the relationship between the European legal dimension and the national constitutional one.[133]

---

[129] According to Shany, judicial comity is a general legal principle, which might be applicable in cases of jurisdictional competition …[A]ccording to this principle, which is found in the domestic conflict of laws norms of many countries (mostly from common law systems) courts in one jurisdiction should show respect and demonstrate a degree of deference to the laws of other jurisdictions, including the decisions of judicial bodies operating in these jurisdictions. YUVAL SHANY, THE COMPETING JURISDICTIONS OF INTERNATIONAL COURTS AND TRIBUNALS 260 (Oxford University Press 2003). It would be unfair to recognise, on the other hand the virtues of the judicial comity approach. As it has been corrected stated "The principle of comity is important because it alleviates the difficult aspects of jurisdictional competition by encouraging judges to accommodate related procedures; 'in other words, this principle represents a strategy for soft coordination and harmonization between the entire gamut of jurisdictional configurations'. *See* Giuseppe Martinico *Judging in the multilevel legal order: exploring the Techniques of "Hidden Dialogue*", 21 KLJ 257, 270 (2010).

[130] *See* Miguel P. Maduro, *Contrapunctual Law: Europe's Constitutional Pluralism in Action, in* SOVEREIGNTY IN TRANSITION 501 (Neil Walker ed., Hart Publishing, 2003).

[131] *See* Tuori, *supra* note 4.

[132] *See* Maria Rosaria Ferrarese, *Magistratura e diritti: virtù passive e stato attivo, in Democrazia e diritto (special Issue Giudici e Diritti*), 111 (1998); Claire L'Heureux-Dube, *The International Judicial Dialogue: When Domestic Constitutional Courts Join the Conversation*, 114 HARV. L. REV. 2049 (2001); Anne Marie Slaughter, *A Global Community of Courts*, 44 HARV. INT'L L.J. 191 (2003); *Id.*, A NEW WORLD ORDER (Princeton University Press 2004); Sujit Choudry, *Globalization in Search of Justification: Towards a Theory of Comparative Constitutional Interpretation*, 74 IND. L.J. 821 (1999); Christopher McCrudden, *A Common Law of Human Rights?: Transnational Judicial Conversations on Constitutional Rights*, 20 OXFORD J LEGAL STUDIES 499 (2000); ALEC STONE SWEET, ON LAW, POLITCS AND JUDICIALISATION (Oxford University Press 2002); *Id.*, GOVERNING WITH JUDGES: CONSTITUTIONAL POLITICS IN EUROPE (Oxford University Press 2000); ESIN ORUCU, JUDICIAL COMPARATIVISM IN HUMAN RIGHTS CASES (British Institute of International and Comparative Law 2003); Francesco Francioni, *International Law as a Common Language for national Courts*, 36 TEXAS INT'L L. J. 587 (2001).

[133] Vassiolios Skouris, *The position of the European Court of justice in the EU legal order and its relationship with national constitutional Courts*, ZFR 323 (2005); Alec Stone Sweet, *Constitutional Dialogue in the European Community, in* THE EUROPEAN COURT AND NATIONAL COURTS – DOCTRINE AND JURISPRUDENCE: LEGAL CHANGE IN ITS SOCIAL CONTEXT 304 (Joseph Weiler, Anne-Marie Slaughter & Alec Stone Sweet eds., Hart Press 2004); Giuseppe Martinico, *Il dialogo fra le corti nell'arena del Gattopardo: l'Europa fra novità costituzionale e nostalgie di*

In our view, in order to avoid the mistake of one who, looking at a finger pointing to the moon focuses on the former and not on the latter, it should be noted that the notion of judicial dialogue[134] is nothing but a signal which indicates the presence of something else, often particularly problematic, behind it. It is then not a substantive goal in itself but rather a procedural tool to improve a *status quo* that is not completely satisfactory. In particular what seems to emerge from the analysis carried out in the paper is that, if there is something called global judicial dialogue, it very often occurs due to a (real or presumed) risk of collision[135] between the domestic constitutional, European Union, European Court of Human Rights and Global levels, especially with regard to the standard of protection of fundamental rights.

Underlying the idea of a judicial dialogue, therefore, there is a twofold intent. The first is the willingness of one or more courts to resolve (although sometimes they aim to worsen it) an already existing conflict between different but interlocking legal orders, or to prevent one. The second is the tendency of the same courts not to accept passively that which originates from another judicial body legitimately charged with interpreting the provisions of a legal order which, even if vertically interconnected, is other than their own.

With regard to the second element mentioned above, our analysis shows that it is crucial, in the field of Internet regulation, that the allocation of jurisdiction to a particular state should not simply be considered a technical issue, because, as we have seen, it necessarily involves distributional or public choice.[136] It follows that the evolution of technology cannot dominate the public choice of states. From this perspective, it should always be the law, the regulatory expression of legislative and governmental public choice that takes advantage of the presence of technology infrastructure, and not the inverse

(Contd.)

comportamento, *in* GIURISPRUDENZA COSTITUZIONALE E PRINCIPI FONDAMENTALI, ALLA RICERCA DEL NUCLEO DURO DELLE COSTITUZIONI 891 (Sandro Staiano ed., Giappichelli 2006); FRANÇOIS LICHÈRE, LAURENCE POTVIN-SOLIS & ARNAUD RAYNOUARD (eds.), LE DIALOGUE ENTRE LE JUGES EUROPÉENS ET NATIONAUX: INCANTATION OUT REALITÈ (Bruylant 2004); Gustavo Zagrebelsky, *Corti europee e corti nazionali*, *in* I COSTITUZIONALISTI E L'EUROPA. RIFLESSIONI SUI MUTAMENTI COSTITUZIONALI NEL PROCESSO D'INTEGRAZIONE EUROPEA 529 (Sergio Panunzio ed., Giuffrè 2002); SERGIO P. PANUNZIO (ed.), I DIRITTI FONDAMENTALI E LE CORTI IN EUROPA (Jovene 2005); PAOLO FALZEA, ANTONINO SPADARO & LUIGI VENTURA (eds.), LA CORTE COSTITUZIONALE E LE CORTI D'EUROPA (Giappichelli 2003); Valerio Onida, *La tutela dei diritti davanti alla Corte costituzionale ed il rapporto con le corti sovranazionali*, *in* LA TUTELA MULTILIVELLO DEI DIRITTI, PUNTI DI CRISI, PROBLEMI APERTI E MOMENTI DI STABILIZZAZIONE 105 (Paola Bilancia & Eugenio De Marco eds., Giuffrè 2004); Ricardo Alonso Garcìa, *Il giudice nazionale come giudice europeo*, *Quad. Cost*. 111 (2005).

134 It is perhaps worth to make clear that the terms judicial dialogue and judicial communication are used here in a sense which is narrow in two main directions: firstly the reference is only to the judicial relations between interconnected "vertically" legal orders situated at different, not hierarchically based, levels (national, European and international); secondly the reference is only to the direct relationship between Courts and not to the broader situation of constitutional cross fertilisation and judicial borrowing between legal systems where the judges generally conduct a form of dialogue through mutual citations. *See* Francis G. Jacobs, *Judicial dialogue and the cross fertilization of legal systems: the European Court of Justice*, 38 TEX. INT'L L.J. 547 (2003); Allan Rosas, *The European Court of justice in the context: forms and Pattern of judicial dialogue*, 1 E.J.L.S. 1 (2007).

135 Neil MacCormik, *Risking constitutional collision in Europe?*, 18 OXF. J. LEG. STUD. 517 (1998).

136 As it has been underlined, "The technologic choice either to filter or not to filter becomes a normative decision to "purposeful avail" of the user's forum state. *See* Reidenberg, *supra* note 52, at 1962. For a background on public choice theory, *see*, *e.g.*, MXWELL L. STEARNS, PUBLIC CHOICE AND PUBLIC LAW: READINGS AND COMMENTARY (Anderson Publishing 1997); JAMES M. BUCHANAN & GORDON TULLOCK, THE CALCULUS OF CONSENT (Liberdy Fund 1962); Daniel A. Farber & Philip P. Frickey, *The Jurisprudence of Public Choice*, 65 TEX. L. REV. 873 (1987); William N. Eskridge, *Politics Without Romance: Implications of Public Choice Theory for Statutory Interpretation*, 74 VA. L. REV. 275 (1988).

process. As it has in fact been rightly observed, to dismiss Internet rules as merely technical standard would dramatically miss the political and constitutional dimension of the Internet.[137]

This means that, as happened in the past for other technological innovations in writing, printing and broadcasting, the law has in itself the potential to evolve in response to a changing world. As has been correctly stated to this regard, "while it seems that the internet is totally new and unprecedented, in many ways it is no more than the epitome of a long standing development towards greater and greater economic globalisation".[138]

In this context, the relationship between transnational law, public choice and constitutional law assumes a crucial importance, under two connected points of view. Under the first one much of the literature on transnational governance has shifted from goal-oriented intentional strategy to a design constellation which places its hopes on the ingenuity of the actors involved.[139] In this respect, it must be assessed that it is essential instead that governance remains an intentional activity even when it is transnational. As in fact it has been correctly argued:

> The transfer of social problems from the constitutionally controlled national space is not a matter of simply following the dictates of technology or the needs of knowledge generation that transcends the national state. The lack of national control is often the result of deliberate choices on the part of private actors or even government entities. [140]

The second related aspect that should be underlined is that even when the said transfer takes place, even partially, from a national dimension to a transnational one, precisely because public choice issues are not disappearing, but simply transferred, constitutional law could not leave the field entirely to the international law scholarship. Even if states, as happens in the field of Internet law, cannot fully achieve control over the private, they cannot simply turn away their gaze, claiming that no relevant generation is taking place. The consequence would be, as has been astutely pointed out, to accept passively, from a constitutional law perspective, that the allocation of private risk and injustice and so forth are generated, sometimes, within the confines of constitutionally protected private autonomy.[141]

Finally, with respect to the third point listed above, it should be also noted, with regard to the ICANN regime and its possible collision with the legal norms of one (but in general at least two) national legal orders, that, as has been underlined,[142] the rules on the conflict of laws have to be rethought from conflicts between national legal orders to conflicts between transnational sectorial regimes and national legal orders. The immediate emerging, question connected to the said assumption is obvious: can we apply to such collisions the conflict settlement rules that coordinate the interconnection between interacting national legal orders, or should we rather create new rules for deciding conflicts of legal orders involving transnational laws?

---

[137] *See* Lawrence Lessig, *The Limits in Open Code, Regulatory Standard and the Future of the Net*, 14 BERKELEY TECH. L.J. 759 (1999): *see also* GRALF PETER CALLIES & PEER ZUMBANSEN, ROUGH CONSENSUS AND RUNNING CODE 136 (Hart Publishing 2010).

[138] Kohl, *supra* note 22, at 52.

[139] Christian Joerges, *Constitutionalism and Transnationalism Governance: Exploring a Magic Triangle*, *in* Joerges et al. (eds.), *supra* note 57, 339, 368.

[140] Andràs Sajò, *Reviews to Transnational Governance and Constitutionalism: International Studies in the Theory of Private Law, Hart, 2004, 386 ff and to Anna-Marie Slaughter, A New World Order, Princeton University Press, 2004, 341 ff* , 4 INT'L. J. CONST. L 697, 702 (2005).

[141] *See id.*, at 699.

[142] *See* Gunther Teubner & Peter Korth, *Two Kinds of Legal Pluralism: Collision of Transnational Regimes in the Double Fragmentation of World Society*, *in* REGIME INTERACTION IN INTERNATIONAL LAW: FACING FRAGMENTATION (Margaret Young ed., Oxford University Press 2010). *Available at* http://ssrn.com/abstract=1416041.

B. Second concluding remark: a new fundamental right in the new season of transnational law, the right to access to the Internet

As is well known, freedom of expression is strongly protected by all Western countries' constitutions. For example, in the U.S., free speech is protected by the First Amendment to the Constitution as well as by many state constitutions. Freedom of expression is also protected in the European Charter of Fundamental Rights (Article 11), the European Convention on Human Rights (Article 10), the International Covenant on Civil and Political Rights (Article 19) and the Universal Declaration of Human Rights (Article 19). Moreover, the importance of protecting free speech has been stressed several times in the case law of the European Court of Human Rights, the European Court of Justice and the U.S. Supreme Court.

There is no doubt that in the current digital age people express their opinion and ideas via the Internet. It is on the world wide web where people, organisations, artists, musicians and others find opportunities and chances to form, modify, tailor and express their ideas. Thus, gaining access to the Internet has become an important prerequisite for people and organisations to acquire the knowledge necessary to form and express their opinions and creativity.

Access to, and use of, the Internet strongly enhances freedom of speech. Indeed, in the off-line world the only way for an individual to spread his or her own ideas was either by standing on a chair at Hyde Park Cornern or accepting the mediation and filtering of media enterprises. This compulsory use of the traditional media business model has chilled and still chills individuals' freedom of speech. Yet the advent and development of the Internet have strongly marginalised the role played by traditional media enterprises, which no longer constitute a *condicio sine qua non* for the enjoyment of freedom of speech. Indeed, anyone having a computer can easily and cheaply set up a website, a blog or other forum in the Internet and thus have the possibility to spread his or her opinions worldwide without any economic and legal constraint. Thus, in the digital context individuals' creativity and innovation are capable of breaking the barriers present in the off-line world and regain all their value. This is possible provided that a basic condition is met: access to the Internet must be guaranteed (both technically and economically) to anyone.

It is therefore not surprising that there has recently been a push by the United Nations to make Internet access a human right. The right to Internet connection – also known as right to broadband – has been increasingly perceived as acquiring the same relevance as the right to other public goods, such as water, air, healthcare, education, and so on. The Internet has become vital in everyday life (e.g. for connecting families and friends, banking, shopping, earning a living, etc.) and positively affects the ability of people to communicate, work, manage finances, learn, and generally participate in the collective life of our society.[143]

Finland has been the first country to introduce at constitutional level a legal right to Internet access,[144] and also Estonia in 2000 passed a law stating that Internet access is a fundamental human right of its citizens. Moreover, in a 2009 decision the French Constitutional Court basically confirmed that the right to Internet access belongs to the category of fundamental rights.[145]

---

[143] *See* Annemarie Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, 89 OR. L. REV. 81 (2010). *Available at* http://ssrn.com/abstract=1565038.

[144] Already in the above commented *Yahoo* case, in 2000, it was at stake a right of access to cyberspace. *See* Gunther Teubner, *Societal Constitutionalism, Alternative to State-Centred Constitutional Theory ?, in* Joerges et al. (eds.), *supra* note 57, at 4.

[145] French legislator has recently taken in serious consideration the phenomenon of on line copyright infringement and particularly of unauthorized file sharing. In May 2009 the first version of the so-called HADOPI law was adopted. This law aims at controlling and regulating Internet access as a means to encourage compliance with copyright provisions. It was strongly lobbied by the French president Nicolas Sarkozy, who believed that a strong legislative action to react against online infringement of copyright was badly needed. This law also created an ad hoc administrative agency, called HADOPI **(**Haute autorité de diffusion des oeuvres et de protection des droits sur internet**),** which has been given the

Also the Constitutional Chamber of the Supreme Court of Costa Rica recently declared Internet access to be essential for the exercise of fundamental rights.[146] At the European level, Article 3-*bis* of Directive 2009/140/EC is relevant.[147] This provision attaches great importance to the right to Internet access and expressly makes reference to the fundamental rights and freedom of natural persons enshrined in the European Convention on Human Rights.

(Contd.)

task to control that **"**internet subscribers screen their Internet connections in order to prevent the exchange of copyrighted material without prior agreement from the copyright holders" (Art. L. 336-3 French Intellectual Property Code).The law states that individual subscribers must ensure that their accounts are not accessed and used to reproduce or make available artistic works without the authorization of the copyright holder. It provides the "three-strikes rule", also called "graduated response": if subscribers fail to properly supervise their account within the year following the receipt of the first recommendation (and after a second recommendation has been sent to him), the administrative agency could - after an administrative hearing - either suspend internet access for between two months and a year (during which the subscriber is enjoined from entering into a service agreement with any other Internet service provider) or order subscribers to implement security measures aimed at preventing other unauthorized downloads, with penalty fees for non-compliance. Thus, one of the main features of this first version of the HADOPI law is the following: the preeminent role of an administrative agency entrusted with the power to decide sanctions, including the disconnection of Internet access. Why has the first version of Hadopi law provided that such a sanction be decided by an administrative body? It should be noted that judicial proceedings are usually expensive and slow: that might be a reason why a speeder and cheaper "extra-judicial" approach was chosen as opposed to a standard court proceedings[145]. This law was scrutinised by the French Constitutional Council which in June 2009 found a portion of the law unconstitutional. As terminating individuals' Internet access affects individuals' right to free expression (which is a fundamental right), the French Constitutional Court held that any decision involving Internet disconnection should be taken by a court after a careful balancing of the two interests at stake, i.e. copyright protection and freedom of speech. As the HADOPI law gave an administrative agency the power to terminate individuals' Internet access, the Court held such grant of authority as unconstitutional. In other terms, according to the Court, in light of Article 11 of the Declaration of the Rights of Man and the Citizen of 1789[145], French Parliament was not at liberty to vest an administrative authority with the power of terminating individuals' Internet access. The Constitutional Court's finding that freedom of speech entails access to online communications services was also interesting. In particular, when commenting on the right enshrined in the above Article 11 of the Declaration of the Rights of Man and the Citizen, the court stressed that "in the current state of the means of communication and given the generalized development of public online communication services and the importance of the latter for the participation in democracy and the expression of ideas and opinions, this right implies freedom to access such services" (para. 12). Such finding not only clearly recognizes the importance of the right to have access to Internet in the present era, but also impliedly ascertains, as shown above, its fundamental nature. On September 2009 the French parliament passed another bill (informally known as HADOPI 2), which was intended to remedy the enforcement gap left by the Constitutional Court's decision. The most relevant difference between the first version of the law and HADOPI 2 is that the sanctions to be applied against the alleged infringer will be decided by a court and not by the administrative agency (as indirectly recommended by the Constitutional Court). However, the entire process is still speeded up by the Hadopi-driven administrative procedure.

146 Supreme Court of Costa Rica, 20-7-2010. The Court specified that the "*retardo verificado en la apertura de las telecomunicaciones, además de quebrantar el derecho a una aplicación pronta de las leyes*" has "*incidido en el ejercicio y disfrute de otros derechos fundamentales*".

147 Precisely: Article 3-bis Directive 140/2009 amending Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services, Directive 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and Directive 2002/20/EC on the authorization of electronic communications networks and service. This provision states that "Measures taken by Member States regarding end-users access' to, or use of, services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law. Any of these measures regarding end-users' access to, or use of, services and applications through electronic communications networks liable to restrict those fundamental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall be subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms and with general principles of Community law, including effective judicial protection and due process. Accordingly, these measures may only be taken with due respect for the principle of the presumption of innocence and the right to privacy. A prior, fair and impartial procedure shall be guaranteed, including the right to be heard of the person or persons concerned, subject to the need for appropriate conditions and procedural arrangements in duly substantiated cases of urgency in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms. The right to effective and timely judicial review shall be guaranteed".

A few additional comments on the right to Internet access are necessary. First, such a right could be identified as one of the first human rights belonging to the last generation of fundamental rights (fifth generation). It could be argued that this right emerged when it became clear that the rights identified as fundamental in the digital era (fourth generation) enjoyed the same constitutional status as traditional "off line" freedoms.

Second, just identifying the right to Internet access as instrumental for other fundamental freedoms would not pay tribute to its essential role. Indeed, this right clearly represents a necessary precondition to the enjoyment of many constitutional freedoms in the digital era.[148]

Thirdly, as has been noted,[149] the birth and development of this new constitutional right has called into question the well known dichotomy between negative and costless fundamental freedom and costly social rights. Indeed, this is a "newborn" right which – no one can deny – is fundamental. Moreover, guaranteeing and protecting the right to Internet access requires states to adopt specific policies aimed at ensuring its effective enjoyment by individuals and particularly to carry out expensive investments, especially in terms of infrastructure facilities (e.g. broadband cabling).

Lastly, but not least, since we have seen as in the Internet governance constellation a great role is played by private multinational and extremely powerful corporations, it becomes essential, in order to give effective protection to the new born "right of access to cyberspace" and also to the other related web-based fundamental rights, to go, as it has convincingly asserted,[150] definitively beyond the limits fixed by the state action doctrine.

This means that should be supported without any doubt the idea of the horizontal effect of fundamental rights and, consequently, with specific regard to our topic, to admit the possibility to assert the fundamental right positions relate to cyberspace not only against political bodies, but also against non-state actors, often responsible, on the Net, of the less evident, but more dangerous, human rights infringements.[151] On the one hand there is no doubt that, as it has been observed,[152] "cyber law" global governance structures that operate outside international law have the advantage to empower private actors with their scientific, technological and emancipatory resources without any prior formal government involvement.

But, on the other hand, it also true that the lack of government involvement cannot mean neither that those private entities are not to be considered responsible for their fundamental rights infringements, nor that the nation states are free from their protective obligations imposed upon them in order to combat threats to fundamental rights in areas remote from the state.[153]

It is exactly this one the right scenario in which constitutional law could rediscover its original roots in the new season of transnational law.

---

[148] Vincenzo Zeno Zencovich, *L'accesso alla rete come diritto fondamentale, held at Il diritto dell'informazione tra regole antiche e nuovi media*, Workshop in memory of Corso Bovio, Milan (May 20th, 2010).

[149] *Id.*

[150] Paul Schif Berman, *Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private" Regulation*, 71 U. COLO. L. REV. 1263 (2000). *Available at* http://lsr.nellco.org/uconn_wps/9.

[151] *See* Teubner, *supra* note 143, at 7. *See also* Jordan J. Paust, *Human Rights Responsibilities of Private Corporations*, 35 VAND. J. TRANS'L L. 801 (2002) and Peter Muchlinski, *Human Rights and Multi-Nationals, Is There a Problem*?, 77 INT'L AFFAIRS 31 (2001).

[152] Von Bernstoff *supra* note 57, at 278.

[153] *See* Teubner, *supra* note 143, at 7.

Authors Contacts:

Oreste Pollicino and Marco Bassini
Comparative Public Law
Bocconi University
Via Roentgen 1,
20136, Milan
Italy
Email: oreste.pollicino@unibocconi.it; marco.bassini.86@gmail.com


European
University
Institute
European University Press