THE RIGHT TO AN «OPEN AND ROBUST HIGH-SPEED INTERNET»

María Estrella Gutierrez David

Profesora visitante del Departamento de Derecho Público I y Ciencias Política
Universidad Rey Juan Carlos

Keywords

Open Internet; Net neutrality; Traffic Management; Two-speed Internet; Freedom of expression; Privacy; Fundamental rights.

Abstract

This paper explores the existing debate on the open Internet after the recent rules in this matter released by the US Federal Communications Commission in 12 March 2015. In doing so, it will be analysed how its underlying principle of net neutrality operates, how it has been endorsed by international and national legislation —specially, in Europe and the United States— and how traffic management practices by broadband providers may have implications on end users Internet experience. In this sense, deviations from net neutrality may have a serious impact not only on market competition and consumers, but also on fundamental rights, especially freedom of expression and privacy. For this later reason, this paper raises the question of whether the access to the infrastructure should be granted as a citizen right itself, the nature and scope of such a right and the public service value underlying the open Internet.

I. INTRODUCTION

«Having an Internet connection is crucial to everyday life». This is what the German Federal Court of Justice, the *Bundesgerichtshof*, ruled in 2013 while granting the customer

of a telecommunications company damages for the loss of several weeks his DSL connection[1].

This statement of the *Bundesgerichtshof* poses some fundamental questions that will be explored in this paper: whether the access to the infrastructure of Internet should be considered as a citizen's right; whether this right should be granted, and if so, to which extent it should be granted. Or for better saying in the wording of the Council of Europe, whether the Internet has a «public service value»[2] and thus «*users should have the greatest possible access to Internet-based content, applications and services of their choice […] using suitable devices of their choice*»[3].

Perhaps the answer to some of these questions can be found in the ongoing debate on net neutrality which has been recently revitalised. In an unprecedented statement, the US Federal Communication Commission (the «FCC») Chairman Tom Wheeler announced in January 2015 for Wired magazine[4] the reclassification of Internet access as a «public utility», where the Chairman claimed for a «fast, fair and open» Internet[5]. By March 2015, the FCC released the *2015 Open Internet Order*, a new regulatory attempt to prevent broadband providers from undertaking certain traffic management practices which are considered to endanger the open Internet and its core principle which the network of networks relies on, namely the net neutrality.

According to the US authority, net neutrality is not addressed to preserve *any* Internet architecture, but «the Internet as we know it»[6]. That is to say the Internet built upon the open and end-to-end architecture which has enabled «innovators and consumers at the edges of the network to create and determine the success or failure of content, applications, services and devices, without requiring permission from the broadband provider to reach end users»[7].

---

1 See Bundesgerichtshof, Mitteilung der Pressestelle, n.º 14/2013, Retrieved from: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&pm_nummer=0014/13 (accessed 20 Decemeber 2014).

2 COUNCIL OF EUROPE. *Council of Europe and Internet: maximizing rights and minimizing restrictions. Internet Governance*, 2013.

3 COUNCIL OF EUROPE, *Declaration of the Committee of Ministers on network neutrality* (Adopted by the Committee of Ministers on 29 September 2010 at the 1094th meeting of the Ministers' Deputies).

4 T. Wheeler, «FCC Chairman Tom Wheeler: This Is How We Will Ensure Net Neutrality», *Wired*, 4 February 2015. Retrieved from: http://www.wired.com/2015/02/fcc-chairman-wheeler-net-neutrality (accessed: 15 February 2015).

5 See FCC. Fact Sheet: Chairman Wheeler Proposes New Rules for Protecting the Open Internet. [Commission Documents]. (4 February 2015). Retrieved from: http://www.fcc.gov/document/chairman-wheeler-proposes-new-rules-protecting-open-internet (accessed: 15 February 2015).

6 FCC. Open Internet [Website]. Retrieved from: http://www.fcc.gov/openinternet (accessed: 13 February 2015).

7 FCC. Protecting and Promoting the Open Internet, GN Docket No. 14-28, Notice of Proposed Rulemaking, FCC 14-61 («Open Internet NPRM»), Washington D.C.: 15 May 2014, at para. 1. Retrieved from: https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-61A1.pdf(accessed: 15 January 2015).

Although net neutrality concerns had started much earlier in the United States, in Europe this debate emerged strongly during the process of revision of the regulatory framework on electronic communications which finished by November 2009. As a result of that process, the net neutrality principle was enshrined and protected in a set of European Directives.

What both legal frameworks (American and European) have in common is thatthe market-oriented approach dominates thenet neutrality debate. By contrast, especially in the context of international organisations, a human rights-oriented approach on net neutrality issues is clearly emerging and slowly gaining advocators in the realm of domestic jurisdictions.

According to a FCC's catchphrase, net neutrality ensures that everyone «has access to open and robust high-speed Internet service»[8]. Ironically, there is nothing «neutral» behind the wording carefully chosen by the US regulator. On the contrary, the reference to an «open and robust high-speed Internet service» clearly echoes the well-known vigorous advocacy of a free and public debate on public issues under the First Amendment made by Justice Brennan for the US Supreme Court in the landmark decision *New York Times Co. v. Sullivan* (1964), where it was stablished the far-reaching scope of the constitutional clause. No more and no less than «*a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open[Emphasis added]*»[9].

Not by chance, the Council of Europe has clearly established that electronic communication networks have become basic tools for the free exchange of ideas and information, as they help to ensure «*freedom of expression and access to information, pluralism and diversity and contribute to the enjoyment of a range of fundamental rights*»[10].

Nevertheless, there are enough evidences -some of them documented in this paper- to affirm that certain traffic management practices may pose dangers not only for market competition or protection of consumers but also unjustified interferences with fundamental rights, such as freedom of expression and right to privacy. For this reason, an overarching debate on net neutrality should not forget a human rights dimension.

II. GOALS AND METHODOLOGY

In order to deepen the implications of net neutrality for the future of an open and decentralised Internet —as we know it today, and most importantly, as an environment where fundamental rights can be exercised— this paper has conducted a threefold approach: technical, market and human rights-oriented.

---

8 FCC. *Open Internet* [Website], *cit*.

9 In this case, the Supreme Court extended the First Amendment's guarantee of free speech to libel cases brought by public officials. See *New York Times Co. v. Sullivan*, 376 U.S. 254, 84 S. Ct. 710, 11 L. Ed. 2d 686 (1964), at 270.

10 COUNCIL OF EUROPE, *Declaration on network neutrality* […], *cit.*, para. 3.

First it is necessary to understand the technical meaning an «open and decentralised Internet». For this reason this paper analyses the architectural principles which constitute the fundamentals of the Internet «as we know it», namely, the end-to-end and the net neutrality principles.

Secondly, it will be examined the current debate on net neutrality to better understand to which extent certain practices run by broadband providers when managing Internet traffic may constitute deviations of the net neutrality resulting inserious harms to end users and market competition. In doing so, references to judicial cases and investigations conducted by regulatory authorities will be referred in order to evidence how deviations of net neutrality put at risk the open Internet. To address potential deviations, the European Union and the United States have undertaken a market-oriented regulatory approach whose main guidelines will be analysed in this paper.

Finally, it must be beard in mind that the degree of protection of net neutrality has social and civic implications. From its inception, Courts have long recognised the role of the Internet as a public forum where free speech rights and other fundamental rights need to be protected and guaranteed. For this reason, this paper shall explore also the public service and democratic values underlying the net neutrality principle, along with its human rights-oriented dimension.

Understanding technology means better addressing digital challenges. For this reason, this paper has reviewed the existing literature on net neutrality and its deviations not only from legal resources but also from technical reports and documents. It is important to note, that the existing Spanish legal literature has been mainly focused on market-oriented approaches with some notable exceptions.

In addition, the regulatory framework both in Europe and in the United States has been taken into account to explain how legislation has evolved to address net neutrality issues and how lawmaker is more and more aware of implementing legislative tools to better enforce the net neutrality. Spanish legislation on telecommunications seemingly embraces the principle but fails to adopt specific measures to prevent unreasonable and discriminatory deviations from net neutrality.

Accordingly, in order to complete the regulatory approach, this paper also considers the importance of case law and decisions of international and national regulatory bodies related net neutrality issues, especially those impacting on fundamental rights. Once again, the lack of specific Spanish jurisprudence on this matter is the general trend, except for some isolated decisions not strictly related to net neutrality issues but with «technological neutrality»[11] or «neutrality of private networks» of companies with regards to filters and

[11] See Judgment of the Audiencia Nacional (Spanish National Court) of 19 July 2005 (Appeal no. 410/2002).

blocking measures which restricted discriminatorily the right to information of a specific trade union[12].

In addition, and for methodological purposes, it is necessary to identify the stakeholders involved in net neutrality issues. First, the *broadband providers*, so-called, «last mile providers», that is telecommunications companies which provide with broadband Internet access retail services to end users. In the European Union jargon and literature, broadband providers are also referred as Internet Service Providers (ISP). Secondly, *end user* comprises any individual or entity that uses a broadband Internet access service. Sometimes, end user is also referred as «subscriber» or «consumer» to mean those that subscribe to a particular broadband Internet access service. Finally, in the «virtuous circle of innovation», just between broadband providers and end users, there are other players, namely the *edge providers* which refer to those companies providing with contents, applications and services, and operating at the edge rather than the core of the network.

III. THE ECOSYSTEM OF THE OPEN INTERNET

In *Alta Vista v. Digital*, one of the first cases in the United States concerning a breach of trademark on the Internet environment, the District Court of Massachusetts noted that «[…] [a]s far as the Internet is concerned, not only is there perhaps «no there there», (*sic*) the «there» is everywhere where there is *Internet access*»[13].

In effect, court proceedings adjudicating early cases on Internet first regulation did emphasize the importance of the *ubiquitous access* to the network as an extraordinary medium of worldwide communication. In assessing the consistency with the First Amendment of some provisions of the Communications Decency Act of 1966 (CDA), the Supreme Court held in *Reno v. ACLU* (1997) that:

«The Internet is an international network of interconnected computers […] The Internet is a unique and wholly new medium of worldwide human communication. […] Anyone with access to the Internet may take advantage of a wide variety of communication and information retrieval methods. […] Taken together, these tools constitute a unique medium —known to its

[12] Judgment of the Audiencia Nacional no. 101/2014, of 27 may (Spanish National Court, Labour Courtroom, Section 1), AS 2014\1240. The Court ruled that «*the Company cannot impose veto or censorship of content nor establish inequalities on the different trade unions access to the network which are not justified, as in such a case, these unequal treatment would be deemed as discriminatory. […] Neutrality […] entails prohibition of unjustified inequality by reason of trade affiliation and exercise of trade union freedom to the extent that technical parameters must be equal for the different union member users*».

[13] *Alta Vista Corp. v. Digital Equip. Corp.*, 44 F.Supp.2d 72 (D. Mass. 1998).

users as «cyberspace»— located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet[emphasis added]»[14].

For this universal access being possible, since its very beginning, the Internet was conceived as an open and neutral network of networks through which information, applications and services could freely circulate in a non-discriminatory fashion regardless of its nature, content or identity of their sender or recipient[15].

Before the Supreme Court decision, in *ACLU v Reno* (1996), the District Court of Pennsylvania had already referred to the «unique nature» of the Internet, designed to be, «from its inception», a «common standard», «decentralised» and «open» network of networks. «*The Web's open, distributed, decentralized nature stands [Emphasis added] in sharp contrast to most information systems that have come before it*», the Court said. And precisely, the popularity and success of the Internet was due to «*its open, distributed, and easy-to-use nature*»[16].

Needless to say, that such ecosystem and its underlying infrastructure have relied upon not any design of Internet architecture, but an open design: «*Openness*-not property or contract but free code and *access*- created the boom that gave birth to the Internet that we now know [Emphasis added]»[17].

---

14 *Reno v. ACLU*, 521 U.S. 844, at 849-850, 117 S. Ct. 2329, 138 L. Ed. 2d 874, 1997 U.S. In this case, the Supreme Court analysed the constitutionality of some provisions of the Communications Decency Act of 1996 (CDA) which criminalised communications over the Internet which might be deemed «indecent» or «patently offensive» for minors. Previously, the District Court for the Eastern District of Pennsylvania had granted a preliminary injunction against the said provisions of the CDA (cfr. footnote 14 *infra*). Affirming the District Court decision, the Supreme Court came to the conclusion that the CDA had placed «*an unacceptably heavy burden on protected speech*», remarking «*that the speech restriction at issue there amounted to "burn[ing] the house to roast the pig*"». In its final comments, the Court conceded that the CDA, «*casting a far darker shadow over free speech, threatens to torch a large segment of the Internet community (521 U.S. 882)*».

15 L. Belli, «Network Neutrality and Human Rights» [CDMSI(2013)misc18], Steering Committee on Media and Information Society, Council of Europe Multi-Stakeholder Dialogue on Network Neutrality and Human Rights, Strasbourg: 5th meeting, 3-6 December 2013, at pp. 1-8. Retrieved from: http://www.coe.int/t/dghl/standardsetting/media/cdmsi/CDMSI(2013)Misc18_en.pdf (accessed: 15 January 2015).

16 *ACLU v. Reno*, 929 F. Supp. 824, at 881 (E.D. Pa. 1996). The District Court granted motions for preliminary injunctions against some provisions of the CDA on grounds of unconstitutional restriction upon free speech on the Internet. Plaintiffs, the American Civil Liberties Union (ACLU) and the American Library Association Inc. (ALA), had contended that the said provisions infringed upon rights protected by the Speech Clause of the First Amendment and the Due Process Clause of the Fifth Amendment. In its concluding remarks, the District Court emphasised that «*the Internet may fairly be regarded as a never-ending worldwide conversation*». Hence, the Government could not, through the CDA, «*interrupt that conversation*». Furthermore, as the «*most participatory form of mass speech yet developed*», the Court concluded that the Internet deserved «*the highest protection from governmental intrusion*». On 29 September 1996, the Government filed a direct appeal to the Supreme Court. Cfr. footnote 12 *supra*.

17 L. Lessig, *Code. Version 2.0.*+, Basic Book, New York, 2006, at p. 146.

1. Enhancing an open Internet: e2e and net neutrality principles

As Lessig and Lemley have observed, «[t]he tremendous innovation that has occurred on the Internet […] depends crucially on its open nature». The authors are of the view that the extraordinary growth of the Internet has rested upon its design principles which relate to the openness of boththe Internet's standards and the software implementing such standards. These principles were designed to make the net function more flexibly and efficiently and to encourage «the competition in innovation»[18].

More specifically, the open and decentralized architecture of the Internet is largely the result of the «end-to-end» (e2e) design principle, which simple means that the ««intelligence» in a network must be located at the top of a layered system —at its «ends» where users put information and applications onto the network— and that the communications protocols themselves […] be as simple and general as possible»[19]. Put it simply, the intelligence of the network should be found on its edges, not within the network itself. Indeed, the e2e principle vests the end users (the «edges» of the network) with the responsibility of communication, whereas the network is considered «as a passive and «dumb» infrastructure»[20].

From this perspective, advocators of e2e principle understand that many functions of the Internet are best accomplished by applications themselves provided if this architectural principle is ensured and implemented. They argue that e2e principle must be seen the only way to maintain and protect the open nature of the Internet, where «no prioritisation at all is required»[21].

Accordingly, one of consequences of such open design is the *principle of non-discrimination* amongst services, applications or content. As to Lemley and Lessig, the non-discrimination rule has enhanced «an extraordinary creativity precisely because it has pushed creativity to the ends of the network». In effect, by adopting the e2e architecture, anyone with an Internet connection is able «to design and implement a better way to use the Internet». Therefore, the design of the network should remain «neutral among uses», if we want the Internet still being the «competitive environment where innovators know that their inventions will be used if useful»[22].

---

18 M. Lemley; L. Lessig. «The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era» (October 1, 2000) in *UCLA Law Review*, Vol. 48, at pp. 5-6. Retrieved from: http://ssrn.com/abstract=247737 (accessed: 15 January 2015).

19 *Idem*, at p. 6.

20 L. Belli, *cit.*, p. 8.

21 Cfr. M. J. Scott; P. Nooren; J. Cave; K. R. Carter, *Network Neutrality: Challenges and responses in the EU and in the U.S.* [IP/A/IMCO/ST/2011-02], Brussels: European Parliament, Directorate-General for Internal Policies, 2011, at p. 28. Retrieved from: http://www.europarl.europa.eu/document/activities/cont/201105/20110523ATT20073/20110523ATT20073EN.pdf (accessed: 15 January 2015).

22 M. Lemley; L. Lessig, *cit.*, at p. 8.

Along with the e2e, another architectural principle upon which the original design of the Internet architecture has rested from the first is the net neutrality. According to Tim Wu, who is credited with coining the term, net neutrality must be deemed as a network design principle of open platforms:

«The idea is that a maximally useful public information network aspires to treat all content, sites and platforms equally. This allows the network to carry every form of information and support every kind of application»[23].

Importantly, the net neutrality principle has actually driven the ongoing political debate on the open Internet over the last years. Indeed, every time the openness debate emerges amidst regulators and policymakers there are attempts to define the net neutrality from a legal standpoint.

Precisely, in *Verizon v. FCC* (2014), when confronted with the validity of FCC's *2010 Open Internet Order*[24] imposing disclosure, anti-blocking, and anti-discrimination requirements on broadband providers with regard to Internet traffic management, the Court of Appeals for the District of Columbia Circuit clearly defined the net neutrality:

«*For the second time in four years, we are confronted with a Federal Communications Commission effort to compel broadband providers to treat all Internet traffic the same regardless of source —or to require, as it is popularly known, "net neutrality"* [Emphasis added]—»[25].

Strictly speaking, the net neutrality is «the principle of equal treatment between [data] packets moving across the IP infrastructure», as embraced by the Body of European Regulators for Electronic Communications (the «Berec»).[26] In other words, «that data communications over a network are all processed in the same way, regardless of sender, receiver, application or content»[27].

More specifically, the Berec has drawn the concept of net neutrality as follows:

«A literal interpretation of network neutrality […] is the principle that all electronic communication passing through a network is treated equally. That all communication is treated

---

23 Berec, *Guidelines on Transparency in the scope of Net Neutrality: Best practices and recommended approaches*, BoR (11)67. Riga, December 2011, at p. 7. http://berec.europa.eu/doc/berec/bor/bor11_67_transparencyguide.pdf

24 See FCC, Preserving the Open Internet, GN Docket n.º 09-191, 17941-17950, Report and Order (2010 Open Internet Order), Washington D.C., 21 December 2010, at paras. 62-79. Retrieved from: https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-201A1_Rcd.pdf (accessed: 15 January 2015).

25 *Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014), at p. 4.

26 Berec, *A framework for Quality of Service in the scope of Net Neutrality*, [BoR (11)53], Riga, 8 December 2011, at p.6. Retrieved from http://berec.europa.eu/doc/berec/bor/bor11_53_qualityservice.pdf (accessed: 15 January 2015).

27 R. Davids, *Net neutrality in Europe*. [Briefing], European Parliamentary Research Service, 23 March 2014. Retrieved from: http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140773/LDM_BRI(2014)140773_REV2_EN.pdf (accessed: 15 January 2015).

equally means that it is treated independent of (i) content, (ii) application, (iii) service, (iv) device, (v) sender address, and (vi) receiver address. Sender and receiver address implies that the treatment is independent of end user and content/application/service provider»[28].

For proponents of net neutrality, an open and decentralized Internet enhances innovation and the digital economy. To refer this, the FCC has explained how this «virtuous circle» operates:

«The Internet's openness is critical […] because it enables a virtuous circle of innovation in which new uses of the network —including new content, applications, services, and devices— lead to increased end user demand for broadband, which drives network improvements, which in turn lead to further innovative network uses. Novel, improved, or lower-cost offerings introduced by content, application, service, and device providers spur end user demand and encourage broadband providers to expand their networks and invest in new broadband technologies. Streaming video and e-commerce applications, for instance, have led to major network improvements such as fiber to the premises, VDSL, and DOCSIS 3.0. These network improvements generate new opportunities for edge providers, spurring them to innovate further»[29].

By contrast, opponents argue that legislation on net neutrality will stifle investments in broadband deployment, resulting in higher prices, lower quality of service, and limitations of consumers' choices. Verizon's arguments in its litigation before the Court of Appeals for the District of Columbia Circuit against the *2010 Open Internet Order* are representative of this perspective.

In its opening brief, Verizon contended that net neutrality regulation could impose a «blanket right of access» for content providers, by giving them a «permanent easement for nearly unfettered use of network owners' physical property» at the expense of broadband providers' rights; it could deprive network owners of «their right to exclude others from, and control the use of, their property», and worse it could restricting their editorial discretion and «by compelling them to convey content providers with which they might disagree».

In such a situation broadband providers would not have any incentive to invest in infrastructure deployment leaving users «to bear the full cost of funding networks». In addition, Verizon argued that even if anticompetitive behaviour by the side of broadband providers did occur, «those rare instances could continue to be dealt with through existing antitrust laws»[30].

---

[28] Berec, *Response to the European Commission's consultation on the open Internet and Net Neutrality in Europe*. BoR (10) 42. Riga: 30 September 2010, at pp. 2-3. Retrieved from: http://berec.europa.eu/doc/berec/bor_10_42.pdf (accessed: 15 January 2015).

[29] FCC, *2010 Open Internet Order*, at paras. 13-14.

[30] Verizon, *Appellant*, *v.* Federal Communications Commission, *Appellee*. On Appeal from an Order of the Federal Communications Commission. Case No. 11-1355, 23 July 2012, at pp. 9-10.

2. The ongoing debate on net neutrality: traffic management and deviations from the principle

Some Spanish scholars opine that the debate on net neutrality is mainly focused on «the way in which ISPs may determine (or not) the access and reciprocal communication through Internet between end users and contents, services and applications». In reality, this refers to the «terms and conditions» on which access providers to Internet have the ability to reach end users and thus to what extent such providers would have the technical ability to influence on users' choices[31].

This debate is underpinned by the fact that today the open architecture of the Internet is being challenged[32]. Net neutrality is an ongoing concern given the increasing demands of network traffic[33] which have put an enormous pressure on the Internet and the digital economy resulting from its development[34].

According to CISCO, annual global IP traffic will surpass the 1.3 zettabyte threshold by the end of 2016. This means a gigabyte equivalent of all movies ever made will cross global IP networks every 3 minutes. The number of devices connected to IP networks will be nearly three times as high as the global population and the equivalent of 600 million people will be streaming Internet high-definition video simultaneously by that time[35].

Such demands are to be addressed by Internet providers, not only because temporary traffic peaks can result in congestion and drop of IP packets but also because of security and integrity reasons in order to prevent from harmful or illegal content (e.g. child pornography, spam), malware (e.g. viruses) or attacks (e.g. such as DDoS[36]). In addressing the aforesaid

31 J. Barata, «El concepto de net neutrality y la tensión entre regulación pública y autorregulación privada de las redes», IDP. *Revista de Internet, Derecho y Política,* Universidad Oberta de Catalunya, n.º 13, febrero 2012, at p. 45. Retrieved from: http://idp.uoc.edu/index.php/idp/article/viewFile/n13-numero-complet/n13 (accessed 5 May 2015).

32 M. Kisielowska-Lipman, *Lost on the broadband super highway. Consumer understanding of information on traffic management*, Consumer Focus, 5 December 2012, at p.4. Retrieved from: http://www.consumerfocus.org.uk/files/2012/11/Lost-on-the-broadband-super-highway.pdf (accessed: 15 January 2015).

33 Increasing demands over Internet traffic are mainly due to the wide usage of mobile devices to access the Internet or to the explosion of data-intensive and time-sensitive IP-based applications, for example, file sharing through peer to peer networks, interactive gaming, streaming video, VoD (Video on Demand), IPTV (Television over Internet Protocol) or VoIP (Voice over Internet Protocol).

34 R. Davids, *cit*. at p. 2.

35 Cisco. *Cisco Visual Networking Index: Forecast and Methodology, 2011-2016*. [White Paper]. 30 May 2012.

36 A distributed denial-of-service (DDoS) is a type of computer attack that uses a number of hosts by bombarding the targeted server with information requests in an effort to disable a specific website, either temporarily or permanently. This prevents the main system from operating and leaves the site's users unable to access the targeted website.

categories (congestion, security and integrity), Internet providers usually apply different traffic management techniques, or a combination of them, such as traffic prioritization, packet filtering, packet drop discipline, routing or deep packet inspection («DPI»)[37].

In a broad sense, the International Telecommunications Union («ITU») defines *traffic management* as «a collection of techniques that may be used by an ISP to plan and allocate available resources to attain optimum performance for diverse classes of users across a network»[38].

Generally speaking, traffic management techniques are not to be seen necessarily as negative practices. For instance, blocking measures by using techniques such as DPI or by modifying DNS servers can be used to prevent end users from accessing to illegal content (e.g. child pornography) or to protect third parties' rights against infringement (e.g. intellectual property rights, personality rights)[39].

In a series of cases decided by national Courts, they have referred to some traffic management techniques. In particular, in the British case *Fox v. BT* (2011)[40], the Chancery Division of the High Court of Justice granted blocking measures as a part of an injunction sought by some American film and TV production companies and majors on the website Newzbin which had infringed their intellectual property rights by making available

[37] These are some of the most common traffic management techniques. For instance, *traffic prioritisation* determines the order in which each data packet will be transmitted from a router's outbound queue for a particular transmission link. Prioritization of traffic is possible using *access-tiering techniques*, which consist of giving bandwidth priority, at differentiated prices from Internet access fees to ensure certain quality of downstream traffic for data-intensive and time-sensitive IP-based services, applications and contents. *Packet drop discipline* determines which data packets a router will drop if the number of packets exceeds the memory available for a queue. In addition, *packet filtering* is used to drop packets or otherwise apply special handling based on defined criteria. *Routing* is a tool used by an IP network to determine where each data packet should be addressed next. *Deep Packet Inspection* or DPIis a set of techniques for examining and categorizing packets for different purposes. *Data Cap* is a technical measure to make the price if data packets depend upon volume, by monitoring traffic volume and then blocking or throttling data or charging for extra volume once a pre-defined data cap is reached.

[38] International Telecommunications Union (ITU). *Net neutrality: a regulatory perspective*. GSR12 Discussion Paper, 19 October 2012, at pp. 2-3.

[39] In the European context, in must be noted that in order to benefit from the liability exemption regime applied to intermediaries (e.g. access, proxy caching, or hosting providers) under the e-Commerce Directive of 2000, Internet service providers must have no actual knowledge of the illegal service or content, or if so, they must act with diligence upon request of competent authorities in removing or blocking access to such illegal services or contents.

[40] [2011] EWHC 1981 (Ch). The Applicants (the «Studios») were six well-known film production companies and studios (amongst others, Fox, Warner Bros, Disney) and were owners or exclusive licensees of copyrights in films and television programmes. The Respondent, British Telecommunications PLC («BT») was the largest internet service provider («ISP») in the United Kingdom. By their claim, the Studios sought an injunction against BT pursuant to the Copyright, Designs and Patents Act 1988 («CDPA 1988») intending to block or at least impede access by BT's subscribers to a website currently located at www.newzbin.com (the «Newzbin2»), where copyright infringement occurred.

copyrighted works to subscribers who have purchased premium credit. Particularly, the Court referred to blocking measures implemented by broadband providers such as DNS name blocking, IP address blocking using routers, and DPI-based URL blocking using Access Control Lists on network management systems.

According to the International Telecommunications Union (the «ITU») «[t]raffic management is critical for the proper functioning of the Internet, but it can also be misused by an ISP to create unfair access or use of the Internet»[41].

From this perspective, some practices of traffic management could be contrary to the principle of net neutrality[42]. In fact, as to a DLA Piper study for the European Commission, traffic management techniques may also «serve other purposes than remedying network congestion»[43].

In the United States, the FCC opines that fixed and mobile broadband providers do have the economic incentives[44] and the technical ability[45] «to engage in practices that pose a threat to Internet openness by harming other network providers, edge providers, and end users»[46].

For instance, a broadband provider could block, degrade or throttle VoIP traffic on its network in order to protect its own fixed or mobile telephony business against competitors or to favour its commercial partners' contents, applications or services by charging them for prioritized access to end users. It is thought that such practices could result in reduc-

41 ITU, *Net neutrality*, *cit.*, at p.3.

42 K.R. Carter et al., *cit.*, at p. 1.

43 DLA Piper. «EU study on the New rules for a new age?» EUROPEAN COMMISSION'S INFORMATION SOCIETY AND MEDIA DIRECTORATE-GENERAL. Legal analysis of a Single Market for the Information Society (SMART 2007/0037). November 2009, at p.4. (accessed: 20 December 2014) at p. 4. Retrieved from: http://ec.europa.eu/information_society/newsroom/cf/newsletter-item-detail.cfm?item_id=7022(accessed: 20 December 2014).

44 This is because broadband providers may are in a position to act as a «gatekeeper» between end users' access to edge providers' applications, services, and devices and reciprocally for edge providers' access to end users by preferring their own or affiliated content to the detriment of competitors, or demanding fees or tolls from edge providers to prioritize access to end users, and thus degrading the level of service provided to non-prioritized access. *Cfr*. L. Belli, *cit.*, at p. 12.

45 For example, DPI may be used in a manner that may harm the open Internet by limiting access to certain Internet applications, or blocking certain content. Similarly, traffic control algorithms can be abused to give certain data packets favourable placement in queues or to send packets along less congested routes in a manner contrary to end user preferences. The US regulator comes to the conclusion that the use of these techniques «may ultimately affect the quality of service that users receive, which could effectively force edge providers to enter into paid prioritization agreements to prevent poor quality of content to end users». See FCC. *Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, FCC 15-24 («2015 Open Internet Order»), Washington D.C.: 12 March 2015, at para. 85. Retrieved from: http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0312/FCC-15-24A1.pdf

46 FCC, 2015 Open Internet Order, *cit.*, at para. 78.

ing innovation at the edge, increasing rates for end users, and thus reducing consumer demand[47].

By contrast, European approach on this issue has seemed to minimize the concern about such practices. In this sense, some National Regulatory Authorities (NRAs), like the British communications regulator Ofcom have said that there is «little evidence that these traffic management policies are resulting in specific consumer harm»[48].

Nevertheless, dangers to Internet openness are not «speculative or merely theoretical»[49]. Conversely, a series of cases happened in both sides of the Atlantic evidences that broadband providers have been engaged in «neutrality interferences» such as: blocking, degradation, prioritization, access-tiering, data caps and unreasonable restrictions on running applications and connecting certain equipment[50].

Madison River (2005)[51] and Comcast (2008)[52] are well-known issues investigated by the US regulator evidencing to which extent some practices held by broadband providers consisting of blocking or degrading VoIP and peer-to peer traffic result in unreasonable and unfair deviations from the net neutrality principle. These deviations (either by preventing end users from accessing to legal content, applications or services or by degrading access speeds) seriously harm Internet access or lessen significantly end users' quality of experience to *de minimis*[53].

For the European Commission, differences in treatment are essentially a form of product differentiation which is considered beneficial for competition, as consumers could easily switch between access providers, which will possibly discourage access-tiering practices. Nevertheless, opponents believe that, particularly in markets with insufficient competition or significant switching costs, access-tiering will benefit only established

47 *Idem*, at para. 82.

48 Ofcom., *cit*, par. 4.32.

49 FCC, 2010 *Open Internet Order*, *cit*, at para. 35.

50 DLA Piper. *cit*, at p. 7.

51 *Madison River Communications, LLC and affiliated companies*, File No. EB-05-IH-0110; Acct. No. FRN: 0004334082, Consent Decree, 20 FCC Rcd 4295 (EB 2005) (*Madison River Consent Decree*). In this case, Madison River, a telephone and broadband provider in several States paid a $15,000 fine to settle a Commission investigation into whether it had blocked Internet ports used for competitive VoIP applications, thereby affecting end users ability to use VoIP through one or more VoIP service providers. Madison River agreed «not to block ports used for VoIP applications or otherwise prevent customers from using VoIP applications».

52 *Comcast Network Management Practices Order*, 23 FCC Rcd 13028, at 13055-56, paras. 1, 47-48 (2008) (*Comcast Order*). In 2008, the FCC found that Comcast had been disrupting BitTorrent peer-to-peer (P2P) uploads of its subscribers preventing them from legally sharing files online by masquerading as its user's computer and resetting the connection from a Comcast subscriber to some other Internet user. Comcast customers had not been informed about this degrading traffic practices.

53 *Cfr.* K. R. Carter et al., *cit.*, at p. 25.

companies and be likely result in detrimental effects especially for new innovators[54]. Precisely, in the US, different stakeholders such as the Internet Association, the Consumer Federation of America, Mozilla, Microsoft, Google or Netflix, have denounced pressures to enter into paid prioritized access to end users arrangements. Particularly, Microsoft explained that broadband providers could use their power as gatekeepers «to pressure edge providers into entering such arrangements and demand increasingly higher rates and greater concessions from edge providers over time»[55]. In other words, broadband providers seem to claim edge providers a «toll» for delivering their service to end users in other to assume part of the costs of networks deployment[56].

The commercial dispute between the cable operator Comcast and the online video platform Netflix[57] has shown to which extent a broadband provider may determine interconnection and transit agreements with content providers —*prima facie* excluded from net neutrality rules— and how such agreements may finally affect the quality of service and the services accessed by end users, indirectly impacting on net neutrality. «At the heart of this —the FCC observed— is whether Internet Service Providers (ISPs) that provide connectivity in the final mile to homes can advantage or disadvantage content providers, and therefore advantage or disadvantage consumers»[58].

Evidences that restrictive practices on traffic management have been put in place at European level can be found in the joint investigation of the Berec and the European Commission which stressed the existence of a wide array of traffic management practices resulting in restrictions, where the most frequently reported were blocking and/or throttling of P2P traffic, on both fixed and mobile networks, and blocking of VoIP traffic,

54 DLA PIPER, *cit.*, at 14.

55 FCC, *2015 Open Internet Order*, *cit*. at p. 29, footnote 128.

56 Cfr. EuskalTelebista (EITB), Alierta (Telefónica) advierte a los buscadores de Internet de que tendrán que pagar. http://www.eitb.eus/es/videos/detalle/349899/alierta-telefra-advierte-buscadores-internet-tendrrpagar/ (accessed 15 January 2015).

57 The story begun back in April 2014 when Netflix published on its corporate blog that Comcast customers subscribed to Netflix service had been «experiencing poor streaming quality», as streaming speeds had been throttled by Comcast in past months «as a way to force the streaming service to pay more for its videos to get to subscribers». Netflix came to the conclusion that Comcast was not only charging Netflix for transit service, but also for access to its subscribers. And at the same time, Comcast was also charging its subscribers for access to Internet content providers like Netflix. V. Luckerson, «Netflix's Disputes With Verizon, Comcast Under Investigation», Time. June 13, 2014. http://time.com/2871498/fcc-investigates-netflix-verizon-comcast/ (accessed: 15 January 2015); K. Florance, «The Case Against ISP Tolls». *Netflix Blog*. 24 April 2014. Retrieved from:
http://blog.netflix.com/2014/04/the-case-against-isp-tolls.html (accessed: 15 January 2015).

58 FCC, Statement by FCC Chairman Tom Wheeler on broadband consumers and Internet congestion. Washington D.C.: 13 June 2014. Retrieved from: http://www.fcc.gov/document/chairman-statement-broadband-consumers-and-internet-congestion (accessed: 15 January 2015).

mostly on mobile networks. In some cases, the investigation was unable to draw any reliable conclusion on certain practice of restrictions as data provided by broadband operators was «not clear enough». This last finding evidenced an obvious lack of transparency about the practices incurred by operators[59].

At domestic level, data caps practices have been also matter of concern for German Courts. The broadband operator, Deutsche Telekom («DT»), had announced plans to cap data speeds over fixed broadband lines. This meant that, from 2016, customers who had signed up for flat-rate Internet deal and who exceed their monthly data download limit would see their surfing speed capped at 2 megabits per second. In a ruling of 30 October 2013, the Cologne District Court, the *Landgericht Köln* decided that the operator was not entitled to cap transmission speeds when customers who had paid a «flat rate» subscription fee exceeded data limits. The Court held that, at least in the fixed-network market, the term «flat rate» should be construed to mean a «fixed price», paid by the customer for Internet access at a certain broadband speed without any restrictions or hidden additional costs. The disadvantage introduced by DT was unreasonable because the disproportionate reduction in speed to less than 10% of the agreed minimum speed violated the balance between the value of the service and the price paid. In addition, the Court observed that contract with customers had failed to mention any speed caps[60].

Other «neutrality interference» is imposing restrictions on the use of certain applications and/or equipment used by end users. These kinds of restrictions have been suggested to be put in place against the iPlayer streaming and download video platform launched by the British broadcaster BBC. It was found that some access providers, such as British Telecom (BT), appeared to be throttling back iPlayer speeds without noticing their customers[61].

---

59 The investigation concluded that, for instance, in fixed markets, at least 21 % of about 146 millions of broadband users were affected by P2P related restrictions, either technically or contractually; whereas in mobile markets the percentage reached at least 36 % of about 214 millions of broadband users. In mobile markets, at least 21 % of broadband users are affected by VoIP related restrictions, either technically or contractually. In this later case, the investigation highlighted that the data was not clear enough to enable reliable conclusions to be drawn about the remaining 18% of mobile broadband users who might or might not face such restrictions. See Berec, A view of traffic management and other practices resulting in restrictions to the open Internet in Europe. Findings from Berec's and the European Commission's joint investigation. BoR (12) 30, 29 May 2012, at p. 21. Retrieved from: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20Berec_2.pdf (accessed 15 January 2015).

60 Landgericht Köln Judgment of 30.10.2013, Az.: 26 O 211/13, at paras. 49-52. Retrieved from: http://www.justiz.nrw.de/nrwe/lgs/koeln/lg_koeln/j2013/26_O_211_13_Teil_Anerkenntnis_und_Schlusurteil_20131030.html(accessed: 20 December 2014).

61 The iPlayer is a peer-to-peer (P2P) application that allows subscribers to view recent BBC programmes free of charge by streaming or downloading them. The success of the service drove significant demand for bandwidth to the extent that some Internet access providers acknowledged having been engaged

IV. CODIFYING NET NEUTRALITY: MARKET APPROACHES ON EUROPE AND UNITED STATES

To grasp the nettle of foregoing concerns about net neutrality, legal framework in the European Union (the «EU») and the United States (the «US») has been characterised by two features.

On the one hand, to a greater or lesser extent national proposals have codified the principle, even though quite often such recognition is a vague formula which lacks clear-legislative measures to enforce the principle[62].

On the other hand, legislative attempts to address net neutrality issues have been specifically focus on the quality of the service provided in relation to the price paid for the bandwidth used and access speed, the requirement of transparency about traffic management practices run by broadband providers, and general restrictions to unreasonable, discriminatory and unjustified blocking or degradation of services, applications and contents over the Internet[63].

Although addressing market power, only when necessary, has been historically the regulatory philosophy undertaken by the EU and the USrelated to open Internet issues[64], effective regulation of last mile fixed and mobile access in both contexts have responded to different market realities.

Most scholars are of the view that the US is far different from Europe in relevant aspects of market structure, regulatory framework, and competition law. Whereas effective regulation of last mile fixed access in Europe has seemingly ensured a strong competition and meaningful choice of broadband network operators for end users, US fixed broadband markets constitute a series of *de facto* duopolies, with no effective competition, and thus, serious limitations on consumers choice. As a result of this, in the European market this competition has likely reduced the incentives of broadband

in dropping speed of those users who downloaded large files at peak times. In fact, the fine print of its fair policy posted on BT website included a clause saying: «[W]e do limit the speed of all video streaming to 896 Kbps on our Option 1 product, during peak times only, which is between 5pm - midnight every day». See R. Cellan-Jones. BBC v BT. BBC News: dot.life [blog]. 2 June 2009. Retrieved from: http://www.bbc.co.uk/blogs/legacy/technology/2009/06/iplayerbbc_v_bt.html (accessed 15 January).

62 In this sense, European Commission openly recognises that there are «no clear rules on net neutrality today at EU level, leaving 96% of Europeans without legal protection for their right to access the full open internet». See EUROPEAN COMMISSION. Digital Agenda for Europe. A Europe 2020 Initiative. Retrieved from: https://ec.europa.eu/digital-agenda/en/eu-actions (accessed 5 May 2015).

63 *Cfr.* P.A. Asensio. «Caracterización y organización de internet: perspectiva jurídica», *Derecho Privado de Internet*. Estudios y Comentarios Legislativos, Civitas-Aranzadi, Cizur Menor, 2015, at pp. 5-6; J. Barata, *cit*. at pp. 48-49.

64 K.R. Carter, *cit*, at p. 40.

operators to deviate from network neutrality in harmful ways. Meanwhile, in absence of rules until recently, US regulator would have no ability to prevent or remedy network neutrality harms [65].

1. Net neutrality in Europe: addressing competition and consumer protection

In the EU, policies over net neutrality and open Internet have relied on the following regulatory aspects: (i) the explicit adoption of the net neutrality principle in late 2009 after the amendment of the Directive 2002/21/EC, of 7 March 2002, on a Common Regulatory Framework for Electronic Communications Networks and Services (the «Framework Directive») [66], by establishing establish the right of end-users to access content, applications or services of their choice; (ii) requiring a minimum quality of service (the «QoS») standards on network operators; (iii) the enforcement of transparency rules to ensure that consumers are informed of the relevant practices of their network operators related to Internet traffic management; (iv) vesting European Commission and Member State National Regulatory Authorities (NRAs) with supervisory and sanctioning powers, thereby shaping competition law as an *ex post* remedy for violations broadband providers who have Significant Market Power (SMP).

The regulatory basis of the net neutrality has been broadly established by Article 8 (4) (g) of the Framework Directive. The said provision imposes NRAs the obligation of fostering competition amongst electronic communications networksservices by, *inter alia*, «promoting the ability of end users to access and distribute information or run applications and services of their choice».

Completing the provision of the Framework Directive, the Article 20(1)(b) of the Directive 2002/22/EC, of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (the «Universal Service Directive») places obligations on access providers of transparency with regards the information provided to end users.

Accordingly, contracts with end users shall include, in «a clear, comprehensive and easily accessible form», specific information covering, such as the minimum levels of QoS offered, traffic management policies and any limits to services or applications. In particular, the provision establishes that contracts shall specify: (i) «information on any other conditions limiting access to and/or use of services and applications»; (ii) «the minimum service quality levels offered, namely the time for the initial connection and, where appropriate, other quality of service parameters, as defined by the national regulatory authorities»; (iii)

65 M.J. Scott et al. *Network Neutrality*, *cit.*, at p. 15.

66 See Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009.

«information on any procedures put in place by the undertaking to measure and shape traffic so as to avoid filling or overfilling a network link, and information on how those procedures could impact on service quality».

In addition, Articles 21(3)(c) and (d) of the Universal Service Directive also empower NRAs to impose Internet access providers the obligation «to publish transparent, comparable, adequate and up-to-date information on standard terms and conditions in respect of access to, and use of, services provided by them to end-users and consumers», which shall include specific information on the QoS offered, traffic management policies and any limits to services or applications operated by access providers.

Finally, Article 22(3) of the Universal Service Directive introduces the competence of NRAs to set minimum Quality of Service (QoS) requirements «[i]n order to prevent the degradation of service and the hindering or slowing down of traffic over networks».

In order to assess how to best enforce the aforesaid provisions, the Berec has released a series of reports analysing a variety of aspects such as transparency in traffic management practices[67], degradation of services with respect to the QoS[68], or differentiation practices operated by broadband providers which may pose competition issues in the context of net neutrality[69].

The Europe 2020 Strategy (EU2020) and one of its flagship initiatives, the Digital Agenda for Europe (DAE), have established that broadband connectivity is of strategic importance for European growth and innovation in all sectors of the economy and for social and for territorial cohesion. In such context, by September 2013, the European Commission launched a draft regulation on the European single market for electronic communications in which it proposed to harmonise rules to ensure unhindered connection to all content and services (except where necessary for «reasonable» traffic management) in the «public» internet[70].

---

67 Berec, *Guidelines on Transparency in the scope of Net Neutrality: Best practices and recommended approaches*. [BoR (11)67]. Riga: December 2011. http://berec.europa.eu/doc/berec/bor/bor11_67_transparencyguide.pdf

68 Berec, *A framework for Quality of Service in the scope of Net Neutrality.* [BoR (11)53], Riga: 8 December 2011. Retrieved from http://berec.europa.eu/doc/berec/bor/bor11_53_qualityservice.pdf

69 Berec, *A view of traffic management and other practices resulting in restrictions to the open Internet in Europe. Findings from BEREC's and the European Commission's joint investigation*. BoR(12)30. 29 May 2012. http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20Berec_2.pdf

70 EUROPEAN COMMISSION, Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012, COM (213)627 final, Brussels: 11 September 2013.

The proposed regulation recognises a bundle of end users rights which are intended to «safeguard access to the open internet»[71], namely, the elimination of discriminatory requirements or conditions of access or use to end-users (Article 21.1), freedom to provide and avail of open internet access, and prohibition of blocking, slowing down, degrading or discriminating against specific content, applications or services, except where necessary to apply reasonable traffic management measures (Article 23), safeguards for quality of service (Article 24), transparency and publication of information, especially with regards to actually available data speed for download and upload in the end user's Member State of residence, including at peak-hours, level of applicable data volume limitations, actually available speed and other quality parameters, measures taken to avoid traffic congestion (Article 25), and information requirements for contracts with end users (Article 26).

2. Net neutrality in the United States: from non-intervention to codification

By contrast, in United States regulatory policies on the Internet have been traditionally flexible and discouraging of governmental regulation. In fact, first approaches of US policies on net neutrality were led by a non-intervention principle in broadband market and lack of regulation.

The statements made by the former FCC's Chairman, Michael K. Powell, on 8 February 2004, in its *Preserving Internet Freedom*, inaugurated this non-intervention policy age. He observed that «broadband consumers generally enjoy such internet freedom» and «they can access and use the content, applications and devices of their choice»[72]. Consequently, first FCC's policy would consist on giving «the private sector a clear road map by which *it can avoid future regulation* on this issue by embracing unparalleled openness and consumer choice. [Emphasis added]»[73].

Reinforcing Chairman Powell's guidance, the Commission unanimously approved the *Internet Policy Statement* on 2005[74] whereby it established four general Internet policy principles. Specifically, subject to «reasonable network management», the

71 See para. 3.4 of the Explanatory Memorandum or the Proposal.

72 M.K. Powell, «Preserving Internet Freedom: Guiding Principles for the Industry», Silicon Flatirons Symposium on «The Digital Broadband Migration: Toward a Regulatory Regime for the Internet Age» (Preserving Internet Freedom), (8 February 2004), at p. 3. Retrieved from: https://apps.fcc.gov/edocs_public/attachmatch/DOC-243556A1.pdf (accessed: 20 December 2014).

73 *Id.* at p. 5. Such guidelines could be summarized as follows: (i) Freedom to Access Content. (ii) Freedom to Use Applications and to Attach Personal Devices. (iii) Freedom to Obtain Service Plan Information.

74 FCC, Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, (Internet Policy Statement) [GN Docket No. 00-185, CC Docket Nos. 02-33, 01-33, 98-10, 95-20, CS Docket No. 02-52, Policy Statement, 20 FCC Rcd 14986, 14987-88], (5 August 2005). Retrieved from: https://apps.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf (accessed: 20 December 2014).

principles entitle consumers to (i) access the lawful Internet content of their choice; (ii) run applications and use services of their choice, subject to the needs of law enforcement; (iii) connect their choice of legal devices that do not harm the network; and (iv) enjoy competition among network providers, application and service providers, and content providers[75].

Since then, the story of net neutrality in the US can be summarised as the FCC's attempts to assert its authority by placing specific requirements on Internet access providers in order to prevent unreasonable and discriminatory network management practices. In short, the threshold question has resided in the statutory qualification of Internet access services under the Telecommunications Act of 1996: whether an «information service» pursuant to the Title I of the Actor a «telecommunication service» subject to *common carriage* provisions of Title II. Whereas under common carrier regulations the FCC could place on telecommunication providers strict statutory requirements to offer their services to all customers at reasonable prices and to refrain from discriminating in the provision of those services, Title I provided the FCC with a very limited authority to regulate information services directly. Ironically, to a large extent, much of the judicial review incurred on account of FCC orders to address net neutrality issues derived from the Commission own decision to classify Internet as an «information service» in 2002 upheld three years later by the Supreme Court[76].

In 2007, several parties filed complaints with the Commission alleging that Comcast was interfering with its customers' use of peer-to-peer applications[77] in violation of the *Internet Policy Statement*. The Commission concluded in a 2008 Order that the company's practice contravened federal policy by «significantly imped[ing] consumers' ability to access the content and use the applications of their choice». Comcast challenged that

[75] The Commission applied open Internet principles of 2005 in the context of particular enforcement proceedings. In effect, just before the Commission adopted the Internet Policy Statement, the Enforcement Bureau had entered into a consent decree with Madison River Communications, a telephone company and provider of digital subscriber line (DSL) service, arising from complaints by Vonage that Madison River was blocking ports that were typically used by Vonage customers to make Voice over Internet Protocol (VoIP) telephone calls. The consent decree required Madison River to stop blocking VoIP ports and refrain from otherwise inhibiting customers from using the VoIP applications of their choice.

[76] In its Cable Broadband Order (2002), the Commission decided to treat the provision of broadband Internet access by cable providers as «an information service». As a result of this interpretation, Internet access services were exempt from Title II common carrier regulations. In fact, the Supreme Court upheld the FCC's decision in National Cable & Telecommunications Ass'n v. Brand X Internet Services, 545 U.S. 967 (2005). The Court found that the definitions of telecommunications service and information service in the Communications Act were ambiguous, and as a result, it was within the FCC's discretion to determine which regime should be applied to Internet access services.

[77] Such applications allow users to share large files directly with one another without going through a central server, but also can consume significant amounts of bandwidth.

decision in the D.C. Circuit, arguing that the Commission lacked authority to impose obligations on broadband providers. On 6 April of 2010, the D.C. Circuit granted Comcast's petition for review and vacated the Commission's enforcement decision.

While the Comcast case was pending, the Commission issued the *2010 Open Internet Order* adopting some basic rules in order to enforce the net neutrality principle.[78] Nevertheless, Verizon challenged the *2010 Open Internet Order* before the D.C. Circuit on several accounts. On the one hand, once again, it was argued that the Commission lacked statutory authority to adopt the rules; on the other hand, that the rules violated First and Fifth Amendments of the Constitution.

On 14 January 2014, the D.C. Circuit ruled on Verizon's challenge to the Open Internet Order. Although the Court rejected Verizon's challenge to the transparency rule, it however struck down the «anti-blocking» and «anti-discrimination» rules. The District Court held that the blocking and non-discrimination rules violated the Communications Act of 1996 by imposing *common carriage* regulations on an information service. In response, the FCC on 15 May 2014 launched a new rulemaking processseeking public comment on how best to protect and promote an open Internet and to «close the gap» of absence of legally enforceable standards[79].

Finally, on 26 February 2015, the FCC passed by a 3-2 vote the new *Open Internet Order*. In its Order, the Commission found that the nature of broadband Internet access service has changed since its initial classification as «information services», basically because «broadband providers have even more incentives to interfere with Internet openness today». In fact, according the 2015'Order the record reflects that«broadband providers hold all the tools necessary to deceive consumers, degrade content, or disfavour the content that they don't like».

78 First, the Order imposed a transparency rule, requiring both fixed and mobile providers to «publically disclose accurate information regarding the network management practices, performance, and commercial terms» of their broadband Internet access service. The rule specified that such disclosures be «sufficient for consumers to make informed choices regarding the use of such services and for content, application, service, and device providers to develop, market, and maintain Internet offerings». Second, the Order adopted anti-blocking requirements. The rule barred fixed providers from blocking «lawful content, applications, services, or non-harmful devices subject to reasonable network management». It prohibited mobile providers from blocking «consumers from accessing lawful websites», as well as «applications that compete with the provider's voice or video telephony services» subject to «reasonable network management». Third, the Order adopted an anti-discrimination rule for fixed providers, barring them from «unreasonably discriminat[ing] in transmitting lawful network traffic» subject to «reasonable network management».

79 See FCC, Protecting and Promoting the Open Internet, GN Docket No. 14-28, Notice of Proposed Rulemaking, FCC 14-61 («Open Internet NPRM»), Washington D.C.: 15 May 2014, at para. 9. Retrieved from: https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-61A1.pdf (accessed: 15 January 2015).

To respond to this changing landscape, the new Open Internet Order establishes the FCC's legal authority to fully address potential threats to openness networks by reclassifying broadband Internet access as a telecommunications service under Title II of the Communications Act. In addition, while the FCC's *2010 Open InternetOrder* had limited applicability to mobile broadband, the new 2015 rules would apply to fixed and mobile broadband alike, protecting consumers no matter how they access the Internet, whether on a desktop computer or a mobile device.

For the FCC, there are three specific practices which invariably harm the open Internet: blocking, throttling and paid prioritization. The Order bans each of them applying the same «bright-light rules» to both fixed and mobile services [80].

Not all the stakeholders have applauded the new Order. Some believe that the FCC's new Open Internet Order is «an attempt to undo two decades of bipartisan consensus against heavy-handed government control of the Internet». It is thought that the best policy for the Internet should be «to maintain the 'Hands off the Net' approach», in which the role to be performed by regulators is remaining vigilant and to intervene «only where there is clear evidence of actual harm» [81].

Neither has there been a general agreement within the Commission. In his statement against the *2015 Open Internet Order*, the dissenting FCC Commissioner Ajit Pai objected that broadband Internet access reclassification as telecommunication service should be deemed as a «radical departure» from and an abandonment of «the bipartisan and market-oriented policies» agreed by republicans and democrats by the time of the

[80] The «No Blocking rule» states that consumers who subscribe to a retail broadband Internet access service must get what they have paid for –access to all (lawful) destinations on the Internet. Thus the Order adopts a straightforward ban: any person engaged in the provision of broadband Internet access service, shall not block lawful content, applications, services, or non-harmful devices, subject to reasonable network management. According to the «No Throttling rule», the 2015 Order prevents any person engaged in the provision of broadband Internet access service from impairing or degrading lawful Internet traffic on the basis of Internet content, application, or service, or use of a non-harmful device, subject to reasonable network management. Under «No Paid Prioritization rule», such practice occurs when a broadband provider accepts payment (monetary or otherwise) to manage its network in a way that benefits particular content, applications, services, or devices. To protect against «fast lanes», the Order adopts a rule that establishes that any person engaged in the provision of broadband Internet access service shall not engage in paid prioritization. Finally, pursuant to the «Transparency rule», any person engaged in the provision of broadband Internet access service shall publicly disclose accurate information regarding the network management practices, performance, and commercial terms of its broadband Internet access services sufficient for consumers to make informed choices regarding use of such services and for content, application, service, and device providers to develop, market, and maintain Internet offerings.

[81] E. Swarztrauber, «Dear Chairman Wheeler, Don't Break The Net!» *Tech Freedom*, 2 September 2014. http://techfreedom.org/post/96440064567/dear-chairman-wheeler-dont-break-the-net (accessed: 20 December 2014).

enactment of Telecommunications Act of 1996. This Order —the Commissioner said— «seizes unilateral authority to regulate Internet conduct, to direct where Internet service providers put their investments, and to determine what service plans will be available to the American public» [82].

3. Common relief for net neutrality deviations: the reasonableand non-discrimination rule

It is clear from both regulatory frameworks that the main challenge of public policies on net neutrality is to determine which traffic management practices are reasonable to handle congestion of networks, or on the contrary, which of those practices may harm interests of end users and competitors.

In doing so, it is worth noting that public policies in both US and Europe codifying the net neutrality principle usually include commitments with the non-discrimination principle, by meaning that «all traffic on the Internetis treated *equally*, whatever its source, content or destination», and in «absence of *unreasonable discrimination* on the part of network operators in transmitting Internet traffic» [83].

For instance, the Norwegian Communications Authority, the Nasjonal Kommunikasjonsmyndighet (NKOM), stresses that the main goal of network neutrality is to ensure that «the Internet remains an open and non-discriminatory platform for all types of communication and content distribution» [84]. In the same way, the Organisation for Security and Co-operation in Europe (the «OSCE») is of the view that net neutrality principle should apply by enabling users to run any application or to access any service of their choice «without the traffic related to the services they use being managed, prioritized or discriminated by the network operators» [85].

As some commentators point out, «[…] it is necessary a guarantee that intervention of ISPs over [the Internet] traffic will not unduly hamper such exchanges (either by giv-

82 FCC, Dissenting Statement of Commissioner AjitPai on Protecting and Promoting the Open Internet, (GN Docket No. 14-28), 12 March 2015, at p. 1. Retrieved from: http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0312/FCC-15-24A5.pdf (accessed 15 March 2015).

83 M.J. Scott, P. Nooren, et al., *cit*, p. 17.

84 See Nkom. Network neutrality. Guidelines for Internet neutrality. [Version 1.0].Post-ogteletilsynet, 24 February 2009, at p. 2. Retrieved from: http://eng.nkom.no/technical/internet/net-neutrality/the-norwegian-model/_attachment/9222?_ts=1409aa375c1 (accessed: 15 January 2015).

85 Y. Akdeniz, Report on Freedom of Expression on the Internet. A study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States, OSCE, September 2010, at p. 40. Retrieved from: http://www.osce.org/fom/80723?download=true (accessed 15 January 2015).

ing priority to some providers to the detriment of others, or by blocking or making very difficult the access to some offers)»[86].

In this sense, non-discrimination as a necessary consequence of net neutrality has been embraced to a greater or lesser extent by domestic legislations in Europe. For instance, the *Spanish Law 9/2014, of 9 May,on Telecommunications*, endorses both principles when it establishes that the goals of legislation on electronic communications: on the one hand, the promotion of the development of electronic communication networks services by «enhancing connectivity and end-to end interoperability and its *access onequal conditions and with non-discrimination*» (Article 3.c); on the other hand, the protection of users interests, by «ensuring their right to access to electronic communication services on suitable conditions of choice, price and good quality, enhancing the ability of end users to access and disseminate the information or use applications and services of their choice in particular through *access to an open Internet*» (Article 3.j).

Thus, the problem is how to draw theline between reasonable practicesand unreasonable and discriminatory traffic management practices resulting in unduly interferences with net neutrality. For example, by stablishing the bright-line bans on blocking, throttling, and paid prioritization, the 2015 FCC Order prevents broadband providers from engaging in «*unreasonably interfere(nce) with or unreasonably disadvantage* (i) end users' ability to select, access, and use broadband Internet accessservice or the lawful Internet content, applications, services, or devices of their choice, or(ii) edge providers' ability to make lawful content, applications, services, or devices available to end users». But also,the Order clearly establishes that: «*Reasonable* network management shall not be considered aviolation of this rule».

When analyzing whether a conduct satisfies the «no-unreasonable interference/disadvantage standard» to protect the open Internet, the 2015 Order proposes «a case-by-case approach» considering a set of concurring circumstances: (i) the degree of end user control and choices in the use of Internet; (ii) the competitive effects on edge-providers of the measures applied by the operator; (iii) the consumer protection standard prohibiting broadband providers from employing any deceptive or unfair practices (e.g. in billing or failures in protecting the confidentiality of end user's proprietary information); (iv) the effect on innovation, investment, or broadband deployment; (v) the existence of application-agnostic practices which do not discriminate between end users and edge-providers in the application of traffic management measures; (vi) the existence of standard practices adopted by open, broadly representative, and independent Internet engineering, governance initiatives, or standards-setting organization; (vii) the transparency and disclosure

[86] J. Barata, *cit*, at p. 46.

of the traffic management practices; (viii) and importantly, the degree of impairment of freedom of expression by the traffic management practices (e.g. blocking contents)[87].

V. A FUNDAMENTAL RIGHTS-ORIENTED APPROACH ON NET NEUTRALITY

Contrary to some opinions[88], there is a wide consensus on the idea that net neutrality is more than an architectural design principle more or less endorsed by legislations. In this sense, it is argued that protecting a free and open Internet not only fosters innovation and competition and protect users' ability to choose the network they want free from providers, but it also preserves fundamental rights[89].

In fact, understanding of Internet as a democratic forum where free speech rights can be enhanced and fully exercised is common a place since early Court decisions involving this new medium. In *ACLU v. Reno* (1996), the US District Court for the Eastern District of Pennsylvania described Internet as a democratic and public forum:

«It is no exaggeration to conclude that the Internet has achieved, and continues to achieve, the most participatory marketplace of mass speech that this country —and indeed the world— has yet seen. The plaintiffs in these actions correctly describe the «democratizing» effects of Internet communication: individual citizens of limited means can speak to a worldwide audience on issues of concern to them»[90].

It is clear from European Court of Human Rights (the «ECHR») jurisprudence, that access to Internet plays a relevant role in the exercise of freedom of expression:

«In the light of its *accessibility* and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the *public's access* to news and facilitating the dissemination of information in general»[91].

In Europe, some national jurisdictions have recognised access to the Internet as a part of the more general right to freedom of expression. For instance, the French Constitutional Council has openly stated that freedom of expression implies freedom of access to

87 FCC, *2015 Open Internet Order*, *cit*, at paras. 138-145.

88 See L. Downes, VC/DC - «When Internet 'Neutrality Principles' Conflict With Engineering, Everyone Loses». Forbes. 12 September 2014. Retrieved from: http://www.forbes.com/sites/larrydownes/2014/09/12/vcdc-when-internet-neutrality-principles-conflict-with-engineering-everyone-loses/ (accessed: 15 January 2015). The author thinks that «[i]n reality, «net neutrality» is at best an engineering principle—a legal academic's term for the underlying packet-switching architecture of the Internet […]»

89 DLA Piper, *cit*., at p. 13.

90 *ACLU v. Reno*, 929 F. Supp. 824, at 881 (E.D. Pa. 1996). See footnotes 18 and 20 *supra*.

91 *Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2)* (nos. 3002/03 and 23676/03, at para. 27, ECHR 2009); *Ahmet Yildirim v. Turkey*, (no. 3111/10, at para. 48, ECHR 2012).

the Internet, and restrictions on the public's right to access online communication services could be ordered only by a judge, following a fair trial, and have to be proportionate [92].

1. The public service value and democratic implications of net neutrality

As Mercedes Fuertes says, «[p]ublic services and infrastructures depend upon the Internet much more» [93]. The iPlayer case referred above also poses a further interesting question on whether degradation of services, applications and contents provided online by public broadcasters can be deemed as an interference with the public service remit which they have been vested with, and thus with the underlying democratic values and media pluralism represented by them [94]. Such a case introduces a new element on the net neutrality debate which has to do with the extension of public service remit to the Internet.

«A current issue in the debate over the future of [Public Sector Broadcasting] is the means and the legitimacy of extending its scope to cover the variety of platforms used by viewers to access broadcast content, from digital terrestrial television on IPTV and mobile services» [95].

Behind the net neutrality principle there are also public policies choices. Importantly, the regulator has recognised the public service value underlying the open Internet. For instance, the Ofcom opines that, by enforcing clear and consistent net neutrality rules, access to an open Internet would enable citizens to access «a range of public services over the internet» and «to participate in the process of public debate and democracy» [96].

The European Council has widely embraced the public service value emerging from the Internet. In its Recommendation (2007)16, of the Committee of Ministers to member states on measures to promote the public service value of the Internet, adopted on 7 November 2007, it is stressed that the Internet and other ICT services have «high public service value in that they serve to promote the exercise and enjoyment of human rights and fundamental freedoms for all who use them, and that their protection should be a priority with regard to the governance of the Internet». And it extends the «remit of public service media», in line with the Recommendation (2007)3, of the Committee of Ministers to member states on the remit of public service media in the information society, adopted on 31 January 2007, so as to cover the Internet and other new communication services.

---

92 Decision of 10 June 2009, no. 2009-58 DC.

93 M. Fuertes, *Neutralidad de la red: ¿realidad o utopia?*, Marcial Pons, Madrid, 2014, p. 12.

94 See the Amsterdam Protocol of 1997 on the System of the Public Broadcasting in the Member States in the context of the European Union.

95 D. Goldberg, G. Sutter, I. Walden, *Media Law and Practice,* Oxford University Press. Oxford, 2009, at p. 30.

96 Ofcom, *cit.*, par. 1.21.

In the same way that, almost twenty years ago, the Amsterdam Protocol recognised the public service value of broadcasting, today the Council of Europe clearly assumes the role played by the Internet and its services providers in democratic societies: it has a public service value and it is a mean to exercise human rights: «Internet service providers (ISPs), in providing the basic infrastructure and the basic services that allow users to access and use the Internet and thereby exercise their rights to benefit from the information society, deliver services with a significant public service value to society». In this sense, all ISPs (Internet access, proxy caching, hosting, search engines providers), have a «unique position and possibility of promoting the exercise of and respect for human rights and fundamental freedoms». In addition, the provision of Internet services is increasingly becoming a «prerequisite for a comprehensive participatory democracy» [97].

Some opine that this public service value is better represented the public Internet lane in contrast to the managed Internet lane.

From its beginning, the open and public Internet lane has allowed any end user to access any content, application or service because data packets are transmitted on a *best-efforts basis*, regardless of what type of data is transmitted [98].

In this public lane model, the broadband provider provides an Internet access service to the end user, through which the user will gain access to the information and the applications on the public Internet. In this public Internet lane, if the end user wishes to access specific content, services or applications, he is likely to enter into an agreement or contract with a content provider (such as the online video services Netflix or Wuaki.tv or the streaming music services iTunes or Spotify).

Under best-efforts' Internet access, «network operators attempt to convey all traffic on more or less equal terms» [99], but with *no delivery guarantee*, which means that in cases of traffic peaks, there is no assurance that packets reach their end point without delaying or dropping [100]. As the Ofcom says, on a best-effort basis, this public Internet lane «results in an «open internet with no specific services being hindered or blocked, although some may need to be managed during times of congestion» [101].

---

97 COUNCIL OF EUROPE, *Human rights guidelines, cit.*

98 R. Davids, «Net neutrality in Europe» [Briefing], *European Parliamentary Research Service*, 23 March 2014, p. 2. Retrieved from: http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140773/LDM_BRI(2014)140773_REV2_EN.pdf (accessed: 15 January 2015).

99 *Ibíd.*

100 K.R. Carter, M.J. Scott, C. Wernick, *Net Neutrality: Implications for Europe*. Bad Honnef: Wissenschaftliches Institut für Infrastruktur und Kommunikations-dienste, December 2008, at p. 36. http://ssrn.com/abstract=1522039 (accessed: 21 December 2015).

101 Ofcom. *Ofcom's approach on net neutrality*. 24 November 2011, par. 1.4. Retrieved from: http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/statement/statement.pdf [accessed 20 December 2014).

The best-efforts approach is considered to be more consistent with net neutrality and open Internet as it «implies that bottlenecks in the transmission path or network congestion will lead to data packets being held, rerouted or dropped on a random basis»[102].

Nevertheless, public policies may spur different business models resulting in either public Internet lane or managed services lane, and the establishment of a minimum quality of service in Internet access concretised in best-effort service or differentiated IP-based service.

In effect, broadband providers are increasingly providing IP-based services along with Internet access service over their DSL, cable or fibre infrastructure, such as IPTV or IP telephony. Although such value-added services are delivered over the same network infrastructure as the Internet access service, they are offered as «managed or specialized services». In this «managed service» lane, the broadband provider usually enters an agreement with the end user to provide him specific services.

Unlike the best-efforts public Internet lane, where no measures are taken to guarantee the quality of specific services, in the «managed service» lane, the broadband provider takes measures to guarantee a quality of the service by the reservation of dedicated bandwidth. In doing so, broadband providers may have the economic incentive and the technical ability to disfavour access to not affiliated content, application or services by blocking, throttling or to prioritize their managed services to the detriment of the public Internet lane, resulting in Internet fast lanes in contrast to public Internet lanes[103].

For instance, by implementing access-tiering, access providers no longer transmit data on a *best-efforts* basis as they have an incentive to give priority to the delivery of packets from content providers who have paid for such priority to the detriment of non-paying providers.

Furthermore, the democratic implications of net neutrality have been suggested by some. Tim Berners-Lee, the founding father of the World Wide Web, has highlighted this aspect of the principle:

«One of the ways in which we protect the Web is by ensuring Net Neutrality. Net Neutrality is about non-discrimination. Its principle is that if I pay to connect to the Net with a certain quality of service, and you pay to connect with that or a greater quality of

[102] DLA Piper, *cit.* at p. 13.

[103] For obvious reasons, edge providers are more interested in the application of the best-effort service (public Internet lane) instead of managed or specialized services (fast lane). The popular streaming video service Netflix says there can be no «prioritization» of content delivered to end users by last-mile providers in a best-efforts network, where «all packets necessarily move at the same speed». See Comments of Netflix, Inc. on Protecting and Promoting the Open Internet, GN Docket No. 14-28, at p. 6 (filed 15 July 2014). Retrieved from http://apps.fcc.gov/ecfs/document/view?id=7521491186 [accessed 15 January 2015].

service, then we can both communicate at the same level. This is important because it allows an open, fair market. It's essential to *an open, fair democracy*»[104].

The FCC is firmly convinced of the fact that «[o]penness also is essential to the Internet's role as a platform for speech and civic engagement. An informed electorate is critical to the health of a functioning democracy […]. Due to the lack of gatekeeper control, the Internet has become a major source of news and information, which forms the basis for informed civic discourse»[105].

In the same line, Barbara van Schewick explains that net neutrality is intended to foster not only innovation in applications or to protect users' ability to choose how they want to use the Internet free from network providers' interference, but also to enhance «the Internet's ability to improve democratic discourse, facilitate political organization and action and to provide a decentralized environment for social, cultural and political interaction in which anyone can participate»[106].

2. **Is there a right to Internet access?**

But one thing is that access to the Internet can be considered as «an enabler of rights», and a very different issue is that such access shall be deemed as a «right itself». More than a human right, Cerf opines that Internet access is actually civil right in the sense that it is conferred upon us by law. Particularly, he observes that broadband Internet come close with notion of «universal service»[107]: the idea that, as well as telephone service and electricity, Internet access must be available even in the most remote regions of the country. «When we accept this idea, -the author says- we are edging into the idea of Internet access as a civil right, because ensuring access is a policy made by the government»[108].

As the Council of Europe declared in 2010, it seems to be clear that «access to infrastructure is a prerequisite for the realisation» of net neutrality and open Inter-

[104] T. Berners-Lee, The many meanings of Open. [blog] Telefonica Innovation Hub, 9 October 2013. http://blog.digital.telefonica.com/2013/10/09/tim-berners-lee-telefonica-open-agenda/ (accessed: 15 January 2015).

[105] FCC, *2010 Open Internet Order, cit.*, at para. 13.

[106] B. Van Schewick, Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like, The Center for Internet Society, 11 June, 2012, at p. iv. Retrieved from: http://cyberlaw.stanford.edu/files/publication/files/20120611-NetworkNeutrality_0.pdf (accessed: 21 December 2014).

[107] In fact, the concept of universal service related to Internet access has been embraced by European Directives to ensure the availability of a minimum set of high-quality fixed location and telephone services, including functional Internet access, to all users at affordable prices, without distortion of competition. See Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).

[108] V.G. CERF, «Internet Access Is Not a Human Right». The New York Times, 4 January 2012. Retrieved from: http://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html?_r=2&ref=opinion (accessed 5 May 2015).

net.[109] Thus, the foregoing debate on net neutrality and the threats over the open Internet poses fundamental questions. Is there a right to Internet access? And if so, in which terms should this right be granted?

Accordingly, some Spanish scholars wonder whether net neutrality can be deemed as «a citizen right liable to be exercised against third parties pursuant to the specific systems of guarantees established for any right»; or, on the contrary, whether the net neutrality is a mere «regulatory principle» which governs the legal authority of Administrations over electronic communications and public policies on the Internet[110].

The prevailing opinion amongst international actors —such as the United Nations, the European Union, the Organization for Security and Co-operation in Europe (OSCE), the Council of Europe, the ITU— is that access to Internet should be recognised as a fundamental right[111].

In *Ahmet Yildirim v. Turkey* (2012), the ECHR has gone further by recognizing a «right to Internet access» and the «positive obligation»of the State to guarantee it:

«A survey carried out by the Court of the legislation of twenty member States […] reveals that the *right to Internet access* is protected in theory by the constitutional guarantees applicable to freedom of expression and freedom to receive ideas and information. The right to Internet access is considered to be *inherent in the right to access information and communication* protected by national Constitutions, and encompasses the right for each individual to participate in the information society and the *obligation for States to guarantee access to the Internet for their citizens*. It can therefore be inferred from all the general guarantees protecting freedom of expression that a right to unhindered Internet access should also be recognised»[112].

Based upon constitutional legislations, the ECHR infers that the right to Internet access is inherent to the right to receive ideas and opinions. Nevertheless, the unclear language of the Strasbourg Court («in theory», «a right to unhindered Internet access should be recognised»)[113] raises some interesting questions.

---

[109] Declaration of the Committee of Ministers on Network Neutrality, adopted on 29 September 2010, at para. 4.

[110] J. Barata, *cit.*, p. 48.

[111] J. Pelkonen (Rapporteur), *The right to Internet access*. Parliamentary Assembly of the Council of Europe [Doc. 13434], Strasbourg: 4 March 2014.

[112] *Ahmet Yildirim v. Turkey* (Application no. 3111/10, §31, ECHR 2012).

[113] What is the meaning of «in theory»? Does I mean that the State has a margin of appreciation to determine the scope of the right to Internet access? What is the meaning of «unhindered» Internet access? Absence of restrictive legal provisions on Internet access which do not meet the triple test of legality, proportionality and necessity or legal provisions prohibiting unreasonable and discriminatory traffic management practices?

First, to what extent the State should guarantee Internet access as a fundamental right or how constitutional guarantees of freedom of expression should be applied to the right to Internet access still remain to be discerned far beyond the ECHR general declaration. Simply put, the statement of Court includes Spain in the list of the member States which «in theory» would protect the right to Internet access through constitutional guarantees applicable to freedom of expression and freedom to receive ideas and information. Does it mean that also, «in theory», specific guarantees set forth in Articles 20 and 53 of the Constitution should apply the right to Internet access? For instance, should an appeal of unconstitutionality against statutory legislation contravening the right to Internet access be feasible? Answers should be carefully drafted[114].

Secondly, the ECHR judgment does not determine the content and the scope of the positive obligation of the State to guarantee the right to Internet access. This point is relevant because, in reality, what the Court analyses in Ahmet case is whether the application of a legislative measure by a national Court resulting in the wholesale blocking of the access to Google Sites constitutes an State interference with freedom of expression.

In effect, it must be noted that along with the primarily negative undertaking of a State to abstain from interference in the rights guaranteed by the Convention, amongst others, freedom of speech shrined in Article 10, there may be positive obligations inherent in those rights. Nevertheless the scope of the *Ahmet* decision refers to the former aspect rather than the «positive obligations» related to the Internet access. In addition, it is worth to note that the Court has determined the existence of positive obligations on States only on a case-by-case basis rather than articulating a «general theory as to their scope»[115].

Thirdly, the advocacy of a right to Internet access requires analysing the horizontal effect of fundamental rights (Drittwirkung) on this particular ground. In effect, given the fact that Internet access is usually governed by private relationships between broadband providers and end users, a relevant question to be answered is whether or not, in the context of net neutrality deviations, the right to Internet access could have horizontal effects between such private parties[116].

---

[114] Nonetheless, it seems difficult to applied specific guarantees, such as the prohibition of prior censorship, that are constitutionally tailored to protect against public authorities interferences rather than private conducts. *Cfr.* the Judgment of the Spanish Constitutional Court 187/1999, de 25 de October, F.J.5 referring to the concept of «governmental censorship» or censorship by «public authorities». By contrast, see the Judgment 161/2005, of 20 June, F.J. 4 where the Constitutional Court establishes that the statutory right of veto of the editor recognised un the Law on Press and Printing of 1966 (still in force) cannot be confused with prior censorship.

[115] *Cfr.* A. Nicol, G. Millar, A. Sharland, *Media Law* & *Human Rights*, 2nd. edition, OUP Oxford, 2009, p. 20.

[116] For further analysis on the horizontal effects of fundamental right in private relations on account of net neutrality, see M. Fuertes, *Neutralidad de la red, cit.*, at pp. 89-93.

This question can be rephrased by saying whether an end user can invoke his right to Internet access against unreasonable blocking or throttling practices by his broadband provider affecting applicant's fundamental rights, such as freedom of expression or privacy.

Some precedents in Strasbourg jurisprudence could be useful to justify the possible horizontal effect of the right to Internet access in the sense described below. In this sense, the ECHR has held that «in some cases, the State has a positive obligation to protect the right to freedom of expression against violations even from private persons»[117]. On a case-by-case basis, positive obligations could involve the duty to protect freedom of expression in the context of unfair dismissals by an employer:

«This is also the case for freedom of expression, of which the genuine and effective exercise does not depend merely on the State's duty not to interfere, but may require positive measures of protection, even in the sphere of relations between individuals. In certain cases, the State has a positive obligation to protect the right to freedom of expression, even against interference by private persons»[118].

Positive obligations are also required to protect the exercise of freedom of expression against attacks by private persons in a case where a newspaperwas forced to cease publication due to a campaign of acts of violence on journalists and others associated with the newspaper as a result of the Government failure to take measures of protection and to conduct adequate investigations[119].

In determining the scope of a right to Internet access, the Parliamentary Assembly of the Council of Europe recommends the member States to ensure in their domestic legislation such right on the basis of the following principles[120]:

(i) Everyone shall have the right to Internet access as an essential requirement for exercising rights under the European Convention on Human Rights.

(ii) The right to Internet access includes the right to access, receive and impart information and ideas through the Internet without interference by public authority, regardless of frontiers and subject only to the limitations laid down in Article 10 of the European Convention on Human Rights.

(iii) As Internet access is also essential for the exercise of other human rights, such as the right to freedom of assembly and the right to private and family life, member States should recognise the fundamental right to Internet access in law and in practice.

117 *Fuentes Bobo v. Spain* (Application no. 39293/98, §38, ECHR 2000).

118 *Palomo Sánchez and Others v. Spain* (Applications nos. 28955/06, 28957/06, 28959/06 and 28964/06, §58-59, ECHR 2011).

119 *Özgür Gündem v. Turkey* (Application no. 23144/93, §42, ECHR 2000).

120 J. Pelkonen (Rapporteur). *The right to… cit.*, at para. 5.

(iv) Internet access and service providers must comply with universal service requirements regarding the Internet, which have been established for instance by the United Nations and the European Union.
(v) The availability of a minimum quality of Internet services for all is the joint responsibility of member States and Internet access and service providers; particular emphasis should be placed on the affordability, interoperability and integrity of Internet services, taking account of the latest technological developments.
(vi) There should be no discrimination in the treatment of Internet data and traffic, based on the device, content, author, origin or destination of the content, service or application, thus ensuring net neutrality.
(vii) National law and practice should recognise individual Internet access, and any restrictions to this right should be provided by law, pursue a legitimate aim and be necessary in a democratic society.

3. **Deviations of net neutrality impacting on fundamental rights**

Due to this unique nature, the ECHR has stressed that the distinctive characterisation of the Internet as an information and communication tool -particularly distinct from traditional media, in particular as regards the capacity to store and transmit information-, makes the risk of harm to the exercise and enjoyment of human rights and freedoms «certainly higher than that posed by the press» [121].

In effect, far beyond competition, innovation and protection of end users' interests concerns, deviations from net neutrality principle may endanger or hinder fundamental rights. Concerns are mainly focus on the impact of net neutrality deviations of net neutrality on freedom of expression and right to privacy. The BEREc has expressed such concerns in this way:

«There have also been some concerns expressed relating to the effective exercise of fundamental rights and freedoms such as freedom of expression or privacy, that could arise if operators were to give preferential treatment to some kinds of data flows that they consider more valuable (for instance search traffic, which can bring them additional advertising revenue)» [122].

The European Council has observed that certain practices of traffic management operated by broadband providers may affect fundamental rights: «Equally, to the extent

121 *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*, (Application no. 33014/05, §63, ECHR 2011).
122 Berec, BoR (10) 42, *cit.*, at p. 5.

that access-providers may enforce decisions and actions with regard to the accessibility of services (e.g. remove, block or filter content), this can impact on rights and freedoms»[123].

For instance, Comcast, the second largest broadband provider in the United States, was engaged in another net neutrality dispute, when it was accused in 2004 of blocking content for political purposes, as it allegedly had filtered email messages to its subscribers containing the URL *afterdowningstreet.org*, belonging to a coalition of activists who oppose the war in Iraq. The filtering technique examined the content of the email, not the sender's domain or originating IP address. In response to complaints from After Downing Street, Comcast argued that the said URL was on its list of spammer domains; although it failed to explain why the content of the emails including the URL had been being filtered systematically[124].

With regards to arbitrary blocking measures with impact on freedom of expression, some teachings can be learnt from *Ahmet Yildirim v. Turkey* (2012) *supra* cited. In this case, the ECHR examines whether, in the context of judicial proceedings, an injunctive remedy consisting of a wholesale blocking order preventing an indeterminate segment of users from accessing to web services amounted to an interference with freedom of expression as set forth in Article 10 of the European Convention, when the blocking of access results from a prohibition initially imposed on a third-party website which hosts unlawful contents[125].

The concurring opinion to the decision went further qualifying the contested measure as «pure censorship»:

«Thus, any indiscriminate blocking measure which interferes with lawful content, sites or platforms as a collateral effect of a measure aimed at illegal content or an illegal site or platform fails per se the «adequacy» test, in so far as it lacks a «rational connec-

123 COUNCIL OF EUROPE, *Human rights guidelines for Internet service providers*, Strasbourg: Directorate General of Human Rights and Legal Affairs Council of Europe, 2008, at Guideline 6.

124 K.R Carter at al., *cit.*, at pp. 27-28.

125 The Court finds that a measure as such constitutes an interference with Article 10 unless it satisfies a triple test: the measure shall be «prescribed by law», pursues any of the legitimate aims referred to in Article 10.2 and is «necessary in a democratic society» to achieve those aims (§55-56). The Court concludes that the contested measure does not satisfy the «rule of law» criterion as the legislative provision which the measure relies on fails to meet the foreseeability requirement under the Convention (§67). In the Court's view, the measure does not take into consideration, among other elements, whether «a less far-reaching measure could have been taken to block access specifically to the offending website» (such as the blocking of the specific URL of the offending website), or «the fact that such a measure, by rendering large quantities of information inaccessible, substantially restricted the rights of Internet users and had a significant collateral effect». (§ 64-65). Furthermore, the measure in question appears to be in direct conflict with the actual wording Article 10.1 of the Convention, according to which freedom of expression and right to information are secured «regardless of frontiers» (§67).

tion», that is, a plausible instrumental relationship between the interference and the social need pursued. By the same token, blocking orders imposed on sites and platforms which remain valid indefinitely or for long periods are tantamount to inadmissible forms of prior restraint, in other words, to pure censorship».

Cases described above, where blocking measures applied by ISPs (including broadband providers) are the result of compliance with law[126] or the cooperation with Court orders enforcement (e.g. injunctive measures)[127], do constitute what Keimercalls «censorship by proxy».

«The Internet's resistance to direct regulation of speakers and listeners rests on a complex chain of connections, and emerging regulatory mechanisms have begun to focus on the weak links in that chain. Rather than attacking speakers or listeners directly, governments have sought to enlist private actors within the chain as proxy censors to control the flow of information»[128].

According to this argument, last attempt of «censorship by proxy» could be the case *Google Spain SL and Google Inc.v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (2012) where search engines services are required to weigh the competing interests —particularly personal data protection and freedom of expression— on a case-by-case basis, with the judgment to be left to the intermediary on whether or not to delist from the results displayed following a search made on the basis of a person's name links to web pages published by third parties[129].

Keimer observes that: «Putting the censorship decision in the hands of the intermediary allows commercially powerful blocs of customers a potential veto on the speech of others»[130].

With regards to filtering and blocking measures put in place by ISPs, Lessig opines that there is a general lack of awareness of the risk of private censorship:

«It has taken key civil rights organizations too long to recognize this private threat to free-speech values. The tradition of civil rights is focused directly on government action alone. I would be the last to say that there's not great danger from government misbeha-

126 For instance, the «safe harbor» regime set forth in Articles 13-17 of the Spanish Law 34/2002, of 11 July, on Services of Information Society and Electronic Commerce so that ISPs are able to avoid vicarious liability for third parties infringements by using their intermediary services.

127 Article 141.6 of the Spanish Legislative Decree 1/1996, 12 April, on Intellectual Property, establishes as an injunctive remedy the suspension of services provided by intermediaries ISPs when such services are being used by the wrongdoer to infringe third parties' intellectual property rights.

128 S.F. Kreimer, «Censorship by proxy: the first amendment, internet intermediaries, and the problem of the weakest link», 155 *University of Pennsylvania Law Review* 14, November 2006.

129 See Case C-131/12, of 13 May 2014, at para. 81.

130 S.F. Kreimer, *cit.*, at p. 29.

vior. But there is also danger to free speech from private misbehavior. An obsessive refusal to even consider the one threat against the other does not serve the values promoted by the First Amendment»[131].

Other controversial issue in the net neutrality debate is the privacy concerns that may arise with the use of DPI, as data about a users' behaviour on the Internet (which will often include sensitive data) may be monitored and used for various purposes[132]. In fact, the Berec openly recognised that «when blocking/throttling is implemented in the network, it is typically done through deep packet inspection (DPI)»[133].

The European Data Processor Supervisor (the «EDPS») has highlighted that a serious policy debate on net neutrality must address the confidentiality of communications as well as other privacy and data protection implications due to the increasing use of traffic management policies based on the inspection of network traffic in order to differentiate and apply different policies to it.

For the EDPS, DPI techniques based on the analysis of the metadata and the content of a communication itself are highly intrusive. In the same way as in the postal service, DPI is equivalent to opening the envelope and reading the letter inside.

«Inspection techniques based on IP headers and more particularly those based on packet inspection involve the monitoring and filtering of these data and have serious implications in terms of privacy and data protection. They can also be in conflict with the right to confidentiality of communications»[134].

In this regard, it must be beard in mind the decision of the ECHR of Justice in *SABAM v Netlog* (2012) where the Court found that an injunctive remedy seeking to prevent future infringement of intellectual property rights and consisting of an indiscriminate system for filtering most of the information stored on the servers of a hosting provider in order to identify electronic files with copyrighted works, and subsequently to block the exchange of such files, did infringe the Directive 95/46/EC, of 24 October 1995, on the protection of individuals with regard to the processing of personal data.

The Court noted that the said measure would oblige the hosting provider to «actively monitor almost all the data relating to all of its service users» in order to prevent any future infringement of intellectual property rights:

131 L. Lessig, *Code*…, *cit*. at p. 256.

132 ITU, *Net neutrality*, *cit*., at 16.

133 Berec, *A view of traffic management*…, *cit*., at p. 22.

134 EDPS, Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data, 7 October 2011, at para. 33. Retrieved from: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-10-07_Net_neutrality_EN.pdf (accessed: 10 May 2015).

«Moreover, the effects of that injunction would not be limited to the hosting service provider, as the contested filtering system may also infringe the fundamental rights of that hosting service provider's service users, namely their right to protection of their personal data and their freedom to receive or impart information, which are rights safeguarded by Articles 8 and 11 of the [European Charter on Fundamental Rights] respectively. Indeed, the injunction requiring installation of the contested filtering system would involve the identification, systematic analysis and processing of information connected with the profiles created on the social network by its users. The information connected with those profiles is protected personal data because, in principle, it allows those users to be identified»[135].

That is why, in assessing traffic management practices which may constitute a deviation from net neutrality, the Council of Europe has drafted some guidelines to be taken into account by broadband providers when applying such techniques.

These guidelines are in line with the ECHR well-stablished jurisprudence on matters of restrictions on human rights and its triple test of legality, proportionality and necessity. In this sense, such measures should be (i) proportionate, appropriate and avoid unjustified discrimination; (ii) subject to periodic review and not maintained longer than strictly necessary; (iii) subject to judicial control and legal remedies to seek redress[136].

More specifically, blocking access should only be done for law enforcement or other legitimate and strictly necessary reason, such as a violation of contractual obligations or intentional abuse, while having regard to legal safeguards that may be applicable under national law[137].

It also introduces the transparency rule, so that users and service providers should be adequately informed about any network management measures that affect in a significant way access to content, applications or services. The customer should, where appropriate, be properly warned and informed beforehand, be given adequate reasons for the cutting of access and be instructed of the steps to be taken to re-establish the access[138].

IX. **CONCLUSIONS**

Net neutrality is more than architectural principle which the open Internet as «we know it» relays oupon. That is to say the Internet built upon the open and end-to-end architecture which has enabled innovators and consumers at the edges of the network to create and determine the success or failure of content, applications, services and devices.

135 *Sabam v Netlog,* Case C-360/10, 16 February 2012, at paras. 48-49.

136 COUNCIL OF EUROPE, *Declaration of the Committee of Ministers on network neutrality, cit.,* Guideline 8.

137 COUNCIL OF EUROPE, *Human rights guidelines for Internet service providers, cit., Guideline 19.*

138 *Ibíd.*

Traffic management practices run by broadband operators to handle traffic congestion are not necessarily harmful for net neutrality. Nevertheless, there are some documented practices of blocking, throttling or paid prioritisation incurred by broadband operators which are unreasonable and discriminatory posing risks for market competition and end users.

A market-oriented approach dominates net neutrality debate on the existing legal frameworks in Europe and the United States. By contrast, especially in the context of international organisations, a human rights-oriented approach on net neutrality issues is clearly emerging and slowly gaining advocators in some domestic jurisdictions.

A human oriented-approach on net neutrality should take into account the public service value and the democratic dimension of the open Internet as an enabler of fundamental rights.

Facing the question on whether the access to Internet should be considered as a citizen right, the European Court of Human Rights has recognised a right to Internet access, which is considered to be inherent in the right to access information and communication protected by national Constitutions, and encompasses the right for each individual to participate in the information society and the obligation for States to guarantee access to the Internet for their citizens.

Nevertheless, the Strasburg Court has not delimitated the scope of the positive obligation and the possible horizontal effects of such rights in private relationships between broadband providers and end users, especially with regard to deviations of net neutrality which may pose harms to fundamental rights such as freedom of expression and privacy.

As Marsden opines, net neutrality is a «more politically important issue than telecommunications regulators are equipped or legally bound to explore» not only because technologies of censorship are at stake[139] but also because highly intrusive traffic management practices such as DPI are being put in place compromising privacy and confidentiality of communications (99).

Domestic legislations on net neutrality should take into account some criteria to ensure an open Internet. In this sense, traffic management practices should be proportionate, appropriate and avoid unjustified discrimination. They should be subject to a due process of law including legal redress for harmful deviations of net neutrality with impact on fundamental rights. In addition, to better prevent from unreasonable and discrimina-

139 C. Marsden, «Network Neutrality: History, Regulation and Future», IDP. *Revista de Internet, Derecho y Política*, VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet, Universidad Oberta de Catalunya, n.º 13, febrero 2012, at p. 99. Retrieved from: http://idp.uoc.edu/index.php/idp/article/viewFile/n13-numero-complet/n13 (accessed 5 May 2015).

tory practices, broadband providers should disclose to end users in a transparent manner their traffic management practices.

As Friedman J. observed for the District Court of Columbia in *Blumenthal v Drudge and AOL* (1998), one of the first cases related to defamation by means of Internet, «[…] the Internet ha[s] created ever-increasing opportunities for the exchange of information and ideas in «cyberspace». […] Needless to say, the legal rules that will govern this new medium are just beginning to take shape».

TÍTULO

EL DERECHO A UN «INTERNET ABIERTO, ROBUSTO Y DE ALTA VELOCIDAD»

SUMARIO

PALABRAS CLAVE

Internet abierto; Neutralidad en la red; Gestión del tráfico en la red; Internet a dos velocidades; Libertad de expresión; Privacidad; Derechos fundamentales.

RESUMEN

Este trabajo examina el debate existente sobre «Internet abierto» después de la aprobación reciente de normativa concreta en esta materia por la Comisión Federal de las Comunicaciones americana el pasado 12 de marzo de 2015. Para ello, se analizará cómo opera su principio subyacente de neutralidad de la red, cómo ha sido recogido por la legislación nacional e internacional —especialmente en Europa y en Estados Unidos— y cómo las prácticas de gestión del tráfico en Internet aplicadas por los proveedores de banda ancha pueden tener implicaciones en la experiencia de los usuarios finales en el acceso a la red. En este sentido, las desviaciones del principio de neutralidad tecnológica pueden tener graves impactos no sólo en la competencia del mercado o en la protección de los consumidores, sino también en los derechos fundamentales, especialmente la libertad de expresión o la privacidad. Por esta última razón, este trabajo plantea la cuestión de si el acceso a la infraestructura debería considerarse como un derecho del ciudadano en sí mismo, cuál debiera ser la naturaleza y ámbito de tal derecho y el valor de servicio público subyacente en el Internet abierto.

Fecha de recepción: 23/02/2015 Fecha de aceptación: 18/05/2015