



N° 3336

NATIONAL ASSEMBLY

OCTOBER 4, 1958 CONSTITUTION

THIRTEENTH LEGISLATURE

Recorded at the Presidency of the National Assembly on April 13, 2011

REPORT OF THE FACT FINDING MISSION

SUBMITTED

In application of article 145 of the Rules of Procedure

ON BEHALF OF THE COMMITTEE ON ECONOMIC AFFAIRS

Net and Network Neutrality

PRESENTED

BY CORINNE ERHEL,
Chairperson,

AND LAURE DE LA RAUDIERE,
Rapporteur,

Members of Parliament.

Members of the fact-finding mission on Net and Network Neutrality are: François Brottes, Jean-Pierre Decool, Jean Dionis du Séjour, Corinne Erhel, Jean-Louis Gagnaire, Laure de La Raudière, Pierre Lasbordes, Alain Suguenot, Lionel Tardy, and Jean Proriol.

SUMMARY

	Pages
Summary of the proposals	8
List of proposals	9
I. — THE GENERAL ISSUE.....	11
A. — THE DEBATE ON NET NEUTRALITY.....	11
1. The three aspects of the debate	11
<i>a) The technical aspects</i>	<i>11</i>
<i>b) The economic aspect.....</i>	<i>12</i>
<i>c) The legal aspect.....</i>	<i>12</i>
2. Reasons for the debate	12
3. Current policy debates	13
<i>a) Recent works</i>	<i>13</i>
<i>b) Ongoing works</i>	<i>14</i>
B. — TECHNICAL CONSIDERATIONS: HOW THE INTERNET FUNCTIONS.....	15
1. Introductory remarks	15
2. The Internet in thirty-one points	15
C. — ECONOMY: ALLOCATION OF NETWORK COSTS AND OF ADDED VALUE, AND THE ECONOMIC MODELS	18
1. Elements of analysis	19
<i>a) The lessons of economic theory.....</i>	<i>19</i>
<i>b) Economic models.....</i>	<i>20</i>
2. Issues	21
<i>a) Increase in traffic</i>	<i>21</i>
<i>b) The “monopoly” of Internet access</i>	<i>22</i>
3. The risks.....	22
D. — THE LAW: EXISTING INSTRUMENTS TO MANAGE RISK	22
1. Applicable law	22
2. Provisions stemming from the third Telecom Package.....	23

II. — PRACTICAL CONCERNS	25
A. — LEGAL BLOCKING AND FILTERING	25
1. The techniques.....	27
<i>a) Blocking and filtering techniques</i>	27
<i>b) Bypass methods</i>	28
<i>c) Key points</i>	29
2. The legal framework.....	30
<i>a) Ten years of legislative debate</i>	30
<i>b) Constitutional and European constraints</i>	32
<i>c) Key points</i>	33
3. Policy debate.....	33
<i>a) The players' positions and the arguments raised</i>	33
<i>b) The mission's analysis</i>	35
B. — TRAFFIC MANAGEMENT	36
1. Techniques.....	37
<i>a) Quality</i>	38
<i>b) Traffic management technologies</i>	39
<i>c) Key points</i>	40
2. The legal framework.....	41
<i>a) Regulation directly arising from the law</i>	41
<i>b) Regulation directly arising from sectorial and competition regulation</i>	42
<i>c) Stipulations stemming from the third Telecom Package</i>	44
3. Policy issues	45
<i>a) The players' positions and the solutions proposed by the regulators</i>	46
<i>b) The mission's analysis</i>	48
C. — INTERCONNECTION	48
1. Practices.....	49
<i>a) Technical functioning</i>	49
<i>b) Economic relations</i>	49
<i>c) Evolution</i>	51
2. The legal framework.....	51
<i>a) Applicable law</i>	51
<i>b) Possible interventions</i>	54
3. Policy issues	55
<i>a) The debate on data call termination</i>	55
<i>b) The players' positions and arguments raised</i>	56

<i>c) The mission’s analysis</i>	57
III. — THE MISSION’S PROPOSALS	59
Principle behind the proposals	59
Summary of the proposals	60
List of proposals	60
▶ FIRST STRATEGY: ENSHRINE NET NEUTRALITY AS A POLICY OBJECTIVE ..	62
Proposal n°1: Define the principle of neutrality	62
Arguments:.....	62
<i>Send a clear policy signal</i>	62
<i>Response to the shortcomings of applicable legislation, current and future</i>	63
<i>Begin with a good definition</i>	63
Proposal n°2: Establish neutrality as a policy objective and give regulatory authorities the power to impose obligations for promoting Net Neutrality	65
Arguments:.....	65
<i>Ensure that the regulatory authorities fully consider the Internet</i>	65
<i>Give an adequate normative scope to the principle of neutrality</i>	66
▶ SECOND STRATEGY: STRICTLY REGULATE INTERNET BLOCKING OBLIGATIONS	66
Proposal n°3: Further investigate the justifications for legal blocking measures, despite apparent legitimacy, due to their inefficiency and potentially negative consequences.....	67
Arguments:.....	67
<i>Remember that general law applies to the Internet</i>	67
<i>Weigh the technical aspects</i>	67
<i>Precisely identify the effects of blocking</i>	68
<i>Encourage the development of “parental control”- type filtering software</i>	69
Proposal n°4: Immediately establish a single procedure for judicial intervention	69
Arguments:.....	69
<i>Protecting freedom of expression and communication</i>	69
<i>A unified legal framework</i>	70
<i>Rationalize the legal procedure</i>	70
▶ THIRD STRATEGY: PROTECT UNIVERSALITY AND GUARANTEE INTERNET QUALITY	70
Proposal n°5: Reserve the “Internet” trade name solely for offers that respect the principle of neutrality	70
Arguments:.....	71
<i>Increase transparency with a simple equation: Internet = neutrality</i>	71

<i>Encourage Internet access providers to offer the best possible Internet access</i> .	71
Proposal n°6: Create an Internet quality watchdog.....	71
Arguments:.....	72
<i>Allow the consumer to choose between Internet access offers based on quality</i> .	72
<i>Develop existing measurement tools</i>	72
<i>Involve the ARCEP in monitoring operators' practices</i>	72
Proposal n°7: Request the ARCEP to guarantee access to an Internet of sufficient quality	72
Arguments:.....	73
<i>Intervene in cases of market shortcomings</i>	73
<i>The ARCEP's competence</i>	73
► FOURTH STRATEGY: ENSURE VIABLE FINANCING OF THE INTERNET	73
Proposal n°8: Document the economic issues related to the Internet network	73
Arguments:.....	74
<i>Rely on objective data</i>	74
<i>Develop a “panoramic” knowledge of the markets</i>	74
<i>Demonstrate the necessary caution to avoid disrupting economic models</i>	74
Proposal n°9: In-depth evaluation of data call termination at the European level.....	74
Arguments:.....	75
<i>Be at the right level</i>	75
<i>Consider the substantial arguments in favor of “data call termination”</i>	75
<i>Precisely evaluate the impact of implementing “data call termination” on the economic models of the various categories of players</i>	75
<i>Encourage the European Commission to conduct an in-depth analysis on the subject</i>	76

Article 11 of the Declaration of the Rights of Man and of the Citizen establishes “*the free communication of ideas and opinions.*” What media currently embodies these principles better than the Internet?

We must therefore strive to preserve the tremendous societal advances of the Internet:

- The democratization of access to knowledge; like the printing press in its time;
- Public participation in political debates;
- Ease of promoting new ideas;
- Rapid dissemination of new technologies;
- Universal marketing of products and services;
- Facilitated cooperation between players of all sizes within an industry;
- Economic development of small businesses, etc.

France must take full advantage of the opportunities for growth that can benefit all industries. In Europe, the digital domain already accounts for a quarter of growth and the net creation of jobs, as well as for 40% of productivity gains.

The importance of these issues merits that certain rules are defined to preserve the universal Internet, an immense collective asset that must not be molded according to the interests of its various players. It is a political, economic, and societal objective.

Discussions on Net Neutrality began in a heated environment, first emerging in the United States, in the early 2000s, in the context of perpetuating a monopoly of local cable providers. In Europe, because of greater regulation on the various sectors, discussions only began in 2008, during the examination of the third Telecom Package.

Right now, the increase in traffic and the pressures to implement blocking measures clearly threaten this neutrality.

The fact-finding mission of the National Assembly’s Committee on Economic Affairs interviewed more than a hundred industry players, published a pre-report, on January 27, 2011, collected their opinions, and conducted complementary interviews on issues that deserve more in-depth study.

Upon completion of this work, the Committee formulated nine pragmatic proposals that strike a balance between the absolute necessity for guaranteeing neutral, universal Internet access and the potential for network innovation—many, occasionally conflicting, interests that must be regulated prudently.

Summary of the proposals

The objective of the first proposal strategy is to protect the Internet by explicitly including it in the perimeter of electronic communications regulation. The current risk is the rise of non-neutral practices that would reduce Internet users' ability to choose how to use their network. To counter this risk, we recommend giving the principal of Net Neutrality legal scope by generally defining its promotion as an objective for regulatory authorities (the purpose of the first proposal strategy) and, more specifically, providing guarantees on the points that give the greatest cause for concern (the purpose of the proposal strategies that follow). Proposal n°1 defines Net Neutrality under the Law, and proposal n°2 defines its promotion as an objective for regulatory authorities.

The objective of the second proposal strategy is to avoid, as far as possible, requiring operators to block electronic communications, since blocking has both direct (restricting the freedom of expression and communication) and indirect (over blocking, encouraging encryption, etc.) negative effects, which are not always correctly taken into consideration in legislative decisions. Furthermore, fragmentation of the legislative framework (the 2004 LCEN [Law on Confidence in the Digital Economy], the 2010 Law on Online Gaming and Betting, the Code of Intellectual Property) is a source of confusion. This is why we recommend further inquiry into the justifications for legal blocking measures, despite their apparent legitimacy, because of their inefficiency and unintended negative consequences (proposal n°3), and immediately provide for systematic judicial intervention to rule on the required blocking measures to better protect freedom of expression (proposal n°4).

The objective of the third proposal strategy is to preserve the Internet as the open platform it is today. There is the risk of a rapid deterioration in the quality of the public Internet due to a substantial increase in flows should Internet access providers fail to invest in networks or if they privilege the marketing of managed services. Safeguarding consumer choice seems to be the first solution in meeting this risk: in the absence of market shortcomings, ensuring the transparency of Internet access by reserving the Internet trade name for neutral accesses only would seem sufficient for protecting this choice (proposal n°5), along with creating an Internet quality watchdog (proposal n°6); in the event that competition no longer permits consumers to choose a quality, neutral Internet access at a reasonable cost, maintaining the consumer's ability to choose must be restored through more restrictive means, by imposing requirements that guarantee Internet quality on Internet access providers (proposal n°7).

The objective of the fourth proposal strategy is to carefully achieve an economic balance between the different categories of Internet players, so that the Internet ecosystem can continue to develop and innovate, while also guaranteeing the coverage of network investments to maintain a quality Internet. The increase of asymmetrical Internet traffic, combined with caps on consumer prices, and the arbitrary nature of financial flows on two-sided markets, create the risk of a

significant uncertainty in the evolution of economic relations between the various categories of players and the viability of their economic models. Since Internet access providers are required to provide a sufficient level of quality, we must ensure that their economic model allows them to do so. According to the information collected by the mission, establishing “data call termination,” which would allow the network’s variable costs to be covered, could be a good solution. We must continue to study this point since the markets related to the Internet network are still not well understood (proposal n°8). and the appropriateness of implementing such a solution must be evaluated in depth (proposal n°9).

List of proposals

► **First strategy: enshrine Net Neutrality as a policy objective**

Proposal n°1: Define the principle of neutrality

Proposal n°2: Establish neutrality as a policy objective and grant regulatory authorities the power to impose obligations for promoting Net Neutrality

► **Second strategy: Strictly regulate Internet blocking obligations**

Proposal n°3: Further investigate the justifications for legal blocking measures, despite their apparent legitimacy, due to their inefficiency and potentially negative consequences

Proposal n° 4: Immediately establish a single procedure for judicial intervention

► **Third strategy: Protect universality and guarantee Internet quality**

Proposal n°5: Reserve the “Internet” trade name solely for offers that respect the principle of neutrality

Proposal n°6: Create an Internet quality watchdog

Proposal n°7: Request the ARCEP to guarantee access to an Internet of sufficient quality

► **Fourth strategy: Ensure viable financing of the Internet**

Proposal n°8: Document the economic issues related to the Internet network

Proposal n°9: In-depth evaluation of data call termination at the European level

I. — THE GENERAL ISSUE

This first section introduces the general principle of Net Neutrality and explains why its protection by legislative intervention must be considered. On a provisional basis, we can define Net Neutrality as the absence of discrimination in the conveyance of flows. Presenting the developing debates on (A) Net Neutrality; (B) its technical functioning, and (C) its network economy indicate that there is currently a risk of operators developing non-neutral practices (C). Existing law does not seem capable of responding to this threat (D).

A. — THE DEBATE ON NET NEUTRALITY

1. The three aspects of the debate

While at first confusing, debates on Net Neutrality seem clearer when presented as the superimposition of three actual debates that have developed successively: a technical debate, an economic debate, and a legal debate.

a) The technical aspects

The principle of Net Neutrality was originally a technical issue.

The Internet network was designed to function differently from standard telephone networks. Based on the principle of “packet routing” rather than on “circuit switching,” the Internet is both more flexible (when a circuit is unusable, packets can take other paths) and, theoretically, less reliable (the conveyance of packets vary in quality, since they are not routed in a reserved circuit)⁽¹⁾. As a result, the Internet network is historically viewed as a network whose intelligence is located at its endpoints, in the machines connected to it.

In the early 1980s, researchers in computer and network science supported the idea that implementing mechanisms in the lower layers of a distributed computer system was generally not justified. This viewpoint was termed the “end-to-end argument”⁽²⁾.

This argument was subsequently reinterpreted by jurists advocating Net Neutrality, who believed that the network was more efficient when it did not

(1) *These characteristics specifically find their origins in the way TCP and IP protocols developed by Vinton Cerf and Robert Kahn function: see V. G. Cerf and R. E. Kahn, “A protocol for packet network interconnection,” IEEE Trans. Comm. Tech., 1974.*

(2) *See J. H. Saltzer et al. “End-to-End Arguments in System Design,” 1984. This article “presents a design principle that helps guide the placement of functions among the modules of a distributed computer system. The principle, called the end-to-end argument, suggests that functions placed at low levels of a system may be redundant or of little value when compared with the cost of providing them at that low level.”*

contain intelligence at its heart⁽¹⁾. The concept of Net Neutrality was popularized on this basis by the American jurist Tim Wu in an article from 2003⁽²⁾, “*The idea is that a maximally useful public information network aspires to treat all content, sites, and platforms equally.*”

b) The economic aspect

To this technical aspect is added an economic aspect arising from the fusion of the studies on network design with the economic analysis of two-sided markets. Specifically, on which participants can be remunerated on the two categories of players they put into relation with each other, which recommends that one side “subsidize” the other⁽³⁾.

c) The legal aspect

Finally, debates arose from a third angle, that of legal blocking and filtering, which raised questions relating to freedom of expression on the Internet⁽⁴⁾. This last aspect of the debate is essentially European, and, in a sense, represents the consequences, in terms of neutrality, of the discussions on suspending Internet access, in the context of the 2009 HADOPI Law,⁽⁵⁾ and of the administrative measures for blocking Internet content that ensure freedom of communication, in the context of the 2011 LOPPSI Law.

2. Reasons for the debate

It is helpful to briefly outline the principal motivations for the discussions on Net Neutrality. The escalation of the debate in the 2000s is essentially due to two factors:

– The first factor is the increase in traffic as a result of an increase in video flows on the fixed market, and the development of terminals connected to the Internet on the mobile market. Internet access providers used the conveyance costs of the traffic generated as a factor in their negotiations with content providers and transit operators. There is a correlation with the costly deployment of new local

(1) See for example, Lawrence Lessig and Robert McChesney, “No Tolls on the Internet,” The Washington Post, 2006.

(2) See “Network Neutrality, Broadband Discrimination,” Journal of Telecommunications and High Technology Law, 2003.

(3) See Nicholas Economides et Joacim Tag, 2007, “Net Neutrality on the Internet: A Two-sided Market Analysis,” Working Papers 07-27, New York University, Leonard N. Stern School of Business, Department of Economics.

(4) This aspect of the debate is essentially European.

(5) We must emphasize that this discussion resulted in a postponement of the adoption of the third Telecom Package for several months and the French Constitutional Council’s censure of the legislation giving HADOPI the power to suspend Internet access without judicial intervention. See Laure de La Raudière’s opinion n° 2789 of the National Assembly on the transposition of the third Telecom Package (p. 12).

fiber networks that ensure the quality delivery of the traffic demanded by the new usages;

– The second factor is increasing government pressure to seek ways to enforce Internet laws and fight cyber crime, and from cultural industries whose classic economic models have been destabilized by the development of “illegal” digital exchanges, specifically “piracy.” These two categories of players advocate the development of blocking measures to prevent access to “illicit” content. The concern arose that operators could use “illegal” flows as a pretext for blocking, at their own initiative, categories of traffic in part illicit, but also licit, such as peer-to-peer flows.

Finally, we must note that there was another factor that acted as a catalyst in France: the uniformity of fixed triple-play offers, provided at the lowest cost in Europe, that give unlimited Internet access independent from the traffic consumed, even though additional traffic generates costs.

3. Current policy debates

a) Recent works

Debates progressed simultaneously in the United States, Europe, and France due to the intervention of public authorities—essentially regulators.

As early as 2005, the American Federal Communications Commission (FCC) unanimously issued a policy statement on the Internet that recognized four fundamental rights of Internet users, who are entitled to: (i) access to 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; (iv) competition among network providers, application and service providers, and content providers. The continuing discussions led to a partisan decision in December 2010⁽¹⁾ in which the FCC imposed two even more restrictive rules upon Internet access providers: (i) no blocking; (ii) no unreasonable discrimination in the transmission of traffic.

The European legislator addressed the issue in the course of discussions on the third Telecom Package, which included several measures for protecting neutrality⁽²⁾, to which the European Commission agreed to give their full attention⁽³⁾.

(1) *Majority Democrats vs. minority Republicans.*

(2) *See Laure de La Raudière’s opinion n° 2789 of the National Assembly on the transposition of the third Telecom Package (p. 19-21).*

(3) *See the Commission’s declaration in the annex of directive 2009/140/EC: “The Commission attaches high importance to preserving the openness and neutrality of the Internet, taking full account of the will of co-legislators now to enshrine net neutrality as a policy objective and regulatory principle to be promoted by the national regulatory authorities, alongside strengthening the related transparency requirements and the creation of safeguarding powers for national regulatory authorities to prevent the degradation of services and the hindrance or deceleration of traffic over public networks. The Commission will closely monitor*

In the framework of the 2009 Law on the Digital Divide, the French legislator requested that the Government provide a report on this issue. To respond to this request, the Government brought the matter before the General Council for Industry, Energy, and Technologies (CGIET), which provided a “technical” report⁽¹⁾, subsequently drafting its own report, which remained prudent on the measures to be adopted⁽²⁾. The ARCEP simultaneously conducted in-depth investigations that resulted in a detailed set of non-binding recommendations⁽³⁾.

On February 17, 2011, the National Assembly finally examined members’ bill n° 3061 on Net Neutrality, initiated by Christian Paul and tabled by the Socialist group. The National Assembly rejected this members’ bill on March 1, 2011.

b) Ongoing works

Several works are currently in progress.

– In France, the ARCEP launched three series of works following its initial guidelines: (i) on the wholesale interconnection market: it is preparing a decision on the periodical collection of data, which could be rendered before summer 2011; (ii) on quality of service over the Internet: it continues its in-depth investigations, specifically on methods for measurement; (iii) it requested that the French Telecom Federation, in coordination with other players, create a work group on traffic management.

– At the European level, the European Commission will: (i) publish a communication on Net Neutrality, initially scheduled for the end of 2010 but postponed to May 2011; (ii) organize work groups at the level of senior company managers on several neutrality related issues, which should submit its first conclusions in July 2011.

– Finally, in the United States, industries initiated discussions to define the “best practice” for Internet traffic management.

implementation of these provisions in the Member States, introducing a particular focus on how the "net freedoms" of European citizens are being safeguarded in its annual Progress Report to the European Parliament and the Council. In the meantime, the Commission will monitor the impact of market and technological developments on "net freedoms," reporting to the European Parliament and Council before the end of 2010 on whether additional guidance is required, and will invoke its existing competition law powers to deal with any anti-competitive practices that may emerge."

(1) See François Cholley et al., “La neutralité dans le réseau internet,” CGIET, 2010.

(2) See “La neutralité de l’Internet : Un atout pour le développement de l’économie numérique,” Government report to Parliament, 2010.

(3) See Arcep, “Neutralité de l’internet et des réseaux : Propositions et recommandations,” September 2010.

B. — TECHNICAL CONSIDERATIONS: HOW THE INTERNET FUNCTIONS

1. Introductory remarks

To understand the debates on Net Neutrality, a minimal command of the technical background on which they are based is necessary:

– For Internet users, the Internet functions like a “platform” that directly connects them with each other and allows the display of web pages, etc. In a broad outline, the principle of neutrality seeks to protect this open platform. In fact, the Internet network is complex and undergoes frequent adjustments implemented by a multitude of players. To understand the effects of the various practices and whether some should be prohibited, it is necessary to address the technical aspects;

– On the basis of the aforementioned end-to-end argument, the neutrality principle can be seen as a “technical” principle that would prohibit any interference on the part of Internet access providers on the transmission of flows and require them to establish networks that only convey data to the recipient based on the same principles, regardless of the data conveyed.

2. The Internet in thirty-one points

The complexity of the Internet requires simplification. The following presentation therefore does not attempt to be exhaustive but only educational.

1 Let us suppose a person wishes to transmit data via the Internet. This information is “digital,” which means that it is a logical sequence of 0s and 1s recorded in one way or another on a physical medium.

2 Contrary to standard telephone networks, or “circuit switching” networks, the Internet is a network that functions on the basis of “package routing.” The line used by a person who wants to transmit data and his recipient is not reserved, since a great number of communications will in fact use the same line.

3 For this mode of transmission to be efficient, data will be split up into sequences of 0s and 1s smaller than the data transmitted, called “IP packets.” IP is short for Internet protocol.

4 Since there is no “line” established between the Internet user and his/her correspondent, the correspondent's address must be recorded in the packet. This address is a sequence of 0s and 1s placed on the packet's “header.” We must note that the header also includes data other than the recipient's address—such as a port number—and that routers usually read only the header, except when equipped with deep packet inspection (DPI) systems.

5 The address written on the packet's header must be an address that corresponds to a location on the Internet network. This is why a common address system was globally implemented (IPv4 followed by IPv6).

6 The packet with a unique address in its header will then be sent on the Internet network. When it reaches an intersection, it is in contact with an active equipment called a "router." As its name indicates, the "router" handles routing; that is to say, it assigns the correct route to the packet.

7 The router defines the right route for each packet based on the destination address contained in the router's header and a network map called a "routing table," which determines the best path from one point to another.

8 Let us now suppose that the Internet user knows the IP address of the recipient who just connected to the network. The path leading to the recipient's IP address can be found in the manner described below, which functions schematically like a border gateway protocol (BGP).

9 The router closest to the recipient first recognizes that the recipient is directly connected to it. It then automatically sends a message to the surrounding routers to inform them that it is directly in contact with the recipient's address. They in turn will inform routers around them that they are located just one router away from the recipient's address, and so forth.

10 Routers will then usually orient the packet to the "shortest" path between them and the destination address.

11 Once the packets are delivered to the recipient, they are assembled following the removal of their header, and the recipient then is in possession of the transmitted data.

12 Let us now suppose that an Internet user wants to connect to a website. This website is hosted on a "server" connected to the Internet.

13 In most cases, the Internet user has no knowledge of the IP address of the server hosting the website, but only the website's name. A system is therefore needed to establish correspondence between a website's name and the server's IP address. A domain name system (DNS) was therefore globally implemented.

14 When an Internet user wishes to access a specific domain name, he/she sends a packet with a special number in the header, which the routers will send to a DNS server capable of sending back the IP address that corresponds to the domain name.

15 The Internet is therefore established on a series of links that allow navigation from resource to resource via "url" addresses.

16 The preceding explanations describe the Internet’s logical functioning only rudimentarily and do not describe the physical infrastructures on which the Internet is based.

17 The general public initially accessed the Internet from their telephone networks and the copper “local network.” The “core network,” as opposed to the terminal level called the “local network,” and occasionally an intermediate level called the “collection network,” were rapidly equipped with optical fiber, allowing much greater speeds than copper. The local network, the collection network and the core network constitute the “access network.”

18 The creation of a network that interconnected the various networks used to provide Internet access became necessary. This network was called the “network backbone,” or simply the Internet (the cloud), different from access networks.

19 For purposes of concision, the following presentation on the principal Internet infrastructures is limited to wired access. For network access, the local network is still essentially copper wire pairs, aerial or buried in sleeves (ADSL), even though optical fiber lines are starting to be deployed (FTTH). On the wired networks, this portion of the network (local network) is generally dedicated to a single home or business. These dedicated wires range from the Internet user’s access (usually a “box”) to equipment called DSLAM, which can be a cabinet or room containing the equipment necessary for inserting packets to optimize the space available on networks.

20 Buried optical fibers usually interconnect the DSLAMs in the heart of the networks, where high-speed broadband routers will rapidly process substantial quantities of data.

21 The access network is then connected via interconnection points (peering, for example) to other networks, including the backbone network, generally to physical spaces called data centers.

22 The backbone network is essentially made up of these interconnections—long-distance optical fiber cables, specifically submarine, as well as routers and repeaters—to prevent attenuation of the optical signal.

23 The development of the Internet network and the flexibility of the IP technology on which it is based create a convergence of communications networks toward shared “all-IP” networks. In practical terms, the same infrastructure, the same network architecture, and the same protocols are increasingly used to transmit the different types of electronic communications.

24 This is why the telephone (which formerly depended on switched telephone networks) or company networks (which depended on physical “leased lines”) have become “managed services,” provided on IP networks.

25 The network’s complexity is further increased by the intervention of a multiplicity of players, whose cooperation is based on a set of non-binding standards that are essentially standardized and discussed. The number of entities recognized as Internet operators, and therefore allocated blocks of IP addresses called autonomous system (AS), gives some indication of the number of players operating on the Internet network—at least 27,000⁽¹⁾. We must emphasize that the following description of the various players is intentionally simplified. There are too many players intervening on several market segments to detail everything without departing from the educational purpose of this presentation on the Internet network.

26 While Internet operators are required to observe a minimum of the common rules at the level of interconnection, they can opt for very different technical solutions at the level of their networks.

27 Among Internet operators, we must also distinguish between Internet access providers that service final clients and therefore operate at the level of access networks, and transit operators that interconnect Internet access providers and therefore operate at the level of the backbone network.

28 Finally, other players intervene to provide services related to the Internet network. “Hosts” handle data storage on servers usually located in data centers (secured physically, electrically, and at the level of air conditioning) to avoid any disturbance in the servers’ functioning.

29 Certain points of interconnection between Internet operators are managed by independent entities. In this case, the equipment is also hosted in data centers.

30 Cache providers (CDNs or content delivery networks) offer temporary storage services for the most popular content, which brings users closer and therefore allows faster delivery.

31 Finally, “content providers” intervene at the end of the process and use the Internet to provide services, content, and applications.

C. — ECONOMY: ALLOCATION OF NETWORK COSTS AND OF ADDED VALUE, AND THE ECONOMIC MODELS

It is important to understand in detail the economy related to the Internet network: (i) beyond the aforementioned technical rules, the Internet functions via the intervention of a multiplicity of players with occasionally diverging economic interests; (ii) threats to Net Neutrality essentially result from these divergent interests; (iii) the issue is poorly documented.

(1) See OECD, *Communications Outlook 2009* (p. 180).

The fact-finding mission created by the National Assembly's Committee for Economic Affairs specifically focused on elucidating these economic issues. Observing that the markets related to the Internet network remain opaque, the mission asked in its initial guidelines that players communicate additional information via a detailed questionnaire. These initiatives have not resulted in definitive conclusions, thus motivating the mission's proposal that the ARCEP, the Government, and the European Commission conduct in-depth investigations on how the markets for Internet traffic delivery function.

1. Elements of analysis

a) The lessons of economic theory

The theory of two-sided markets provides a useful framework for the analysis of issues related to Net Neutrality⁽¹⁾.

This theory was developed on the example of credit cards. Credit card companies operate on a market that connects two categories of participant, sellers and their clients, and are remunerated by these two categories. The theory of two-sided markets specifically seeks to determine the economic effects of the possible modes of remuneration. The concept of two-sided markets is usefully applied to the Internet network, which is made up of several intermediation markets: Internet access providers can be remunerated by both Internet users and transit or content providers; transit providers can be remunerated by both Internet access providers and content providers; and so on.

Two-sided markets are characterized by cross-network effects: the more numerous the players on one side, the greater the economic value of the players on the other side. Applied to the Internet, the number of Internet users increases the economic performance of content providers, and an increase in Internet content increases the advantages of having Internet access.

To maximize the comprehensive advantage, the theory of two-sided markets would recommend a rate structure in which the side with the lowest rate elasticity and cross-network effect would "subsidize" the other. Applied to the Internet, we must determine whether the gains expected from higher subscription rates paid by Internet users for the production of content, thanks to a decrease in bandwidth costs paid by content providers, outweigh the losses related to a decrease in the number of Internet users as a result of higher subscription fees. This would have a negative impact on the profits expected by content providers and reduce the consumer's surplus⁽²⁾.

(1) See specifically Jean-Charles Rochet and Jean Tirole "Platform Competition in Two-Sided Markets" Journal of the European Economic Association, 2003.

(2) See Nicolas Curien and Winston Maxwell, "Le modèle du marché biface," in *La neutralité d'internet*, 2011.

The conclusions of these theoretical studies favor consumer subsidization of content providers' bandwidth⁽¹⁾. The fact-finding mission is unaware of applied economic studies that confirm or invalidate these recommendations on an empirical basis.

b) Economic models

The Internet represents a growing portion of the economy⁽²⁾, yet activities related to the network form only a part of it⁽³⁾. The fact-finding mission did not find precise information on the value of the various market segments for Internet traffic transmission, but it seems that global annual revenues related to transit and cache services represent a few billion euros, while the global market for access represents several hundred billions euros.

Historically, Internet access providers were remunerated by final users and paid transit providers, allowing content providers, or their aggregators (CDN, hosts), access to their network via settlement-free peering agreements. Transit providers were remunerated both by Internet access providers and content providers or their aggregators. Content providers or their aggregators therefore paid transit providers for transit but did not pay Internet access providers for peering.

Currently, these financial flows tend to evolve under the pressure of Internet access providers, who terminated a portion of their settlement-free peering agreements, specifically those with CDNs, and asked to be remunerated in order to give traffic generators access to their networks to cope with the increase in traffic volume and the degree of asymmetry.

Exact financial flows are difficult to establish, yet the markets' size and the direction of the flows indicate that content providers pay in the area of a few billion euros to transit providers and CDNs; Internet access providers pay sums in the same order of magnitude to transit providers; and subscribers, individuals, and businesses pay far greater amounts to Internet access providers.

(1) See Nicholas Economides and Joacim Tag, 2007, "Net Neutrality on the Internet: A Two-sided Market Analysis" Working Papers 07-27, New York University, Leonard N. Stern School of Business, Department of Economics; Robin Lee and Tim Wu, "Subsidizing Creativity through Network Design: Zero-Pricing and Net Neutrality," *Journal of Economic Perspectives*, 2009; Jacques Crémer, "La neutralité des réseaux," *Les Echos*, November 3, 2010.

(2) See McKinsey's study "Impact de l'internet sur l'économie française", 2011, according to which the Internet "industry" represents 3.7% of the French GDP, 72 billion euros of revenue, 1.15 million jobs, and a quarter of the economic growth and the net creation of jobs in the last fifteen years. We must note that Google financed this study.

(3) See AT Kearney's study "Internet Value Chain Economics," 2010, according to which the Internet globally represents 1.930 trillion dollars including 325 billion for activities related to connectivity. We must note that this study was financed by Internet access service providers (see appendix, pp. 45 and fol.).

Transit is charged on the basis of maximum incoming or outgoing speed. Access for individuals, at least in France, is all-inclusive⁽¹⁾. For mobile access, telephony continues to represent a substantial portion of operators' revenues in most countries and bears no relation to the costs generated, which implies that it "subsidizes" Internet access. These two factors illustrate why discussions on neutrality are particularly heated in France, where the issue of transitioning to a new commercial model for mobile access is coupled with a revenue cap on the fixed network, due to truly unlimited packages, for which Internet access providers attempt to complement their revenues.

2. Issues

a) Increase in traffic

Since the beginning of the 2000s, Internet traffic has grown extremely fast as a result of the development in the last few years of peer-to-peer and video. Increasing centralization of flows related to the development of Web 2.0 hosting platforms resulted in an increasing asymmetry in traffic; that is to say, the ratio between incoming volumes on Internet access providers' networks and outgoing volumes. We must emphasize the terminals' specific role in the increase of flows in the most recent period: smartphones and tablets caused an explosion in mobile traffic; connected televisions could have a similar impact on the fixed network in the near future.

If there is currently broad consensus on the forecasted increase in traffic⁽²⁾, there is still debate regarding the need to modify financial flows between the different categories of players to cover the costs that this traffic is likely to generate. The cautious position of the authorities on this issue⁽³⁾, and the absence of independent evaluations of these costs⁽⁴⁾, clearly point to the need to pursue this analysis. As the CGIET emphasized in its report, Internet access providers have three theoretical solutions at their disposal in order to cope with the increase in traffic: (i) degrade the quality of the Internet, (ii) make the consumer pay, and (iii) make content providers pay⁽⁵⁾.

(1) In many countries (Canada, England, etc.), "fair use" clauses were enacted and speed was reduced or the exceeding volumes invoiced beyond a certain use.

(2) See "Cisco Visual Networking Index, Forecast and Methodology: 2009-2014", 2010; and "Cisco Visual Networking Index, Global Mobile Traffic Forecast", 2011.

(3) In its first guidelines, the ARCEP therefore cautiously believes that "the strong increase in uses, in terms of data consumption, specifically video [...], poses an issue for financing the necessary capacity increase on different levels," but that "simultaneously to the increase in flows, a substantial decrease in storage, routing, and transmission costs was observed." Transit operators therefore state that the projected increase in transmission capabilities is exponential.

(4) See AT Kearney's study "A Viable Future Model for the Internet" provides an estimate of 9 billion euros for the fixed network and 19 billion for the mobile network, representing the additional financing Internet access providers will need to manage the increase in traffic.

(5) In the event the third option is chosen, recent economic studies indicate that it would be preferable for Internet access providers to monetize their networks vis-à-vis content providers by developing premium

b) The “monopoly” of Internet access

Because of their strategic position on the value chain, the debate on neutrality has focused on Internet access providers, since their network is the exclusive passageway to access their subscribers. This is why the threat of compromised neutrality weighs specifically on this network segment. Other market segments seem more competitive.

3. The risks

Facts assembled by the ARCEP, the FCC, and the BEREC, as well as information and data communicated by players contacted by the fact-finding mission, establish the existence of blocking practices and a degradation in the quality of certain types of flows. We must note, however, that to this day no dispute resolution procedure has been initiated.

We can provide three examples of non-neutral practices:

- Blocking Internet applications, such as the VoIP, that compete against those marketed by Internet access providers, either in the form of managed services or not;
- The degradation of certain flows, such as peer-to-peer, to off-load the network during peak hours;
- The targeted refusal to upgrade interconnections to compel content providers to abandon their transit providers and directly contract paid peering agreements with Internet access providers.

D. — THE LAW: EXISTING INSTRUMENTS TO MANAGE RISK

The capacity of the current legal framework to respond to neutrality issues will be analyzed in detail in the following section. It is useful, however, to present a broad outline of this framework to determine its capacity for responding to the aforementioned risks.

1. Applicable law

The relevant provisions currently included in the Postal and Electronic Communications Code (CPCE) are as follows:

- Operators are required to comply with the principle of neutrality with regard to the content they convey (articles L. 33-1 and D. 98-5) and respect the confidentiality of correspondences (art. L. 32-3); if these rules prohibit them from

transmission services rather than making all content providers pay for access to the network. See Robin Lee and Tim Wu, "Subsidizing Creativity through Network Design: Zero-Pricing and Net Neutrality," Journal of Economic Perspectives, 2009.

modifying the content of the data transported, they may modify the characteristics of the transmission;

– The objectives determined for regulatory authorities in article L. 32-1, allow for the promotion of certain aspects of neutrality, but not all of them (specifically ensuring “*nondiscrimination, under similar circumstances, in the relations between operators and online public communications service providers for the transmission of traffic and access to these services,*” as well as “*the electronic communications operators’ respect of the confidentiality of correspondences and the principle of neutrality with regard to the content of the messages transmitted.*”);

– Symmetrical regulatory powers relevant to interconnection and access (art. L. 34-8 and fol.), as well as asymmetrical regulation (art. L. 37-1 and fol.) have only a limited scope, due to the difficulty in establishing the need to regulate the interconnection market, which the Commission already rejected in a specific case;

– On the other hand, the ARCEP’s dispute resolution powers (art. L. 36-8) could be useful. However, it is difficult for small players to use it, since they must prove unfair treatment. To be efficient, the regulator must also have a better understanding of the Internet network.

Contrary to common opinion, general competition laws do not provide all the necessary guarantees. It is inapplicable in cases of peer-to-peer degradation, which raises issues that do not pertain to competition. In other cases, abuse of a dominant position means first proving the existence of a dominant position on a market, which is not always easy, and the prohibition of cartels does allow for exceptions in order to promote innovation. Details on this point are provided in the section on traffic management.

2. Provisions stemming from the third Telecom Package

In brief, the third Telecom Package contains three sets of measures that pertain to neutrality⁽¹⁾:

– Enshrine the principle of neutrality as a regulatory objective, both in its economic aspect (promotion of true competition between Internet access providers and content providers for the benefit of the consumer, “*including for the transmission of content*”); and in its societal aspect (objective of “*favoring access of final users to information and preserving their capacity to disseminate as well as use the applications of their choice*”);

– Impose transparency obligations for traffic management and network access restrictions on operators to ensure the protection of the principle of

(1) See opinion n° 2789 of Laure de La Raudière on the transposition of the third Telecom Package, National Assembly, 2010.

neutrality via competition (new compulsory information included in electronic communications service agreements must appear clearly and in detail and be easily accessible: traffic management procedures, access restrictions to certain services or equipment, measures to ensure the network's security and integrity, etc.);

– Grant new powers to the regulator to prevent violations of the principle of neutrality (power to define minimum requirements in terms of quality of service; dispute resolution powers extended to disputes over the transmission of traffic between operators and other companies, including content providers).

With regard to the examples cited, these provisions seem useful, specifically since they could allow: (i) a VoIP operator or a content provider who claims to have suffered from degraded interconnection to request that the ARCEP initiate a dispute resolution procedure; (ii) the ARCEP to impose minimum-quality-of-service requirements to prevent excessive degradation in the quality of protocol delivery. However, these indications should be examined in detail. Following this assessment, the next section concludes with the necessity of reinforcing existing law to provide further guarantees.

II. — PRACTICAL CONCERNS

The first section of the report presented the Internet network and emphasized that the development of certain practices threatened the Internet’s future. This explains why the issue of the appropriateness of government intervention to protect neutrality was raised. To respond to this question, the practical concerns pertaining to the violation of Net Neutrality must be analyzed. There are three concerns, which, in broad outline, correspond to the different technical, economic, and legal aspects of the debate: (A) legal blocking and filtering, which encompasses most of the legal issues; (B) traffic management, which pertains to the technical aspect of the discussion; (C) interconnection, which is at the center of the economic issues.

A. — LEGAL BLOCKING AND FILTERING

► We must first clarify the vocabulary. Since the terms are not used uniformly, the distinctions are somewhat arbitrary, even though they allow for the differentiation of several situations. Among the techniques used to restrict data exchange over the Internet, we recommend distinguishing, by convention and for the purpose of the present report, between:

– “Blocking,” which prevents a communication without inspecting content, and “filtering,” which implies the inspection of content⁽¹⁾;

– Blocking and filtering implemented at the heart of the network, and parental “control” or other systems that filter access to certain content from the network’s end-points, generally via software installed on a computer;

– “Legal” blocking and filtering, and blocking and filtering implemented by operators at their own initiative.

► This section deals with the issue of legal blocking and filtering only. Since blocking and filtering implemented on the operators’ initiative are understood as either a technical measure for traffic management or a commercial measure, they are dealt with in the following section.

The case of parental control is omitted since these systems are controlled by Internet users who can select the parameters and deactivate them, and therefore does not seem to raise a concern regarding neutrality.

Issues related to legal blocking and filtering are specific: (i) because they are binding for both operators and Internet users, which raises questions regarding

(1) That is to say, in the context of IP networks, if we read only the data contained in the packet’s header without implementing deep packet inspection (DPI). See the presentation in the report’s first section of the technical functioning of the Internet network.

civil liberties; (ii) because they are directly implemented in the operator's network, which raises many technical questions. Currently, French operators can be subject to blocking obligations, but not to filtering obligations.

We must also note that measures pertaining to filtering and blocking techniques necessary for ensuring the network's security, and which are largely consensual, are excluded from the following analysis.

► A few clarifications as to why the issue of Net Neutrality is related to the issue of legal blocking and filtering.

The FCC took the position, as of 2005, to exclude “illegal” content from the field of regulation with regard to neutrality⁽¹⁾. The European Commission did not address this issue in its public consultation⁽²⁾. In its first guidelines, the ARCEP briefly addressed the issue by stating that it was up to the Constitutional Council and the legislator to determine whether blocking and filtering obligations infringe upon civil liberties⁽³⁾. The restraint shown by these players on what blocking and filtering measures should or should not be required by law can be explained by their lack of legitimacy to intervene on this issue, which, as a legislative issue, falls within the competence of the Member States. Regulators such as the FCC and the ARCEP exercise regulatory powers only, and the European Commission intervenes only in the areas of competence of the European Union.

However, the very definition of neutrality, in terms of the Internet user's liberty to access all content, services, and applications, indicates that the issue of legal blocking and filtering is closely related to that of neutrality. Since the outset of the legislative debates on mandatory blocking measures, Internet access providers have pointed out that were these kinds of measures to be imposed on them, they would be compelled to intervene on the content they deliver—in violation of neutrality—when their role as an operator is really only to transport content.

In its report on neutrality, the Government also emphasized that the debate on Internet blocking is but one aspect of the debate on neutrality⁽⁴⁾.

(1) In section 107 of its 2010 decision, the FCC emphasizes that none of the rules enacted to protect neutrality has the purpose of restricting the obligations access providers are subject to or deprive them of an authorization they are granted by virtue of the law, nor would they limit their efforts to prevent illegal activities, specifically access to unlawful content.

(2) Except indirectly, via question n° 15, which pertains to other issues related to neutrality, specifically those regarding freedom of expression, media pluralism, and cultural diversity.

(3) See the ARCEP's first guidelines of 2010 p. 52.

(4) However, the report briefly addresses the issue by establishing that a differentiated processing of flows is necessary in order to comply with the legal blocking obligations and by reiterating the existing legal basis with regard to blocking.

1. The techniques

There is a near consensus in the analysis of blocking and filtering techniques and their efficiency. The following considerations summarize the main conclusions to be drawn from the interviews conducted and from the analyses in the documents written by players both for and against implementation of legal measures for blocking or filtering⁽¹⁾.

a) Blocking and filtering techniques

Among the technical solutions available, we can distinguish four principal blocking and filtering methods, depending on what is being blocked.

► Blocking an IP address.

The principle is either to block packets with an address in their header that is listed as an IP address to be blocked directly at the router level, (“blocking IP address”), or distribute “wrong paths” via the BGP protocol from certain routers, which attract packets destined to addresses that are included on a list of blocked IP addresses (“BGP blocking”).

Blocking IP addresses has at least two disadvantages: (i) blocking does not distinguish between websites sharing the same IP address, for example, because these websites are hosted on the same server, which occurs frequently. This can be avoided by using “hybrid” filtering (see “url blocking” hereafter); (ii) while the advantage of the BGP method is quicker updating, it may jeopardize the network when “wrong paths” are distributed beyond the ISP network (as was the case when Pakistan blocked YouTube in 2008, which resulted in the inability to access YouTube worldwide for several minutes).

► Blocking a domain name.

The principle here is to falsify the responses to DNS queries by not providing the IP addresses that correspond to blocked domain names. This method allows the exchange of data between an Internet user and a website to be blocked upstream (“DNS blocking”) and requires Internet access providers to implement filters at the level of their DNS servers.

Disadvantages of this technique are: (i) does not distinguish between different pages of a website; (ii) is easily bypassed by Internet users who can

(1) See *Mission entrusted to Denis Olivennes*, The development and protection of cultural works, 2007 (pp. 27 and fol.); Steven J. Murdoch and Ross Anderson, “Tools and Technology of Internet Filtering,” in Ronald J. Debeirt et al. *Access Denied: The Practice and Policy of Global Internet Filtering*, 2008; “Les enfants du net III,” *Forum des droits de l’internet*, 2008; “Principe, intérêts, limites et risques du filtrage hybride à des fins de blocage de ressources pédopornographiques hébergées sur des serveurs étrangers,” Christophe Espern, 2008; *étude d’impact de la LOPPSI* (pp. 7-17), 2009 ; “Etude d’impact du blocage des sites pédopornographiques,” *Fédération française des télécoms*, 2009 ; Cormac Callanan et al. *Internet blocking balancing cybercrime responses in democratic societies*, 2009.

address their DNS queries to DNS servers other than those of their Internet access provider.

► Filtering by content inspection.

Routers usually read only the headers of IP packets and do not inspect content. Filtering content requires installing content inspection servers so that the entirety of the traffic passes through these servers. The servers then allow the content of the packets to be analyzed and blocked according to a wide range of criteria. This technique was specifically mentioned in the Appendix of the Olivennes mission report as a possible solution for filtering unlawful exchanges of protected works, in association with digital fingerprint databases following tests to confirm the system's technical feasibility.

There are multiple problems related to this technique: (i) it requires analysis of the entire content of Internet exchanges, with all the risks of abuse that would entail; (ii) it requires concentrating traffic on a limited number of points, with the risk of a decrease in service quality for all users; or installing content inspection servers on many points of the network with a potentially prohibitive cost; (iii) the tests conducted were limited and there is still considerable uncertainty about the possibility of generalizing this system.

► Blocking urls.

This method, which combines BGP blocking and filtering via the inspection of content, would block requests by urls listed as blocked (“hybrid blocking”). The issues are the same as those for BGP blocking and filtering via inspection of content.

b) Bypass methods

There are bypass methods specific to each filtering technique and general bypass methods:

– The use of “mirror” websites, meaning a duplicate website on another IP address with another url and another domain name, which in theory allows the website to circumvent the available blocking and filtering techniques—except for filtering by inspection of content—but requires that the Internet user know the IP address of the mirror website, and also requires that the website is not frequently updated;

– The use of a proxy, meaning a website that serves as an intermediary between the user and the site the user wishes to connect to, also permitting the circumvention of most blocking techniques;

– Fast-flux techniques rapidly change an IP address to bypass IP address-blocking techniques. However, they are not efficient against methods based on DNS blocking;

– Internet users can very easily bypass DNS blocking if connected to a DNS other than that of the Internet access provider;

– Finally, encryption or the use of a virtual private network (VPN) masks the content of IP packets to bypass filtering.

c) Key points

First point: we have shown that technically blocking measures can be implemented. This is already the case in other countries, including democratic countries⁽¹⁾, yet not so much in France⁽²⁾. With the exception of generalized filtering, these measures do not appear to significantly reduce Internet quality. We must note, however, that following the example of Germany, several countries have recently abandoned blocking because of its cost and inefficiency.

Second point: blocking and filtering are not easy to execute technically, as they require sophisticated implementations on the network. BGP and DNS blocking seem to be much easier to implement than hybrid blocking, particularly filtering by inspection of content. The complexity of implementation also depends on the network, which explains: (i) the difficulty in implementing hybrid blocking in France, due to the decentralization of Internet networks; (ii) in the event blocking measures were imposed, operators want to be able to choose which technical solution to implement.

Third point: these various techniques cause both over-blocking—blocking flows that should not be blocked, also called “false positives”; and under-blocking—not blocking flows that should have been blocked, also called “false negatives.” The existence of techniques capable of bypassing each blocking technique fairly easily should be noted. Given the ability of Internet users to adopt new Internet practices, there is some concern that, faced with blocking, bypassing techniques will quickly be adopted. Some of these, including encryption, pose safety risks far greater than the inefficient defense of protected interests via blocking or filtering.

Fourth point: there are few evaluations of the costs for implementing the various filtering techniques. The only available estimates are those provided by the LOPPSI impact studies conducted by the Government⁽³⁾ and the FFT⁽⁴⁾.

(1) According to the FFT's aforementioned 2009 study, several Anglo Saxon countries and Sweden implemented “hybrid” blocking, while Germany, Italy, and Denmark opted for DNS filtering. The longest list of blocked elements is that established by Canada, which blocks around 10,000.

(2) The only documented case being that of the negationist “Aaargh” website.

(3) See pp. 16-17: “At the meeting held on February 5, 2009 under the aegis of the Ministry of the Interior, attended by Norwegian police officers, computer specialists, and Internet access providers, the cost for implementing DNS blocking was estimated at 4,000 euros per 100,000 subscribers. By comparison, this system cost the Australian authorities 62 million euros, when in Norway ISPs intervened at no cost.

(4) The FFT estimates that BGP blocking would cost from 100,000 euros to 3 million euros, depending on the technical solution adopted, DNS blocking 5 million euros, hybrid blocking 15 million euros, and generalized filtering 140 million euros.

2. The legal framework

Analysis of the applicable legal framework provides an opportunity to review the principal advances that occurred over the last ten years and to identify the margin of latitude at the legislator's disposal.

a) Ten years of legislative debate

► A legislative debate on the required filtering measures arose during the examination of the 2004 Law on Confidence in the Digital Economy, which specifically transposes the 2000 Electronic Commerce Directive. This law gave the judge the power to require Internet access providers to take the necessary measures to halt damage caused by a public online communications service and suspend access to content that infringes on copyrights. Michèle Tabarot⁽¹⁾, the rapporteur for an opinion of the National Assembly's Committee on Laws, where the articles pertaining to blocking measures were examined, noted on this occasion: (i) the partial inefficacy of these measure at a technical level and the possibilities for bypassing; (ii) the greater efficiency of suppressing content compared with blocking, thus justifying the principle of subsidiarity, according to which measures for preventing access to content must be imposed on hosts prior to being imposed upon Internet access providers⁽²⁾; (iii) the need for interventionary measures when the host eludes legal action due to geographical location. The Senate's Economic Committee's report specified that the powers the law now grants the judge do not significantly depart from the general powers stipulated in the new Code of Civil Procedure in the context of emergency proceedings⁽³⁾.

The 2009 HADOPI Law generated important debates on the issue of suspension of Internet access, which does not directly concern blocking. The transposition of the provisions regarding blocking content that infringes on copyright was also an opportunity for a direct discussion on legal blocking. Michel Thiollière⁽⁴⁾, Senate rapporteur, emphasized on this occasion that: (i) the Court of Cassation nullified the principle of subsidiarity invoked by Internet service providers⁽⁵⁾; (ii) on the basis of technical clarifications provided by the Olivennes mission, and on the basis of filtering, which is defined as the filtering of content. To impose “filtering” obligations upon Internet access providers appears incompatible with European law, specifically contravening the prohibition

(1) See report n° 608, commentary of articles 2 and 3.

(2) The report referred to opinion n° 01-423 of the ART [Telecom Regulatory Authority].

(3) Article 809 of the Code of Civil Procedure provides that a judge may order in the context of a emergency proceedings “the protective measures [...] as required, either to avoid an imminent damage or to abate a manifestly illegal nuisance.”

(4) See report n° 5, comment of article 5.

(5) See Court of Cassation, the June 19, 2008 decree n° 707.

stipulated in article 12 of the Electronic Commerce Directive on imposing a general monitoring requirement on technical intermediaries ⁽¹⁾.

The 2010 law on online gaming and betting that stipulated a blocking mechanism for non-approved online gaming and betting websites instigated a reprise of the previous debates, with the rapporteurs of the National Assembly and of the Senate expressing their support for blocking. A new element of the debate—inspired by stipulations in the LOPPSI tabled to Parliament at an earlier date but actually adopted at a later date—concerned the possibility of introducing an administrative blocking procedure rather than via a jurisdiction.

Finally, the examination of LOPPSI was an occasion for heated discussions on the issue of judicial intervention for ordering blocking of child pornography content; the adopted solution was ultimately based solely on the administrative authority's decision⁽²⁾, unlike the law on online gaming and betting.

► There are currently four legislative foundations for requiring blocking measures that stem from these various laws.

Article 6, I.7. of the Law on Confidence in the Digital Economy: “*When justified by the fight against the dissemination of images or the depiction of minors, under Article 227-23 of the Penal Code, the administrative authority shall notify the persons mentioned in 1 of the present I [Internet access providers] of the electronic addresses of public online communications services in violation of the provisions of this article, that these persons must prevent access without delay.*”

Article 6, I.8. of the same Law: “*In the context of emergency proceedings or by petition, the judicial authority may order any person mentioned in 2 [hosts] or, by default, any person mentioned in 1 [Internet access providers], to take all the necessary measures to either prevent an impending damage or halt the damage caused by the content of a public online communications service.*”

Intellectual Property Code, article L. 336-1: “*In cases of copyright infringement or infringement of a similar right as a result of the content of a public online communications service, the Tribunal de Première Instance, acting in the context of emergency proceedings, when applicable, may order, at the request of the holders of the protected works and objects, of assignees, of companies that collect and distribute author royalties under article L. 321-1, or of professional organizations under article L. 331-1, that all necessary measures be taken to prevent or halt the infringement of any copyright or similar right, by any person in a position to do so.*”

Law pertaining to online gaming and betting, article 61: “*After this period, if the operator in question fails to comply with the order to terminate his gaming*

(1) See *infra*. This interpretation was, however, already convincingly refuted by the analysis of the Olivennes mission's report, p. 34.

(2) See article 4.

and betting activity, the chairman of the Regulatory Authority for Online Gaming may refer to the President of the Tribunal de Grande Instance of Paris, in the form of emergency proceedings, for an order prohibiting access to this service to the persons mentioned in 2 of I [hosts] and, if applicable, in 1 of I [Internet access providers] of article 6 of the June 21, 2004 Law n° 2004-575 on Confidence in the Digital Economy.”

b) Constitutional and European constraints

► The Constitutional Council’s jurisprudence.

While, generally speaking, the Constitution does not require the legislator to provide for judicial intervention for ordering measures that restrict individual liberty⁽¹⁾, in its decision on the HADOPI law, the Constitutional Council ruled that because of the importance of freedom of expression and communication, as well as the role of Internet access with regard to this freedom, the legislator cannot permit an administrative authority to suspend such access⁽²⁾. It then stated in its decision on LOPPSI that the provisions which grant the administrative authority the power to decide mandatory blocking measures must “*ensure a proportionate conciliation between the constitutional objective of safeguarding public order and the freedom of communication guaranteed by article 11 of the 1789 Declaration of the Rights of Man and of the Citizen.*” The administrative authority’s decision can be contested before a judge⁽³⁾.

► European law.

Article 10 of the European Convention on Human Rights protects freedom of expression, but also provides that “*The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or the rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*” Article 12 of the 2000 “Electronic Commerce” Directive prohibits imposing a general obligation on Internet access providers to monitor content, even though there is a general agreement that these provisions do little to limit the blocking requirements that can be imposed upon operators⁽⁴⁾.

(1) See *cahiers du Conseil Constitutionnel* n° 20 regarding the January 19, 2006 Decision n°2005-532 DC.

(2) See the June 10, 2009 Decision n° 2009-580 DC.

(3) See the March 10, 2011 Decision n° 2011-625 DC.

(4) See *Forum on Internet Rights*, “*Les enfants du net III*” emphasizes that “in the current law, article 12 of the June 8, 2000 Electronic Commerce Directive 2000/31/EC limits the conditions of the Internet access providers’ liability resulting from the data they transmit. However, article 12 §3 specifies that these rules will not affect “the possibility for a court or administrative authority, in accordance with the legal systems

c) Key points

First point: the legislator has significant latitude to impose mandatory blocking and filtering measures. The standards of Constitutional law and European law do not require more than the fact that blocking and filtering respond to a legitimate objective. However, it is not because the legislator can impose blocking measures that it must do so.

Second point: legislative pressure increases over time. The increase in blocking requests is evident both quantitatively (there was a single legislative framework adopted between 2004 and 2009 compared with three since 2009) and qualitatively (with the will to impose performance requirements upon Internet access providers and avoid judicial intervention).

3. Policy debate

Increasing legislative pressure and the relative technical inefficiency of blocking, as described above, raise questions regarding the justification for mandatory blocking measures.

a) The players' positions and the arguments raised

► The players' positions.

In France, the debate is between the “Internet realm” and “the cultural realm,” specifically:

– Associations of Internet users who: (i) oppose blocking because it restricts freedom of expression, it is inefficient, and because Internet access

of Member States, to require a service provider to terminate or prevent an infringement.” The report of the Olivennes mission observed that “these stipulations must be understood with regard to their purpose: they concern the procedures under which service providers are liable, and are therefore addressed to the judge, who will determine the existence (or not) of damages that can be repaired. The principles of the 2004 Law, which incorporates those of the Directive, seek to avoid having a national jurisdiction rule on the service provider’s fault for the mere fact that illicit content is found on his networks, and that the provider is consequently considered in breach of a general obligation to monitor all of the data he transmits. Articles 14 and 15 emphasize that in cases of infringement on intellectual property rights, a service provider can be ordered to pay damages for identified offenses only, which therefore pertains to civil or penal liability, assessed restrictively. These provisions appear not to affect an injunction or filtering order. Using a filter does not equal network surveillance: it is merely a technical instrument that does not require the access provider’s intervention. (also refer to the judge’s well-argued position in the Court of First Instance of Brussels’ June 29, 2007 decision n° 04/8975/A SABAM v/ SA Scarlet, against which an appeal has been lodged). On this point, recitals 45 and 47 of the Directive are very clear. First, it is stated that the Directive’s provisions on liability must not prevent the development and the actual implementation of technical systems for protection and identification, as well as technical monitoring instruments made possible by digital technology. Second, it is emphasized that the limitations on the liability of intermediary service providers are without prejudice to the possibility of different kinds of injunctions, which can, in particular, consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or disabling access to it.” (p. 37).

providers refuse to also be enforcers; (ii) demand judicial intervention in cases where such measures are nevertheless implemented⁽¹⁾;

– Internet access providers who: (i) oppose blocking on the grounds that it is inefficient and costly; (ii) and, in the event that blocking is implemented, request financial compensation and the right to choose the technical solutions best adapted to their networks and subsequently implement only those measures enacted by the public authorities to avoid liability for the consequences of blocking⁽²⁾.

– Companies of rights holders who request: (i) that the law allow for the blocking of content exchanges that infringe on copyrights⁽³⁾; (ii) that Internet access providers conduct filtering tests at the network’s core, as agreed on in the framework of the 2007 Élysée agreements⁽⁴⁾.

It is useful to reiterate the fact-finding mission’s first guidelines on blocking and the response they elicited:

– Unification of the legal procedures for determining mandatory blocking measures and systematic judicial intervention (§23, third indent) were not opposed;

– However, the proposal to limit “*filtering requirements [...] of the most harmful content, or when there is no risk of developing bypassing techniques detrimental to the Internet's functioning*” (§19, first indent), raised questions on what the fact-finding mission meant by “*most harmful content*,”

– The appropriateness of establishing a proportionality requirement for legal filtering measures and to confer its enforcement to the ARCEP (§24, first indent) was not understood: its purpose was to recommend intervention by the ARCEP in order to evaluate adverse consequences generated by blocking measures on a case-by-case basis and suspend implementation if their impact is too great;

– Blocking and filtering implemented at the operators’ initiative were also considered jointly with legal blocking and filtering (§15, §19 second and third indent). It seems clearer to deal with this issue in the context of the analysis on traffic management as a means to restrict access to certain contents.

(1) See for ex., *The responses of La Quadrature du Net* (p. 8) and of *l’UFC-Que Choisir* (pp. 4-6; 9) to the European Commission’s consultation on Net Neutrality.

(2) See for ex., *The positions included in the aforementioned legislative reports*.

(3) See *Interview of Pascal Rogard, General Manager of the SACD, in the introduction to the ARCEP’s April 2010 conference on Net Neutrality, where he declared that, “Net Neutrality must not mean impunity”* (40-48 sec.) reused in the slogan: “*Net Neutrality must not equal net impunity.*”

(4) *These agreements stipulated that Internet access providers agree “to cooperate with rights holders on the procedures for testing the available network filtering technologies—which require prior in-depth preparation—and deploy them if the results are conclusive, as well as generalize technically and financially realistic solutions, no later than 24 months following the signing of the present agreement.”* (p. 2).

► Arguments exchanged.

The in-depth debates that arose in the course of the examination of LOPPSI served to clarify the content of the arguments exchanged⁽¹⁾.

Those in favor of blocking argued with regard to the proposed blocking system: (i) that such systems have been successfully implemented abroad; (ii) that blocking represents a non-excessive restriction on freedom of expression (and can, in particular, be contested before a jurisdiction); (iii) that a procedure via the administrative authority instead of a judge allows for greater responsiveness.

Those opposed to blocking cited: (i) technical inefficiency due to the possibility of circumvention; (ii) ineffectiveness as a result of hosts quickly removing child pornography content when reported; (iii) the risk of abuses related to the creation of a black list, which have all been established in countries implementing blocking; (iv) the counter productivity of these measures, which in fact reduce international cooperation in the fight against child pornography; (v) risk of over blocking and the threat to the network's resilience; (vi) finally, generalization of the exchange of encrypted data and the use of proxies.

b) The mission's analysis

► The issue of blocking.

The issue of legal blocking can be clarified by identifying three questions.

- First question: What are the circumstances under which it would seem legitimate—given the balance to achieve between the freedom of communication and other public interests—to require operators to implement blocking measures? This is a problem of arbitration between conflicting values, which is the most commonly debated issue at the legislative level. It is useful to emphasize that, generally speaking, it is not incontrovertible that one should prevent “unlawful” electronic communications (prevention) instead of condemning unlawful activities supported by these communications (sanction). The choice between the means to fight unlawful activities depends upon, including but not limited to, the threats that preventive measures pose to civil liberties.

– Second question: Who is to determine what content must be blocked? This question refers to the issue, more recent at the legislative level, of whether a judge or the administrative authority should intervene to impose mandatory blocking measures.

– Third question: Do the positive effects anticipated by implementing blocking measures outweigh the negative effects? This is the standard question

(1) See specifically the Government's impact study (pp. 7-17), referral, the Government's observations, comments in the Constitutional Council's publication regarding the March 10, 2011 decision n° 2011-625 DC (p. 3-5), as well as the memo in *amicus curiae* of La Quadrature du Net “Administrative filtering of the Internet is contrary to the French Constitution.”

surrounding the efficacy of filtering, which should, however, be viewed in the broader context of a cost-benefit analysis. The question to the legislator is not only to determine: (i) whether mandatory blocking measures constitute a balanced conciliation between freedom of expression and other public interests (perhaps); (ii) and whether they are effective (not totally); but also (iii) whether the projected benefits outweigh the costs or risks (apparently not). In this regard, the following analogy may help illustrate the question: Using a mobile phone while driving is dangerous and constitutes an “illegal” communication that the police sanction when it can be established and that is subject to preventive measures in the context of road safety. Does this, however, warrant implementation of a complex and costly system for blocking communications while driving by geolocating calls and systematically analyzing the voice signal to identify those calls made while driving, and have the ability to block them?

► Guidelines.

The arguments against blocking are numerous: low efficacy for persons with a true willingness to commit offenses; negative effects resulting from over blocking and network resiliency; disproportionate costs for more subtle techniques, such as hybrid filtering, compared with the projected benefits, etc. An additional argument of particular importance emerged during the mission’s work: It is not certain that the results of legal blocking are positive in terms of safety. Indeed, many Internet users are committed to freedom of communication and thus capable of collaborating on developing applications to conceal their communications and evade surveillance. This could lead to a convergence between the practices of the general public and those of criminal organizations already employing sophisticated tactics for concealing communications (anonymization, encryption, etc.). These factors have motivated the fact-finding mission’s recommendations, presented in the third section of the report, to systematically include judicial intervention, to conduct additional investigations on the effects of blocking, and, until such time, to refrain from enacting new measures.

In conclusion, systematic blocking does not appear to be a solution to the complications posed by the evolution of the Internet on the future of cultural and entertainment industries, and, more generally, complications related to the territorialization of law in sectors with highly intangible activities.

B. — TRAFFIC MANAGEMENT

► If the issue of legal blocking measures, as just discussed, constitutes an important aspect of Net Neutrality, the heart of the debate focuses on a subject less apparent to the general public, which is “traffic management.”

It is useful to define several concepts prior to presenting this issue:

– According to the ARCEP’s definition, “traffic management” refers to all forms of technical intervention on implemented data flows that identify the type of traffic or the identity or status of its transmitter or recipient⁽¹⁾;

– Public Internet is called “best effort” since by design it does not offer performance guarantees for the delivery of Internet traffic (time frame, data loss, etc.)⁽²⁾;

– “Managed services” can be defined as the various services to electronically access content, services, and applications, for which the network operator guarantees specific characteristics end-to-end (as opposed to best effort public Internet) via the processes implemented, either directly on the network it controls or through agreements with operators handling traffic delivery⁽³⁾.

► The debate over traffic management fundamentally refers to Internet architecture and whether it is appropriate that intelligence is included in the network instead of only at the end points⁽⁴⁾, which, until now, concentrated most of the debate on neutrality⁽⁵⁾. One of the fact-finding mission’s contributions, in relation to previous studies, specifically by the ARCEP, is to perhaps better link this issue with the issues raised by mandatory blocking and interconnection measures⁽⁶⁾. Traffic management, however, poses specific problems, particularly concerning the prioritization of certain flows and Internet quality.

1. Techniques

Methods for traffic management are harder to document than those relating to legal blocking. However, it is possible to provide clarification from studies implemented by public authorities or operators⁽⁷⁾.

(1) See the first ARCEP guidelines (p. 10). It’s not about modifying the traffic’s content, but rather modifying delivery according to some of these characteristics.

(2) *Ibid.*

(3) *Ibid.*

(4) See the defense of an “end-to-end” network architecture, according to J. H. Saltzer et al. “End-to-end arguments in system design,” 1984, specifically used by Lawrence Lessig and Robert McChesney, “No Tolls on the Internet,” Washington Post, 2006, but criticized, for example, in “Engineering Background” communicated by AT&T in response to the European Commission’s consultation on Net Neutrality (p. 13).

(5) Seven of the eight recommendations made by the ARCEP in its initial guidelines, the FCC’s December 2010 four principles, nine of the fifteen questions in the European Commission’s consultation are specifically devoted to the subject.

(6) Some blocking implemented at the operators’ initiative is likely to have effects comparable to legal blocking, such as the development of masking techniques, bringing the practices of the general public closer to those of criminal organizations. Interconnection may, in turn, have a serious impact on the quality of the Internet and be a vector for discrimination

(7) See specifically OCDE, 2007, “Report on Internet Traffic Prioritization” (pp. 7 and fol.); ERG (08) 26b part 3 “Technical Background Information,” 2008 (pp. 53 and fol.); AT&T, “Engineering Background” in response to the European Commission’s consultation on Net Neutrality, 2010.

a) Quality

► The performance of an electronic communications network can be determined via the bandwidth (“size” of the pipe), latency (transmission delay from point of departure to destination), jitter (variation of this delay), the packet loss rate and error rate (no data transmission or transmission of erroneous data)⁽¹⁾.

The needs of the various services and applications in terms of network performance are variable, and it is specifically possible to distinguish between bandwidth-intensive applications (such as video) and those that are not (such as electronic mail), as well as between real-time applications, called “synchronous” (such as telephony) and applications called “asynchronous” (such as file sharing).

We must note that Internet quality from the user’s viewpoint, often called “quality of experience,” does not necessarily correspond to the performance of the operator’s network to which the user is connected:

– It depends primarily on the connection’s bandwidth at the end points: watching a high-resolution video will be difficult with an Internet access with a maximum speed of only 512 Kbps on the user’s side; and if the servers are saturated or if the per-user speed is limited, on the content provider’s side;

– Since most communications pass through several networks, the quality perceived by the user depends not only on the performance of the other operators’ networks, but also on how the various networks are interconnected, that is to say, interconnection;

– Quality is highly dependent on the location of the content or services the Internet user wishes to access: the more distant the content the greater the likelihood of a decrease in quality of communication when crossing congested network points. This explains the development of CDNs as well as the interest in peer-to-peer networks, which are used to distribute file exchanges between multiple users.

The term “quality of service” (QoS) is used in a narrow sense to refer to the quality guarantees for delivery services, mainly implemented on shared IP networks by defining classes of services with different priority levels. The term is also used in a broad sense to designate network performance, as defined above, including quality of experience.

► Traffic management as defined above in other words, as the intervention of operators on data flows, has ambiguous effects on traffic delivery:

(1) See *Rec. Y 1540*, Quoted in the *BEREC’s reponse to the European Commission’s consultation on Net Neutrality* (p. 19) and the *ARCEP’s initial guidelines* (p. 28).

– On the one hand, it can provide guarantees in terms of quality of service, thus providing better service to users, and may also allow smarter management, thus saving bandwidth⁽¹⁾;

– On the other hand, it tends to favor certain flows, which, at equal bandwidth, is detrimental to the other flows, therefore degrading their quality. Hence the problem of discrimination in the delivery of flows arising from traffic management with regard to the principle of Net Neutrality.

b) Traffic management technologies

To understand the discussions on traffic management, it is useful to have information on the available methods and the methods that operators are currently implementing.

Any network is subject to “traffic engineering” operations, which ensure the proper transmission of electronic communications. Traffic engineering includes several types of activities:

– “Planning capacity” implemented on a monthly or yearly basis, which organizes physical infrastructures to achieve the necessary capacities to deliver traffic injected into the network;

– “Traffic management,” which can be implemented in a much shorter time frame, seeks to relieve congestion and is specifically based on: (i) redefining the routes for traffic delivery, (ii) reserving capabilities, and (iii) traffic “shaping.”

To understand the discussion on traffic management, we must clarify two points regarding the Internet’s functioning. First, as mentioned earlier, the Internet is historically a best effort network, meaning it does not provide a guaranteed quality of service. This does not mean, however, that the quality of the Internet is poor: increasing fiber and router capabilities have allowed the delivery of sharply increasing data volumes with an improvement in quality perceptible to the Internet user. Most applications do not need a quality guarantee. Second, the convergence of networks toward all-IP networks has meant that delivery services with a guarantee of quality, or “managed services,” in the terminology adopted by the ARCEP, use mostly the same “pipes” and equipment as the Internet.

Routers now allow traffic management on very-high-speed networks, either by predefining paths (in MPLS, for example), by conserving resources (in

(1) For example, ADSL TV is broadcast in multicast, which means that if several subscribers want to access the same program, it will be sent only once, as long as the same path can reach the various subscribers and is “replicated” when paths diverge. If television were not managed, the program would be sent separately to each Internet user on the entire network, which would consume much more bandwidth. Another example is mobile video broadcast from the operators’ platforms and encoded in a format adapted to the display capabilities of mobile terminals. If Internet users access the same video via the Internet, chances are that the format is adapted to a fixed terminal, therefore needlessly consuming bandwidth.

RSVP, for example), or by a differentiated processing of flows (in DiffServ, for example). Some clarifications on how DiffServ routers function is useful:

– When data packets arrive at a router, they are added to a queue before the router reads the destination address and orients the packet in the right direction from the routing table;

– If there is no congestion, router processing is almost instantaneous and there is no quality-of-service problem; however, if there is congestion, arriving packets are placed into a buffer, then, without sufficient time to be processed by the router when new packets arrive, they are deleted for the router to receive new packets;

– DiffServ routers allow a differentiated processing of flows in the event of congestion by placing them in various buffer zones according to the priority level of each packet, and by programming the router to prioritarily process the packets of priority buffers according to rules that may vary.

Much of the debate centers around the development of deep inspection (DPI) techniques, which allow packets to be distinguished not only according to the priority level written on their header, but also “on the fly” from the routers’ identification of characteristics not included in the header (for example by extrapolation of the protocol).

Finally, the blocking and filtering techniques described in the section on legal blocking that occur at the initiative of the operator; for example, blocking certain applications on the basis of a standard port number listed in the packets’ header, can be considered traffic management techniques.

c) Key points

First, traffic management is especially useful for allowing operators to guarantee the quality of managed services in all-IP networks⁽¹⁾. Its use in coping with increasing traffic and managing congestion seems limited⁽²⁾.

Second, we must emphasize that traffic management is one method among several for ensuring a quality delivery of electronic communications. This essentially depends on the saturation, the applications’ needs, and the location of the content requested by the consumer, and therefore on the operators’ investment in properly sizing their networks and interconnections, the intervention of the CDNs, and the format of the data exchanged.

(1) *We must distinguish the “channels” of the managed services from Best Effort Internet.*

(2) *According to data mentioned by AT&T in its “Engineering background,” submitted in response to the European Commission’s consultation on Net Neutrality, prioritization of 10% of the traffic would virtually double the available bandwidth (note 54, p. 19). Individuals interviewed by the mission spoke of the gains of a lower order of magnitude. In any event, these gains are unrelated to the recurrent traffic increase and the increased capacity of fiber and very-high-speed routers.*

Third, if it is relatively easy to determine what technologies are available, it is much harder to know what technologies have been implemented. A few remarks: (i) operators seem to manage telephony and television services in triple-play offers by reserving capacities for them; (ii) operators offer services with a guaranteed quality of service to companies, and in this context resort to traffic prioritization techniques that could degrade the quality of the Internet⁽¹⁾; (iii) French Internet access providers state that they have no commercial agreements with Internet content providers to prioritize the delivery of their content⁽²⁾.

2. The legal framework

Before presenting the rules that pertain to traffic management, it is useful to make some general remarks on the subject: (i) there are no real constraints arising from the French Constitution or European law; (ii) the legal framework on the whole imposes relatively few constraints on operators; (iii) the content of existing rules is uncertain, as they essentially proceed either from general sectorial or competition regulation, when these applications do not currently exist, or from new powers stemming from the third Telecom Package, which are not yet in force⁽³⁾.

a) Regulation directly arising from the law

Analysis of these obligations concludes that their scope is relatively limited:

– In application of article L. 32-3 of the Postal and Electronic Communications Code, operators and their employees are required to maintain the secrecy of correspondence. The application of secrecy of correspondence poses difficulties that can be illustrated via two examples: (i) if an email manifestly enters in the category of correspondence, what about data exchange initiated on a website or a text written in a forum? (ii) If the header of the IP packet is analogous to the address on a physical letter, should extrapolation of the protocol, or other methods of deep packet inspection, be considered the same as reading a message?

– Article L. 32-3-3 of the Postal and Electronic Communications Code stipulates that any person providing transmission of content on an electronic communications network or access to an electronic communications network may

(1) This point is difficult to assess, as there is no precise information on the traffic management methods operators have implemented, as well as on the level of network congestion and the volumes transported according to type.

(2) The existence of commercial agreements for prioritizing the delivery of content in the United States was raised during the mission's interviews. One difficulty is the changing nature of the concept of managed services.

(3) Interpretation of these rules is based on the analyses of Winston Maxwell and Nicolas Curien in *La neutralité d'internet, 2011* (pp. 101-104; application of competition law), on BEREC's response to the European Commission's consultation on Net Neutrality (pp. 6-7; application of law on sectorial regulation), as well as on its discussions with the ARCEP (application of the new provisions stemming from the Telecom Package).

incur civil or penal responsibility for the content only in the following cases: if it initiates the litigious transmission request; if it selects the recipient of the transmission; or if it selects or modifies the content sought by the transmission. The operators' limited liability with regard to the content they deliver arises from the 2004 Law on Confidence in the Digital Economy that transposes the 2000 "Electronic Commerce" Directive. Implementation of traffic management techniques clearly leaves intact the operators' limited liability, since it does not involve choosing the recipient or modifying the content, as indicated by the preceding technical presentation.

– In application of article L. 33-1 of the Postal and Electronic Communications Code, operators of networks open to the public can be subject to obligations having to do with the confidentiality and neutrality of transmitted messages and data related to the communications. Article D. 98-5 of the same code, which specifies these obligations, merely indicates that operators must take "*the measures necessary to guarantee the neutrality of their services vis-à-vis the content of messages transmitted over its network and the secrecy of correspondence*" and must implement their services "*without discrimination, regardless of the nature of the messages transmitted.*" The aforementioned observations on the ambiguity of the notion of "correspondence" over the Internet also apply to the concepts of "content" and "message" here.

b) Regulation directly arising from sectorial and competition regulation

Competition and sectorial regulation both seek to impose obligations upon economic players in the case of market shortcomings, including "remedies" should competition issues arise. In order to understand the guarantees provided, it is necessary to present an example. One of the main issues raised by traffic management is the discriminatory treatment of same-type flows; the following analyses will use the example of an operator who prioritizes its own content while refusing to market the same priority to a competitor.

► Sectorial regulation.

The legal framework for the actions of the sectorial regulator, namely the ARCEP, in France, allows the regulator, in theory, to react to discrimination.

The objectives defined by the ARCEP, first in article L. 32-1 of the Postal and Electronic Communications Code, also completed in the framework of the transposition of the third Telecom Package, include the protection of several neutrality components; specifically, nondiscrimination between operators and service providers, introduced in the context of the transposition of the third Telecom Package (in 4° bis A of the aforementioned article).

The ARCEP also has three types of instruments at its disposal to handle the issue of discrimination. The practical scope of these three instruments currently appears, if not limited, at least uncertain.

– Asymmetrical regulatory powers allow the ARCEP to impose specific requirements, called “remedies,” on operators that exert a significant influence on a market⁽¹⁾. Using these powers to address the discrimination, as in the example provided, would, however, encounter two obstacles: (i) this market is not included in the European Commission’s 2007 recommendation determining which markets can be directly regulated asymmetrically. This would necessitate demonstrating that this market satisfies the “three criteria” test provided in the recommendation’s second point⁽²⁾, even though the European Commission has already ruled on a specific case against compliance with the transit and peering markets test⁽³⁾; (ii) even if this market passed the “three criteria” test, considering its rapid evolution, it is uncertain whether the tools for asymmetrical regulation, which were intended to function in the much more stable environment of telephony, would be adapted.

– The ARCEP’s powers for symmetrical regulation, specifically regarding access and interconnection, were extended by the third Telecom Package, which explicitly confers upon national regulatory authorities the capacity to impose obligations upon operators that service the final client to compel them to ensure interoperability⁽⁴⁾. However, the BEREC observes that “*due to the new status of the provision, it remains to be seen how this article is implemented in the various Member States, and hence how helpful it will be in solving the issues identified [discrimination issues]*”⁽⁵⁾.

– Finally, article 20 of the new “framework” Directive, along with a new definition of “access,” to be transposed by ordinance into French law⁽⁶⁾, expands the national regulatory authorities’ dispute resolution powers. It is helpful to note the BEREC and the ARCEP’s observations on the scope of this expansion: (i) dispute resolution powers are not a true regulatory tool, since they resolve only specific cases; (ii) such powers may nevertheless constitute a credible threat that imposes a form of unity on the operators’ practices; (iii) when the ARCEP decides in equity, the plaintiff must prove discriminatory treatment. This can be

(1) See articles 8 and fol. of the “access” Directive transposed to articles L. 37-1 and fol. of the Postal and Electronic Communications Code.

(2) The three criteria are: a) the presence of high and non-transitory barriers to entry. These may be of a structural, legal, or regulatory nature; b) a market structure that does not tend toward effective competition within the relevant time horizon. The application of this criterion involves examining the state of competition behind the barriers to entry; c) application of competition law alone would not adequately address the market failure(s) concerned.

(3) See the European Commission’s March 3, 2010 Decision on cases PL/2009/1019 and PL/2009/1020.

(4) See articles L. 34-8 and following of the Postal and Electronic Communications Code (regulation of access and interconnection), article 5 of the modified “access” Directive (to impose obligations to ensure interoperability).

(5) See the response to the European Commission’s consultation on Net Neutrality (p. 7).

(6) In the last version communicated to the National Assembly, the draft ordinance introduces a new paragraph in article L. 36-8 of the Postal and Electronic Communications Code, which will stipulate: “If negotiations fail, a dispute can be brought before the ARCEP with regard to [...] the technical and financial terms and conditions for transmitting traffic between an operator and a company that provides public online communication services.”

complicated, particularly for smaller players, and *de facto* limits the framework's scope.

► Competition Law

In answer to the proposal to enact specific rules to prevent discrimination caused by traffic management, many players invoke the general rules of competition law. This response, however, is not entirely persuasive, in part because the procedures of competition law are often long and complex, and in part because it is uncertain that competition law can solve problems like those in the example offered⁽¹⁾, or by prohibiting cartels and abuses resulting from dominant positions⁽²⁾.

– If competition law sanctions anticompetitive cartels, it nevertheless allows exclusivity agreements, “*analyzed [by the competition authorities] on a case-by-case basis by weighing the negative effects on market dynamics, compared with their potentially positive effects on innovation*”⁽³⁾.

– Abuse of a dominant position is defined by the existence of: (i) abuse, meaning refusing to deliver a competitor's content with the same level of priority, relatively easy to demonstrate in our example; (ii) a dominant position, which requires identifying the market on which an operator holds a dominant position; this can be difficult to establish. It is therefore not incontrovertible that the operator holds a dominant position on the highly competitive wholesale interconnection market (peering and transit), or on the retail market (where market shares are divided between several Internet access providers). The possibility remains of defining a specific market for each operator that services final customers, which precisely consists in serving those final users, as is the case for call termination. As mentioned above, the European Commission did not follow this reasoning in a specific case⁽⁴⁾.

c) Stipulations stemming from the third Telecom Package

Although already discussed in part, it is useful to review the provisions for regulating an operator's traffic management included in the third Telecom Package.

– First, these are new transparency obligations. The transposition ordinance provides for new clauses to be included in all electronic

(1) As Winston Maxwell and Nicolas Curien noted, “*Since competition law, versatile by nature, applies to the entire economy and therefore specifically to the various players of the Internet value chain, and since its objective is to sanction anticompetitive behaviors, it would a priori seem that this law is a panacea for addressing this issue. Reality is much more nuanced*” (see *La neutralité d'internet*, 2011, p. 101).

(2) See Articles 101 (prohibition of cartels) and 102 (prohibition of abuse of dominant position) of the Treaty on the Functioning of the European Union.

(3) See Winston Maxwell and Nicolas Curien, *La neutralité d'internet*, 2011, p. 104.

(4) See the European Commission's March 3, 2010 Decision on cases PL/2009/1019 and PL/2009/1020.

communications service agreements in a clear, comprehensive, and easily accessible manner, that will specifically pertain to: the traffic management procedures implemented, restrictions on access to services or equipment, and procedures to ensure the network's security and integrity (amended Article L. 121-83 of the Consumer Code).

– Second, to extend the ARCEP's dispute resolution powers to cover disputes between operators and other companies on the financial and technical terms and conditions for traffic delivery (Art. L. 38-4 of the Postal and Electronic Communications Code).

– Finally, an important provision, which has not yet been discussed, stipulates that national regulatory authorities can require operators to implement a minimum quality of service on networks to prevent congestion. This provision should be transposed in Article L. 36-15 of the new Postal and Electronic Communications Code, stipulating that *“In order to prevent degradation of service and obstruction or slow-down of traffic over networks, the Regulatory Authority for Electronic Communications and Postal Services can define, in accordance with Article L. 36-6, minimum quality-of-service requirements. Before imposing such requirements, the Authority will inform the European Commission and the BEREC of the reasons for its intervention, and the proposed requirements and approach. The ARCEP gives the utmost consideration to the comments and recommendations of the European Commission when defining such requirements.”* This power has a direct bearing on traffic management, since it was introduced in the Telecom Package to provide guarantees against the risk of managed services “crushing” the public Internet.

3. Policy issues

These technical and legal components clarify the neutrality issues raised by traffic management. Several observations can be made at this stage:

– Regarding the appropriateness of legislative intervention, we must emphasize that it is not: (i) because traffic management is not regulated that it should be (the market is perhaps capable of functioning without regulation), (ii) because it is desirable for certain traffic management practices not to occur, that government measures should be taken to avoid them (it is still imperative that the benefits of intervention outweigh the costs, including those related to legislative inflation);

– It is possible to identify three themes within the issue of traffic management: (i) transparency, around which there is relative consensus, is left out of the present debate (the various players would like the consumer to know what traffic management mechanisms are implemented by operators and what they imply in terms of features offered); (ii) discrimination, which concerns three types of practices: blocking, targeted degradation of quality, and prioritization (which refers to the issue of managed services); (iii) Internet quality, which appears

somewhat peripheral at first glance, but is in fact closely related to the two preceding issues.

a) The players' positions and the solutions proposed by the regulators

► The players' positions.

It is more difficult to clearly identify the positions of the various categories of players on the issue of traffic management than it is for the issues related to mandatory blocking measures and data call termination. This difficulty arises in part from: (i) a fairly broad consensus around the notion that alongside public Internet, where traffic management can be regulated, an area should be left to managed services, which do not require the same regulation; (ii) the variable definition of the concept of managed services.

In view of the traffic management admissible on the Internet, and the extension granted to the notion of managed services, two positions among the players can be identified:

– Neutrality “maximalists” are against: (i) any blocking and (ii) any prioritization of traffic on the public Internet, and therefore against any use of “formatting” techniques on Internet traffic, and (iii) they condone implementation of managed services only for applications that truly require it, or which are not available on the public Internet⁽¹⁾;

– Neutrality “minimalists” are in favor of: (i) the possibility, at least for mobile telephony, of marketing offers that include access restrictions to certain services (without VoIP, for example), (ii) reasonable traffic management practices, that is to say, using formatting techniques on public Internet traffic according to the applications' objective requirements, specifically during peak hours, and (iii) the possibility of marketing, in the form of managed services, services that can be delivered on the Internet without the same guarantee of quality⁽²⁾;

– As revealed by the information communicated by the players interviewed by the fact-finding mission in response to its initial guidelines, there is currently no player in France that explicitly favors complete freedom in traffic management, specifically with regard to prioritizing content, services, or applications accessible on the Internet on a purely commercial basis⁽³⁾.

(1) See for example the stance of *Quadrature du net* or of the French Data Network.

(2) See the stance of most Internet access providers.

(3) Several players have noted that there is no standardization of “classes of service” on the Internet, and that a guarantee of priority from end-to-end would require a complete overhaul of existing interconnection agreements, covering only the best effort. Furthermore, from a technical standpoint, a porous border between the Internet and “managed services,” as well as a rather variable definition of managed service that can go to any flow other than the pure best effort, make it possible to consider delivery agreements with quality of service as “managed services,” which could easily go through the Internet and serve to showcase commercial distribution agreements between content providers and Internet access providers. In

► Comparison between the positions of French and American regulators.

Since the issue of traffic management has been the most studied, the solutions recommended by regulators are quite sophisticated and it is useful to present them in detail.

– The ARCEP has enacted the following recommendations: (i) the principle of no blocking or discrimination⁽¹⁾; (ii) exceptions to these rules are acceptable provided they are relevant, proportionate, effective, nondiscriminatory between players, and transparent⁽²⁾; (iii) free development of managed services, as previously defined, but with guaranteed quality of the Internet, still undefined, to prevent degradation resulting from the development of managed services⁽³⁾.

– The FCC has enacted the following rules: (i) no blocking on fixed networks, no blocking of the Internet, and no blocking of voice and video services that compete with services distributed by operators on the mobile network; (ii) no unreasonable discrimination in quality of delivery; (iii) free development of managed services, while carefully monitoring their impact on the Internet.

The ARCEP's position seems more protective of neutrality than the FCC's, since it contains: (i) a guarantee of Internet quality; (ii) the principle of prohibiting all blocking. However, it should be noted that: (i) the ARCEP only enacted recommendations, while the U.S. regulator enacted binding obligations⁽⁴⁾; (ii) the FCC's decision applies to the data services passing through IP networks, while the ARCEP's decision presumably concerns "Internet access" services only⁽⁵⁾; (iii) regarding quality guarantees, the third Telecom Package granted national regulatory authorities the power to impose minimum quality of service requirements on operators, yet the recommendation does not define a minimum guarantee of quality, which is the central issue; (iv) regarding nondiscrimination: the exceptions the ARCEP recommends implementing do not clarify the difficult practical questions raised in the course of the debates on Net Neutrality any more than the FCC's concept of "unreasonable" discrimination.

this context, it is difficult to define what a "multi-speed" Internet could be: the current "best effort" Internet is already the lowest class of service of all-IP networks.

(1) *These principles stem directly from recommendations n°1 and n°2.*

(2) *The exceptions stem from the framework provided in recommendation n°3.*

(3) *This rule is defined via recommendations n°1 and n°4.*

(4) *There is, however, an intense debate on the legal capacity to enact its recommendations: see specifically Commissioner Robert. M. McDowell, "Extended Legal Analysis: The Commission Lacks Authority to Impose Network Management Mandates on Broadband Networks," in Dissenting Statement, 2010.*

(5) *This stems from the fact that the only sanction provided in the ARCEP's September 2010 first guidelines is the prohibition to use the term Internet access for marketing services that do not respect the principle of neutrality.*

b) The mission's analysis

The discussions held so far and the recommended regulatory frameworks still leave uncertainties as to the appropriate standards to enact. The absence of clear recommendations from regulators to address the main practical traffic management issues indicate that neither the FCC's rules, nor those of the ARCEP offer definite conclusions on the pay-as-you-go options for unlocking mobile VoIP services, the slowing of peer-to-peer during peak hours to handle congestion, or the refusal to upgrade the interconnections of targeted players.

It does not seem appropriate to establish rules based on uncertainties. We must therefore return to the certainties: (i) the consumer must be able to choose between proposed offers; (ii) the Internet should not be discriminatory in order to allow for maximum innovation. Based on this assessment, the fact-finding mission's recommendations for traffic management seek to separate two layers: a layer of neutral Internet, without traffic management, whose quality must be measured and guaranteed; and a layer of managed services freely developed by the operators, provided the quality of the Internet remains at a sufficient level.

C. — INTERCONNECTION

► For introductory purposes, it is useful to clarify the concept of interconnection, which refers:

– Generally speaking: to how the Internet operators' networks are connected to one another or "interconnected;"

– More specifically: (i) to the legal and practical rules that pertain to direct "exchanges of traffic" between operators and, occasionally, between operators and content providers; (ii) to the physical location where these exchanges occur, called "interconnection points."

► Interconnection is fundamental to the Internet's functioning, both: (i) from a technical standpoint, since it is a global network of tens of thousands of networks that must be interconnected to one another; (ii) from an economic perspective, since it is through traffic exchanges that most of the economic relationships between different categories of Internet network players occur, and that financial flows between them are determined.

Interconnection is related to the issues already discussed. Thus, the large number of interconnections between French networks and foreign networks makes it more difficult to implement filtering obligations. To cite another example, the quality of the Internet depends largely on interconnection design; simply put, the "size" of the pipes between Internet access providers and other Internet operators. But it also raises specific issues, such as "data call termination."

1. Practices

a) Technical functioning

Interconnection is fundamental to the functioning of the Internet, since it is a global network of tens of thousands of networks that must be interconnected. As already discussed, each network is an autonomous system (AS) managed by an operator with a block of IP addresses. Through a protocol called BGP, operators automatically exchange “routes,” that is to say, information on the paths to take to effectively reach the IP addresses. Depending on how the routes are exchanged, there are at least two types of interconnection:

– “Transit” is an interconnection by which an operator announces all the Internet routes to another operator, who in response announces only the routes leading to his own IP addresses. To ensure the Internet’s connectivity—that is to say, the ability for every person connected to the Internet to communicate with any other person connected—given the number of Internet operators, it is in fact impossible for every operator to be directly connected to all other operators.

– Peering is an interconnection by which two operators announce only the routes leading to their IP addresses. The shortened path of the Internet flows improves Internet quality by bypassing transit providers.

It should be noted that while voice services are now widely available over IP, telephone interconnection is still physically distinct from Internet interconnection, since there is no common standard for exchanging VoIP traffic and, generally speaking, IP traffic with a guarantee of quality⁽¹⁾.

b) Economic relations

Despite the market’s opacity, due in part to the absence of intervening regulators, along with a rapid evolution and the resulting tensions, we can provide clarifications, at an economic level, on interconnection agreements⁽²⁾.

► Players.

To understand interconnection agreements, we must distinguish between several categories of players:

(1) See the ARCEP’s February 2011 document: “Analyse des marchés de la téléphonie fixe, troisième cycle : 2011-2014, Consultation publique 23 février-23 mars,” in which the ARCEP emphasizes that: (i) although many operators provide their voice services over IP (VoIP is different from the “voice over Internet” provided directly on the Internet as an application, with no guarantee of quality of service), there is currently no standardized interface for VoIP, because of “the diversity of transmission technologies for voice over IP, whether the codecs used to compress voice or the signalling protocols to control voice flows in IP mode (absence of standardization);” (ii) as a result, the TDM (time division multiplexing) interfaces used for conventional switched telephone networks are still employed and, when sent over IP, voice must be converted before interconnection, which is inefficient.

(2) We must note that most tier-one operators, as well as certain Internet access providers, publish their interconnection policy.

– Tier one operators are connected to almost all the networks of the Internet. They convey substantial volumes of data, and offer transit agreements to lower level operators (e.g., AT&T, Cogent, Comcast, Level 3, Orange, etc.);

– Tier two operators include Internet operators, specifically Internet service providers on a national scale, that purchase transit from tier one operators, contract free peering agreements between themselves, and can offer paid peering agreements to content providers (e.g., Free, SFR, etc.);

– etc.

► Agreements.

Transit agreements are paid, and the transit provider invoices his co-contractor. They generally provide: (i) that transit is invoiced at maximum incoming or outgoing speed clipped at the 95th percentile; (ii) a commitment to speed.

Peering agreements are sometimes free, particularly when two operators of a similar size wish to directly exchange traffic, allowing them: (i) to improve the quality of delivery; (ii) avoid using a transit provider; (iii) avoid transaction costs when the volumes they plan to exchange are of the same order of magnitude. There are also paid peering agreements that generally allow content providers to directly access the network of an Internet access provider without using a transit provider.

► Points of interconnection.

There are different types of physical locations through which operators interconnect. It is specifically useful to distinguish between: (i) “public peering” points on which any operator can exchange traffic and “private peering” points, where a limited number of operators interconnect; (ii) peering points that require the purchase of additional services and those that do not; (iii) peering points that require “symmetrical” conditions, meaning conditions identical for all players, and those that require “asymmetrical” conditions⁽¹⁾.

We must also note that peering generates costs in all cases: even in the case of free peering, when traffic is exchanged free of charge, operators must still pay for the delivery of traffic up to the peering point and eventually the costs related to the peering point itself (e.g., routers and data center hosting).

The development of interconnection points in France lags significantly behind Frankfurt, Amsterdam, London, and New York, which appear to be larger peering locations than Paris, even for incoming traffic on the French network.

(1) This asymmetry may put smaller players at a disadvantage, or not, some having taken advantage of the operators' interest in aggregating traffic in order to be able to peer for free with larger operators who offered attractive free peering terms to this end.

French peering suffered during a lengthy period because of acute fragmentation of public peering points.

c) Evolution

Most of the debate surrounding interconnection originates from the increase and growing asymmetry of traffic on access networks. A number of Internet access providers are asking that this development be accompanied by an evolution of the financial flows related to interconnection, which causes tensions. At the same time, the end of the Internet access market's period of rapid expansion resulted in a consolidation of the Internet market as a service distribution market, which probably reinforces this trend⁽¹⁾. Recent controversies between Netflix-Level 3-Comcast in the United States⁽²⁾ and Orange-Cogent-Megaupload⁽³⁾ in France, as well as the nonrenewal of free peering agreements between Internet access providers and CDNs⁽⁴⁾ indicate that traffic exchange negotiations are currently unstable.

2. The legal framework

Compared with legal blocking and traffic management, the legal framework that pertains to interconnection appears: (i) binding for the legislator and subject to specific European standards; (ii) potentially binding for the operators; the powers granted to regulators are relatively numerous even though regulatory requirements are currently weak.

a) Applicable law

► European and legislative standards.

At the European level, access and interconnection systems are laid down by Directive 2002/29/EC, which defines access and interconnection⁽⁵⁾ and establishes the following principles: Member States are prohibited from restricting

(1) See Olivier Bomsel, *L'économie immatérielle*, Gallimard, 2010, Paris.

(2) *Megaupload and Cogent accused Orange of degrading access to the video exchange platform offered by Megaupload, Orange retorted that the cause was poor quality of Cogent's transit service.* See Guerric Poncet, "Orange et Megaupload s'affrontent sur Internet," January 14, 2011, *LePoint.fr*.

(3) *Netflix, a highly developed video-on-demand website in the United States, and its transit provider, Level 3, accused the Internet access provider Comcast of degrading the quality of interconnection to favor its own video-on-demand distribution platform.* See Guillaume de Calignon, "USA: vive concurrence entre Netflix et Comcast," December 9, 2010, *La Correspondance de la Presse*.

(4) See <http://www.itespresso.fr/reseaux-akamai-est-il-en-froid-avec-les-fai-francais-41169.html>.

(5) See art. 1: access is "the making available of facilities and/or services, to another undertaking, under defined conditions, on either an exclusive or nonexclusive basis, for the purpose of providing electronic communications services, including when used for providing information society or broadcast services;" interconnection means "the physical and logical linking of public communications networks used by the same or a different undertaking in order to allow the users of one undertaking to communicate with users of the same or another undertaking, or to access services provided by another undertaking." Interconnection is therefore a specific type of access.

the ability to negotiate agreements for access or interconnection⁽¹⁾; operators are required to negotiate reciprocal interconnection to provide electronic communications services accessible to the public on terms and conditions consistent with the obligations imposed by the national regulatory authority⁽²⁾; national regulatory authorities have the power to impose interconnection obligations upon the various operators under procedures that are objective, transparent, proportionate, and nondiscriminatory⁽³⁾; national regulatory authorities have the power to impose specific obligations upon operators exerting a significant influence on a market⁽⁴⁾.

Access and interconnection are similarly defined in the Directive and in 8° and 9° of Article L. 32 of the Postal and Electronic Communications Code⁽⁵⁾. The principles laid down in the Directive are: the freedom to negotiate interconnection or access⁽⁶⁾; the obligation to satisfy requests for interconnection made by operators of networks open to the public⁽⁷⁾; the power granted to the ARCEP to impose equitable procedures for access and interconnection under objective, transparent, nondiscriminatory, and proportionate conditions, either upon its own initiative⁽⁸⁾ or in the context of a dispute resolution procedure⁽⁹⁾; the power granted to the ARCEP to impose specific obligations upon operators that exert a significant influence on a market⁽¹⁰⁾.

(1) See art. 3.

(2) See art. 4.

(3) See art. 5: specifically concerns the obligations to ensure end-to-end connectivity and to allow interoperability of services for operators controlling access to final users.

(4) See art. 8: specifically concerns the obligations for transparency in relation to interconnection and/or access (art. 9); non-discrimination obligations to ensure that operators apply equivalent conditions in equivalent circumstances to other undertakings providing equivalent services (art. 10); obligations for accounting separation in relation to specified activities related to interconnection and/or access (art. 11); obligations of access to, and use of, specific network facilities (art. 12); and when these measures did not ensure effective competition, from the functional separation (art. 13).

(5) Art. L. 32: “8° Access. Access is understood as any provision of means, equipment or software, or services to allow the beneficiary to provide electronic communications services.” “9° Interconnection. Interconnection is defined as the physical and logical link of networks open to the public run by the same or a different operator in order to allow users of one operator to communicate with users of the same or another operator, or to access the services provided by a another operator.”

(6) Art. L. 34-8: “Interconnection or access are subject to private agreements between the parties involved.”

(7) Art. L. 34-8: “II. Operators running networks open to the public satisfy interconnection requests made by other operators running networks open to the public, including those established in another Member State of the European Community, or another country belonging to the European Economic Area, to provide public electronic communications services.”

(8) Art. L. 34-8.

(9) We must note that in the context of its dispute resolution powers, the ARCEP defines “the equitable technical and financial conditions in which interconnection and access must be ensured” (art. L. 36-8).

(10) Art. L. 38: These obligations can include “publicizing information regarding interconnection or access [...]; providing interconnection or access services under nondiscriminatory conditions [...]; satisfying reasonable requests for access to network components or to associated means [...]; not applying excessive or eviction rates [...]; implementing separate accounting for certain activities [...].”

These rules provide little indication of the obligations required of operators in terms of interconnection, which proceed from the regulatory framework. It is therefore important to describe the regulatory framework in its broadest outlines.

► The regulatory framework.

There is no current regulatory obligation for access and interconnection that pertains to IP interconnection. Describing the obligations that pertain to other types of interconnection, specifically telephone interconnection, provides a useful point of comparison.

Two types of obligations must be distinguished: (i) the “symmetrical” obligations, meaning those that apply equally to all operators; (ii) and the “asymmetrical” obligations, imposed upon operators exerting significant influence on a market. It is important to understand that some of the telephone interconnection obligations were enacted by the ARCEP on the basis of its asymmetrical regulatory powers, but since each operator’s network was defined as a specific market, they apply in an almost identical manner.

Regarding asymmetrical regulation:

– For fixed telephony, Decision n° 2008-0896 defines the obligations that pertain to interconnection, specifically the obligations regarding call termination (prohibition on charging excessive rates for fixed alternate operators and the cost-oriented obligation of an efficient operator for France Télécom) with rate thresholds;

– For mobile telephony, the ARCEP’s Decision n° 2010-1149 applies, which specifically establishes a cost-oriented mobile call termination obligation, also including rate thresholds;

– Moreover, obligations are imposed upon operators that exert a significant influence on other markets (such as SMS termination), the wholesale market for offers to access physical infrastructures constitutive of the local wire network, and the markets for activated broadband or very-high speed broadband offers delivered at a sub-national level.

On symmetrical regulation, it should be noted that in addition to technical standards, the ARCEP enacted symmetrical obligations on the local optical fiber network on the basis of specific legislative provisions⁽¹⁾. This framework will soon be supplemented by rules that apply to the deployment of the local optical fiber network in circumstances not addressed by the ARCEP’s previous decisions.

(1) See decisions n° 2009-1106 and n° 2010-1312 rendered in application of article L. 34-8-3 of the Postal and Electronic Communications Code.

b) Possible interventions

If neutrality issues on the level of IP interconnection are established, the pending legal question is under what legal instruments should they be regulated.

► Stipulations provided in the framework of the third Telecom Package.

Regarding neutrality, interconnection appears to have been overlooked by the third Telecom Package. Therefore:

– Reinforcing transparency pertains only to traffic management, even though design has a strong impact on Internet quality;

– A new power was granted to national regulatory authorities to impose minimum quality-of-service requirements in cases of network congestion in order to address the threat of the public Internet being crushed by managed services; the design of interconnections is not specified in either the legal framework or its recitals, and nothing suggests that it could legally apply;

– Doubts were also expressed regarding the scope of the new provisions under Article 5-1 of the Access Directive;

– Finally, extending dispute resolution powers to the technical and financial terms and conditions for the delivery of traffic between an operator and another company will cover the cases of paid peering but will not affect the regulation of interconnection.

► Intervention of sectorial and competition regulators.

As already mentioned in the sections dealing with traffic management, the scope of these regulations appears uncertain, specifically because of the difficulty of identifying a market where Internet access providers hold a dominant position.

The sectorial regulator's main instrument for intervention is the dispute resolution procedure. Besides the limitations already discussed in the sections on traffic management, the ARCEP's ability to regulate the interconnection market via the dispute resolution procedure faces several challenges:

– The risk of foreign players relocating interconnection points following an unfavorable decision;

– The difficulty of determining an equitable price on two-sided markets;

– The difficulty in discriminating between players because of the heterogeneity of interconnection agreements.

It should finally be noted that legislative intervention would likely render certain provisions of the Access Directive ineffective and therefore contravene

European law. Thus, opportunities for intervention on a national level, and in the current legal framework, appear very limited.

3. Policy issues

Interconnection raises diverse regulatory issues, the question is, for example, whether rules should be established to: (i) guarantee an interconnection design that ensures high-quality Internet; (ii) prevent routing and interconnection design practices that target certain players.

However, much of the debate has to do with “data call termination.” Although uncertainties persist regarding how this system would function if implemented, it is possible to present the idea schematically by saying that under this mechanism operators that generate traffic would pay Internet access providers a sum based on the asymmetric portion of the traffic exchanged and covering the incremental costs generated.

a) The debate on data call termination

► Emergence of the debate.

The issue of data call termination emerged on a policy level only following negotiation of the third Telecom Package, which contained no measures pertaining to the evolution of sharing network-related costs. Among the existing solutions for meeting the costs associated with the increase in traffic, the CGIET’s March 2010 report considered the possibility of “*financial participation on the part of content providers.*” The Government’s report remained cautious on the issue, merely reporting the access operators’ proposal to modify the technical and financial procedures of interconnection and their request that the ARCEP place the market under surveillance. The ARCEP analyses seemed much more detailed, noting that a deep disagreement on how to cover the costs related to the Internet network had developed between Internet access providers and content providers. In their responses to the European Commission’s public consultation, several French players mentioned the evolution of financial procedures for interconnection and data call termination⁽¹⁾. For now, the French authorities have taken a cautious position, but generally appear to be ahead of other European authorities⁽²⁾.

We must finally note that: (i) this issue has not been the subject of specific attention on the part of some players⁽³⁾; (ii) other players have requested that the issue not be addressed in ongoing debates on the grounds that it has nothing to do with neutrality. However, it seems justifiable to address the issue, since: (i) it is at

(1) See the responses of Orange, Dailymotion, and the French Government to the European Commission’s consultation on Net Neutrality.

(2) See the BEREC’s response.

(3) See the response of La Quadrature du Net does not mention the subject, nor does the FCC’s 2010 Decision.

the heart of the economic debate on Net Neutrality⁽¹⁾; (ii) it is an important Internet regulation issue that impacts the other aspects of neutrality⁽²⁾.

► Key points.

With regard to the debate on data call termination, three lessons that advise caution in terms of regulation can be drawn from the aforementioned technical and legal components:

– The economic models for the Internet network’s technical intermediaries are heavily dependent on the financial flows related to interconnection;

– Access networks make up a two-sided market, where the allocation of costs on each side has an arbitrary component, and an economic optimum is difficult to determine;

– Interconnections of French networks may be located in France or abroad.

b) The players’ positions and arguments raised

Based on the players’ contributions to the various public consultations, interviews conducted by the mission, and the reactions to its first proposals, the debate can be summarized as follows:

► Arguments exchanged.

There is broad consensus on the fact that the degree of asymmetry of traffic is increasing, thus generating costs for Internet access providers. There are, however, significant differences on the following points:

– The need to assist Internet access providers in meeting these costs through regulation: according to opponents of data call termination, mobile rates and the development of managed services may be sufficient to cover costs related to increasing traffic.

– Fairness of data call termination: supporters of data call termination emphasize that (i) content providers do not pay for all of the costs generated by their traffic; (ii) data call termination could protect the consumer from higher

(1) See Nicholas Economides and Joacim Tag, 2007, “Net Neutrality on the Internet: A Two-sided Market Analysis” Working Papers 07-27, New York University, Leonard N. Stern School of Business, Department of Economics; Robin Lee and Tim Wu, “Subsidizing Creativity through Network Design: Zero-Pricing and Net Neutrality,” *Journal of Economic Perspectives*, 2009; Jacques Crémer, “La neutralité des réseaux,” *Les Echos*, November 3, 2010.

(2) When referring to Robin Lee and Tim Wu’s article mentioned above, Nicolas Curien and Winston Maxwell write in *La neutralité d’internet, La découverte*, 2011 (p. 40), that “Economic theory knows [...] how to provide a response [to the issue of prioritization of certain contents] that preserves, or nearly preserves, neutrality: Internet access providers continue to apply the general rule of free access to the various content providers for all Internet users, with a guaranteed minimum quality of service, while also offering premium access services.”

package rates based on the increase in traffic; (iii) transparency would also reduce the risk of discrimination between small content providers, major content providers, and subsidiary content providers owned by Internet access providers. Opponents of data call termination argue in response that (i) content providers already pay large sums for their traffic flow, and; (ii) the traffic they inject into the network is done so at the consumer's request.

– Economic efficiency of data call termination: supporters of data call termination argue that implementation of this system would send price signals to economic agents encouraging them to save bandwidth. Opponents of call termination data respond, (i) that such an incentive already exists, since content providers pay for their traffic flow and, (ii) economic theory tends to suggest that content providers should not pay for Internet access.

► The players' positions.

Overall, Internet access providers usually support the measure, while emphasizing that a competitive solution must first be sought. Consumer groups and Internet users are also usually in favor, especially since the system would allow for transparency. Content providers and transit operators are opposed for the reasons already stated and because it would disrupt their business model.

c) The mission's analysis

The mission's analysis can be summarized in three points:

– Today, consumers are actually paying a larger portion of the costs related to the Internet network than content providers, which corresponds to the tenets of economic theory;

– The arguments in favor of data call termination seem compelling, especially since its implementation would allow for a better understanding of who pays what, clearly identify costs, and end discriminatory and unfavorable interconnection rates for small players who do not exert market power;

– However, uncertainties remain, specifically regarding the impact implementation of data call termination would have on the players' business models.

In any event, implementation of this system is not possible in France for both technical and legal reasons. The mission therefore recommends that the European Commission analyze this solution in detail. Regardless of the conclusions, such investigations would have the benefit of clarifying how the wholesale interconnection market functions.

III. — THE MISSION’S PROPOSALS

Principle behind the proposals

The principle behind the fact-finding mission’s proposals is protection of the Internet, while still allowing for the development of future networks and the defense of consumer interests. The purpose is therefore to ensure the tremendous societal advances in communication, freedom of expression, innovation, and economic growth through an economic, technical, and regulatory context favorable to the digital ecosystem.

These guidelines suggest that in the context of digital convergence and the mutualization of electronic communications networks, which are different “layers” of the same infrastructure, we must ensure that a quality Internet layer is maintained. The question that arises is how to provide this guarantee.

The answer proposed by the fact-finding mission is expounded in three stages. First, to guarantee freedom of expression: the Internet is a revolutionary communications tool and this aspect of it must be protected, specifically by the limitation and regulation of filtering and blocking techniques, which threaten the freedom of expression and communication. Second, guarantee innovation: the Internet is a network that has so far adequately conveyed all contents and services, which accounts for its success and should therefore be maintained. Third, guarantee funding: at the applications and network level, the Internet is not gratuitous, and each category of player will continue to innovate only if the economic model remains viable, specifically with regard to increasing volumes of traffic.

The fact-finding mission made proposals for providing these guarantees. Several elements must, however, impel the legislator to intervene cautiously: (i) the general mission assigned to law by article 34 of the Constitution is to set the rules but not the details of the regulation; (ii) the regulation of electronic communications successfully implemented by the ARCEP is very detailed and the precise regulation of Net Neutrality must find its place in this regulatory framework; (iii) the problems raised by neutrality are highly complex and evolve quickly, like the network itself. Therefore the normative scope of the fact-finding mission’s proposals is variable: some may result in legislation with a direct effect (e.g., systematic judicial intervention for ordering mandatory blocking measures, or the exclusive use of the Internet trade name for access offers that respect the principle of neutrality), but the key is to properly define the regulator’s (the ARCEP’s) framework for intervening to protect Net Neutrality. The fact that the legislator relies on the regulator does not mean that the legislator will discharge its responsibility or is content by enacting “soft” laws.

The mission's proposals comprise a pragmatic solution to concrete neutrality issues and reach beyond a simple statement of principles. The proposed regulatory framework may seem sophisticated, but it proceeds from the complexity of issues surrounding the evolution of Internet network usages.

Summary of the proposals

The objective of the first proposal strategy is to protect the Internet by explicitly including it in the perimeter of electronic communications regulation. The current risk is the rise of non-neutral practices that would reduce Internet users' ability to choose how to use their network. To counter this risk, we recommend giving the principal of Net Neutrality legal scope by generally defining its promotion as an objective for regulatory authorities (the purpose of the first proposal strategy) and, more specifically, providing guarantees on the points that give the greatest cause for concern (the purpose of the proposal strategies that follow). Proposal n°1 defines Net Neutrality under the Law, and proposal n°2 defines its promotion as an objective for regulatory authorities.

The objective of the second proposal strategy is to avoid, as far as possible, requiring operators to block electronic communications, since blocking has both direct (restricting the freedom of expression and communication) and indirect (over blocking, encouraging encryption, etc.) negative effects, which are not always correctly taken into consideration in legislative decisions. Furthermore, fragmentation of the legislative framework (the 2004 LCEN [Law on Confidence in the Digital Economy], the 2010 Law on Online Gaming and Betting, the Code of Intellectual Property) is a source of confusion. This is why we recommend further inquiry into the justifications for legal blocking measures, despite their apparent legitimacy, because of their inefficiency and unintended negative consequences (proposal n°3), and immediately provide for systematic judicial intervention to rule on the required blocking measures to better protect freedom of expression (proposal n°4).

The objective of the third proposal strategy is to preserve the Internet as the open platform it is today. There is the risk of a rapid deterioration in the quality of the public Internet due to a substantial increase in flows should Internet access providers fail to invest in networks or if they privilege the marketing of managed services. Safeguarding consumer choice seems to be the first solution in meeting this risk: in the absence of market shortcomings, ensuring the transparency of Internet access by reserving the Internet trade name for neutral accesses only would seem sufficient for protecting this choice (proposal n°5), along with creating an Internet quality watchdog (proposal n°6); in the event that competition no longer permits consumers to choose a quality, neutral Internet access at a reasonable cost, maintaining the consumer's ability to choose must be restored through more restrictive means, by imposing requirements that guarantee Internet quality on Internet access providers (proposal n°7).

The objective of the fourth proposal strategy is to carefully achieve an economic balance between the different categories of Internet players, so that the Internet ecosystem can continue to develop and innovate, while also guaranteeing the coverage of network investments to maintain a quality Internet. The increase of asymmetrical Internet traffic, combined with caps on consumer prices, and the arbitrary nature of financial flows on two-sided markets, create the risk of a significant uncertainty in the evolution of economic relations between the various categories of players and the viability of their economic models. Since Internet access providers are required to provide a sufficient level of quality, we must ensure that their economic model allows them to do so. According to the information collected by the mission, establishing “data call termination,” which would allow the network’s variable costs to be covered, could be a good solution. We must continue to study this point since the markets related to the Internet network are still not well understood (proposal n°8). and the appropriateness of implementing such a solution must be evaluated in depth (proposal n°9).

List of proposals

► First strategy: enshrine Net Neutrality as a policy objective

Proposal n°1: Define the principle of neutrality

Proposal n°2: Establish neutrality as a policy objective and grant regulatory authorities the power to impose obligations for promoting Net Neutrality

► Second strategy: Strictly regulate Internet blocking obligations

Proposal n°3: Further investigate the justifications for legal blocking measures, despite their apparent legitimacy, due to their inefficiency and potentially negative consequences

Proposal n° 4: Immediately establish a single procedure for judicial intervention

► Third strategy: Protect universality and guarantee Internet quality

Proposal n°5: Reserve the “Internet” trade name solely for offers that respect the principle of neutrality

Proposal n°6: Create an Internet quality watchdog

Proposal n°7: Request the ARCEP to guarantee access to an Internet of sufficient quality

► Fourth strategy: Ensure viable financing of the Internet

Proposal n°8: Document the economic issues related to the Internet network

Proposal n°9: In-depth evaluation of data call termination at the European level

► **FIRST STRATEGY: ENSHRINE NET NEUTRALITY AS A POLICY OBJECTIVE**

The objective of the first proposal strategy is to protect the Internet by explicitly including it in the perimeter of electronic communications regulation. The current risk is the rise of non-neutral practices that would reduce Internet users' ability to choose how to use their network. To counter this risk, we recommend giving the principle of Net Neutrality legal scope by generally defining its promotion as an objective for regulatory authorities (the purpose of the first proposal strategy) and, more specifically, providing guarantees on the points that give the greatest cause for concern (the purpose of the proposal strategies that follow). Proposal n°1 defines Net Neutrality under the Law, and proposal n°2 defines its promotion as an objective for regulatory authorities.

Proposal n°1: Define the principle of neutrality

The principle of neutrality should be defined in the law as:

- (i) Internet users' ability
- (ii) to send and receive the content of their choice, to use services or run applications of their choice, connect the equipment and use the programs of their choice provided they don't impair the network,
- (iii) with a transparent, sufficient, and non-discriminatory quality of service,
- (iv) and subject to the obligations resulting from legal proceedings and the measures required for security reasons and unforeseen congestion.

Position: these provisions could be inserted in article L. 32-1 of the Postal and Electronic Communications Code (creation of a IV).

Arguments:

Send a clear policy signal

The legislator must send a clear message to public and private players that it is committed to protecting the Internet—enshrining the principle of neutrality into law is a good method for doing so. The purpose is to send a policy signal to:

- Economic players, to encourage them to organize themselves upstream from the regulation protecting the Internet;
- Regulatory authorities, to encourage them to monitor the evolution of Internet practices;
- Citizens, to assure them that public action seeks to protect their rights.

Response to the shortcomings of applicable legislation, current and future

In the writings the Government intends to adopt via ordinance in the context of the transposition of the third Telecom Package, article L. 32-1 of the Postal and Electronic Communications Code will define the regulatory authorities' objectives pertaining to neutrality as follows: to ensure competition for the transmission of content for the benefit of the consumer (2°), non-discrimination, under analogous circumstances, in relations between operators and public online communications service providers for traffic delivery and access to these services (4° bis A), favor the final users' access to information and preserve their ability to disseminate information as well as to use the applications and services of their choice (15°).

These provisions respond to some of the concerns related to Net Neutrality, but not all of them, namely: regulation of the mandatory filtering measures (see the discussions on article 4 of the 2011 LOPPSI II), discrimination between market and non-market flows (see the reported degradation of peer-to-peer during peak hours), disputes around interconnection (see the Megaupload-Cogent-Orange case in early 2011), and the guarantee of an Internet of sufficient quality, which could suffer from the development of managed services. It is therefore proposed that neutrality be defined in all of its aspects (proposal n°1), and that its promotion be an objective of regulatory authorities (proposal n°2).

Defining the principle of neutrality would also have the advantage, with regard to current legislation, of providing consistency in the decisions rendered by regulatory authorities by giving them a single legislative base.

Begin with a good definition

Note that the fact-finding mission's initial guidelines recommend defining the principle of neutrality "*from the objectives already set out, such as the absence of filtering—excluding technical or mandatory measures ordered by a judge—guarantee a sufficient quality of service, the absence of targeted degradation measures in quality of service, provide nondiscriminatory access to the various levels of quality of service, and guarantee fair technical and financial terms and conditions for interconnection*" (§ 23). Following the players' observations on this proposal, the choice was made to use a definition that enumerates the features that should be offered to Internet users to emphasize the importance of freedom of choice when using the connection. This definition seems likely to gain consensus.

The rest of the argumentation justifies each component of the definition used.

(i) The proposed definitions indicate that there are two approaches for defining neutrality. The definitions proposed by the ARCEP and the FCC ("*To encourage broadband deployment and preserve and promote an open and interconnected public Internet, are entitled to: 1. access to lawful Internet content*

of their choice; 2. to run applications and use the services of their choice, subject to the needs of law enforcement; 3. connect their choice of legal of devices that do not harm the network; 4. to competition among network providers, application and service providers, and content providers.”) focus on the final consumer. The definition proposed by Tim Wu is focused on the delivery of electronic communications (“*Network neutrality is best defined as a network design principle. The idea is that a maximally useful public information network aspires to treat all content, sites, and platforms equally.*”). Each of these approaches has its merits: the first approach because it focuses on what matters in the end, the features offered by the network to users that also allow operators to do their job; that is to say, choose their network architecture and traffic management; the second approach because it focuses on traffic delivery thus emphasizing fair treatment of the various players on the network, whether the final consumer or the economic players, who are not directly covered by the first approach. In order to integrate these two approaches, we recommend defining neutrality based on the features the network offers to all “Internet users,” not only final consumers or users.

(ii) The list of features established to this point has gained broad consensus both in the United States, when it was proposed by the FCC, and in France, when it was put forward by the ARCEP, and requires no particular justification. The general idea is to ensure that users can freely determine use of their connection.

(iii) Reference to a “transparent” quality of service does not pose any difficulties. However, reference to a “sufficient” and “non-discriminatory” quality of service is likely to raise objections and elicits the following comments:

– Reference to a “sufficient” quality is justified by the consensus around the goal of a quality Internet, its relation with the concept of neutrality, and its legal effects. “Sufficient” quality is also included in the definition of neutrality proposed by the ARCEP in its initial guidelines. It should be noted that it is independent of proposal n° 8, which seeks to ensure sufficient Internet quality and does not constitute a significant legal innovation since, pursuant to Article 22 of the Universal Service Directive, which will be transposed to a new Article, L. 36-15 of the Postal and Electronic Communications Code, the ARCEP will soon be granted the power to impose “minimum requirements” in terms of quality of service upon operators to avoid network congestion. This specification, at the level of the definition of neutrality, therefore has the essential effect of clarifying the goals assigned to the ARCEP.

– Reference to a “non-discriminatory” quality of service is, for its part, justified by the fact that the absence of discrimination is a fundamental component of neutrality. As expressed in the definition provided by Tim Wu, neutrality refers to the idea of the absence of discrimination between flows. In its initial guidelines, the fact-finding mission noted that the concept of nondiscrimination can be interpreted in various ways, including as a homogeneous treatment of flows, as a differentiation in how flows are processed according to the objective needs of the

uses they support, or as nondiscriminatory access to various levels of quality of service. The mission specifies that the concept of nondiscrimination is used here in the sense of homogeneous delivery of flows.

(iv) In the context of blocking obligations, and outside legal requirements, traffic management is necessitated by law, to ensure network security—there is a consensus on this point. We must therefore provide for exceptions to the conditions set forth above, including those having to do with nondiscrimination and access to all contents, services, and applications. The difficulty is in determining which exceptions are legitimate and which are not. It seems justified that the only traffic management measures compatible with neutrality, other than those arising from the law or for security needs, are those taken in cases of unforeseen congestion. In effect, the network would not be neutral if, for example, peer-to-peer were degraded during peak hours. Such a practice is undesirable as using this protocol may hamper innovation.

Proposal n°2: Establish neutrality as a policy objective and give regulatory authorities the power to impose obligations for promoting Net Neutrality

The national regulatory authorities should have the objective of promoting Net Neutrality, as defined in proposal n°1.

To pursue this objective, operators of networks open to the public and electronic communications service providers should be subject to the rules governing the promotion of Net Neutrality.

Position: these provisions could be introduced respectively in II of article L. 32-1 and in I of article L. 33-1 of the Postal and Electronic Communications Code.

Arguments:

Ensure that the regulatory authorities fully consider the Internet

The work accomplished by the fact-finding mission established that the Internet's functioning was still largely unknown to the government, since regulation of electronic communications initially focused on telephony and physical infrastructures, including the local network. However, most communication services currently converge on the Internet, and the debate on neutrality can be understood as the policy awareness of this evolution. Thus, it is important that governments, including regulatory authorities, extend their "regulatory perspective" to the Internet to better understand how it operates, measure the effect of standard regulatory decisions on it, and protect its functioning, if necessary. Defining the principle of neutrality as a goal for regulatory authorities will guide regulatory decisions.

Give an adequate normative scope to the principle of neutrality

By defining promotion of the principle of Net Neutrality as an objective for both the Minister in charge of electronic communications and the ARCEP, and by granting the possibility of subjecting operators to obligations to respect the principle, the content of proposal n°2 responds to two points:

– First point: Net Neutrality must be protected to ensure global access to the open exchange platform that constitutes the Internet, and the free choice of each person to do what he wishes with his connection. The pursuit of this goal should not obscure the fact that: (i) useful innovations may occur in the future, not only at the end points of electronic communications networks but also at the heart of these networks; (ii) pursuant to the principle of technological neutrality, it is not up to the legislator or the regulator to define how operators should manage their networks or which architecture they must choose. Operators must, in particular, maintain the possibility of developing managed services alongside the Internet. Transparency vis-à-vis the consumer warrants that those services which are freely managed by operators be clearly distinguished from the neutral Internet. Therefore, the scope of the principle of neutrality should be limited to the Internet. (see proposal n° 5).

– Second point: the emergence of neutrality issues, the complexity of technical issues, and uncertainties affecting the development of the Internet network justify defining clear objectives and provide regulatory authorities with sufficient legal means to pursue them, but not enacting detailed regulation.

Two clarifications can be provided on the legal scope of the obligations that could be imposed upon operators in application of the aforementioned proposal n°2:

– The general framework defined in article L. 32-1 requires regulatory authorities to “*take reasonable measures proportionate with the objectives sought, under terms and conditions that are objective and transparent.*”

– If the ARCEP enacted such obligations, operators disregarding them could be sanctioned in the framework of the ARCEP’s general sanctioning powers under article 36-11.

► SECOND STRATEGY: STRICTLY REGULATE INTERNET BLOCKING OBLIGATIONS

The objective of the second proposal strategy is to avoid, as far as possible, requiring operators to block electronic communications, since blocking has both direct (restricting the freedom of expression and communication) and indirect (over blocking, encouraging encryption, etc.) negative effects, which are not always correctly taken into consideration in legislative decisions. Furthermore, fragmentation of the legislative framework (the 2004 LCEN, the 2010 Law on

Online Gaming and Betting, the Code of Intellectual Property) is a source of confusion. This is why we recommend further inquiry into the justifications for legal blocking measures, despite their apparent legitimacy, because of their inefficiency and unintended negative consequences (proposal n°3), and immediately provide for systematic judicial intervention to rule on the required blocking measures to better protect freedom of expression (proposal n°4).

Proposal n°3: Further investigate the justifications for legal blocking measures, despite apparent legitimacy, due to their inefficiency and potentially negative consequences

The competent authorities should work together to evaluate the appropriateness of blocking, specifically from an operational standpoint.
--

Position: no proposal of codified legislative provisions.

Arguments:

Remember that general law applies to the Internet

When one considers all the costs, risks, and benefits, it is not incontrovertible that one should prevent the communication of all “unlawful content.” In this regard, the following analogy may help elucidate the question. Using a mobile phone while driving is dangerous and constitutes an “illegal” communication that the police sanction when it is established and that is subject to preventive measures in the context of road safety. Does this, however, warrant implementation of a complex and costly system for blocking communications while driving by geolocating calls and systematically analyzing the voice signal to identify those calls made while driving, with the ability to block them?

It should also be noted that no blocking of “unlawful content” does not mean the absence of sanctions. Thus, the unauthorized exchange of files subject to copyright is, in application of Article L. 335-3 of the Intellectual Property Code, a counterfeiting offense. In its decision on the 2006 DAVDSI Law, the Constitutional Council also censured the provisions that would reduce penal sanctions for unauthorized sharing of files subject to copyright on the Internet on the grounds that “*the characteristics of peer-to-peer exchange networks do not justify the difference in treatment established by the contested stipulation*”: this emphasizes that general law must apply to the Internet.

Weigh the technical aspects

The importance of freedom of expression and communication, emphasized in support of proposal n°4, obviously invites the legislator to limit the scenarios in which mandatory blocking measures could be imposed in situations where freedom of expression and communication challenge a fundamental right or a

constitutional objective against which these freedoms constitutes a serious threat. Achieving this balance should be the first step in the legislator's rationale.

But the rationale regarding values is not sufficient. The legislator should subsequently evaluate whether, in practical terms, the benefits from implementing mandatory filtering measures are inferior to the risks incurred, and, if they are, refrain from introducing new legal bases that give judges the power to impose mandatory blocking measures. It is important to take the time to weigh the issues, since there are, on a practical level, forcible arguments against implementing blocking measures:

– The techniques for circumventing filtering measures are relatively accessible. In cases where blocking targets the exchange of truly abhorrent content, such as child pornography, the government faces criminal organizations that are savvy in their use of the Internet and will succeed in eluding these measures. Simply blocking a website is difficult;

– To the partial inefficiency of blocking measures is added the risk of “over efficiency,” as available techniques generate over blocking (blocking content, services, or applications other than those targeted), and threaten network resilience;

– Finally, there is an overall risk associated with the development of techniques to circumvent blocking measures. When blocking measures target “general public” exchanges, such as online games, they can act as a deterrent in the short term. In the long term, however, one must not underestimate Internet users' ability to develop bypassing techniques on a large scale (for example, modules for encryption or for accessing proxies installed directly on Web browsers). Such a development would threaten network security and, moreover, create a serious problem in relations between the virtual world of the Internet and the government. It also raises cyber security concerns.

Precisely identify the effects of blocking

These issues, and caution, justify at minimum a moratorium on blocking—no new cases of filtering should be added to existing cases—and judicial intervention in all cases pursuant to proposal n° 4. They should also motivate further investigation: the relevant public authorities should seriously evaluate the robustness of such measures. On this basis, the conditions under which blocking measures must be implemented should be reexamined, and the legislator could therefore choose between three possible options—extend blocking, maintain the current law, abandon all blocking measures—in a fully informed manner.

Encourage the development of “parental control”- type filtering software

Resorting to filtering systems at network end points can be justified, specifically in the context of parental control. The user must fully control, activate, and parameter these systems.

Proposal n°4: Immediately establish a single procedure for judicial intervention

Internet access providers should be required to block electronic communications only following a single procedure, except for reasons of security, which allows judicial authority to order that access to a content, service, or application be blocked.

Position: these provisions could be included in the Postal and Electronic Communications Code or in another code.

Arguments:

Protecting freedom of expression and communication

The legislator has latitude to determine how to ensure the balance between freedom of expression and communication and the protection of other interests—be it the fight against child pornography or cyber crime, protection of the State’s proprietary interests or of copyright. Several points can be emphasized in this regard:

- European Law requires that Internet access restrictions be subject to “adequate procedural safeguards” (article 1 of Directive 2009/140);
- The Constitutional Council does not admit that a measure suspending Internet access could be ordered by the administrative authority (decision on the HADOPI Law), except in the case of child pornography, where the administrative authority may order Internet access providers to block access to such content; the blocking decision can also be contested before a jurisdiction (decision on the LOPPSI Law);
- These European and constitutional rules give the Law significant latitude, in application of article 34 of the Constitution, under which the rules regarding civic rights and the fundamental guarantees granted to citizens for the exercise of their liberties will be determined.

The eminent political and social importance attached to free communication of thought and opinion justifies its priority for the legislator to achieve a balance between these rights and other legitimate policy interests. It must be clearly stated, however, that it is preferable for people to communicate, even if such communication is damaging, until a judge decides otherwise. The risk of abuses related to the administration establishing a list of services, content, or sites to be

blocked—specifically regarding their advertising and update—is an additional and pragmatic argument in favor of a procedure for systematic judicial intervention, rather than an administrative blocking decision, which can then be contested before a judge.

A unified legal framework

The proliferation in the last few years of laws for imposing mandatory blocking measures (2004 Law on the Confidence in the Digital Economy, 2009 Law on Online Gaming and Betting, 2011 LOPPSI II Law) demonstrates an increasing pressure to restrict freedom of communication on the Internet. Establishing a single procedure would ensure the consistency of legislative decisions and “consolidate” the debates on blocking by clearly including them in a code.

Rationalize the legal procedure

Establishing a single procedure would also have the advantage of giving a single judge—for example, the Tribunal de Grande Instance of Paris, in the same manner as the 2010 Law on Online Gaming and Betting—the role of ruling on mandatory blocking measures, thus allowing an accretion in competence and better monitoring of the jurisprudence.

► THIRD STRATEGY: PROTECT UNIVERSALITY AND GUARANTEE INTERNET QUALITY

The objective of the third proposal strategy is to preserve the Internet as the open platform it is today. There is the risk of a rapid deterioration in the quality of the public Internet due to a substantial increase in flows should Internet access providers fail to invest in networks or if they privilege the marketing of managed services. Safeguarding consumer choice seems to be the first solution in meeting this risk: in the absence of market shortcomings, ensuring the transparency of Internet access by reserving the Internet trade name for neutral accesses only would seem sufficient for protecting this choice (proposal n°5), along with creating an Internet quality watchdog (proposal n°6); in the event that competition no longer permits consumers to choose a quality, neutral Internet access at a reasonable cost, maintaining the consumer’s ability to choose must be restored through more restrictive means, by imposing requirements that guarantee Internet quality on Internet access providers (proposal n°7).

Proposal n°5: Reserve the “Internet” trade name solely for offers that respect the principle of neutrality

Internet access providers should be authorized to market under the Internet access name only those electronic communications services that respect the principle of neutrality as defined in proposal n°1.
--

Position: these provisions could be introduced in the “electronic communications agreements” section of the Consumer Code.

Arguments:

Increase transparency with a simple equation: Internet = neutrality

The third Telecom Package includes provisions that strengthen transparency vis-à-vis consumers. The transposition ordinance provides that new clauses will necessarily be included in electronic communications service agreements in a clear, comprehensive, and easily accessible manner, specifically, the traffic management procedures implemented, access restrictions to certain services or equipment, measures to safeguard the network’s security and integrity (amended Article L. 121-83 of the Consumer Code). Although these provisions are constructive, they do not necessarily guarantee consumers the ability to easily compare the various offers and gain access to a quality Internet. Proposals n° 6 and n° 7 are therefore proposed to allay these shortcomings.

The first way to clarify the choices available to consumers is to introduce requirements ensuring that the Internet access services provided to subscribers correspond to their expectations. When a consumer subscribes to an Internet access service, access to the entire Internet, without discrimination and with a sufficient level of quality, is expected. These expectations are well summarized in the definition of neutrality set out in proposal n°1. It is therefore proposed that the “Internet” trade name be reserved solely for offers that respect the principle of neutrality.

Encourage Internet access providers to offer the best possible Internet access

A second argument motivating this proposal is to find a way to encourage Internet service providers to offer the best possible Internet access at a reasonable cost, while adhering to the principle of neutrality. The Internet ecosystem is based on a great number of users accessing any content, application, or service posted online by other users, which implies having true Internet access. The term “Internet” has an undeniable commercial appeal and reserving the use of this term for neutral access appears to be an effective incentive.

Proposal n°6: Create an Internet quality watchdog

The ARCEP should create an Internet quality watchdog to measure the quality of Internet access services provided by the various operators, and to better understand the effects of the operators’ practices on Internet quality, specifically in terms of routing, interconnection, and traffic management.

Position: no proposal for codified legislative provisions.

Arguments:

Allow the consumer to choose between Internet access offers based on quality

Reserving the “Internet” trade name solely for offers that respect the principle of neutrality is a primary means for ensuring the “actual” transparency of consumer offers, as illustrated by the arguments presented in support of proposal n°6. Implementing public measures for a quality Internet, in the manner of existing public measures for the quality of the fixed or mobile telephone under the ARCEP’s authority, is a second method. The necessity of this measure is all the greater since the quality of Internet access services is more heterogeneous than that of telephone services and is dependent on a multiplicity of factors. Quality must consequently be measured from several perspectives, and is therefore less likely to be directly evaluated by consumers.

Develop existing measurement tools

There is currently no public measure of Internet quality offered by Internet access providers, nor any agreement as to what precisely should be measured. However, several techniques are available to measure the quality of traffic delivery, some that focus on equipment and network performance; others that focus on users and the end result of the data exchange; and, finally, objective quality standards implemented on a service-by-service basis. Considering what is at stake, it is critical to ensure the development of objective tools to measure quality of service.

Involve the ARCEP in monitoring operators’ practices

Establishing an Internet quality watchdog would also ensure that the ARCEP continuously monitors the practices of Internet operators, specifically their routing policy, interconnections, and traffic management. Such monitoring would allow the ARCEP not only to assess the impact of these practices on quality of service, but also to be better prepared for resolving disputes that may arise on Internet related markets.

Proposal n°7: Request the ARCEP to guarantee access to an Internet of sufficient quality

Should competition not provide a quality Internet, the ARCEP should use its power to enact minimum quality-of-service requirements to guarantee that consumers have the ability to choose an Internet access offer that respects the principle of neutrality, as defined in proposal n°1, at a reasonable price. The ARCEP should also define *ex ante* the characteristics of a sufficient quality Internet access.

Position: these provisions could be introduced in article L. 36-15 of the Postal and Electronic Communications Code to be created by the transposition ordinance of the third Telecom Package.

Arguments:

Intervene in cases of market shortcomings

There is some consensus around the idea that transparency obligations are sufficient with regard to Internet quality as long as competition functions properly; that is to say, at least one operator offering good-quality Internet access at a reasonable price. Binding measures seem justifiable only if there is no functional competition.

The ARCEP's competence

To avoid network congestion, the third Telecom Package includes provisions for minimum quality of service imposable on operators by the national regulatory authorities. This provision will be introduced in Article L. 36-15 of the Postal and Electronic Communications Code via a transposition ordinance, and grants the ARCEP a simple faculty, which can be exercised at the authority's discretion. The previous argument, and the concern that the ARCEP may hesitate to intervene, both justify this proposal, which is designed to call upon the ARCEP's competence in cases of market shortcomings. The ARCEP should also define *ex ante* what a sufficient quality of Internet access entails.

► FOURTH STRATEGY: ENSURE VIABLE FINANCING OF THE INTERNET

The objective of the fourth proposal strategy is to carefully achieve an economic balance between the different categories of Internet players, so that the Internet ecosystem can continue to develop and innovate, while also guaranteeing the coverage of network investments to maintain a quality Internet. The increase of asymmetrical Internet traffic, combined with caps on consumer prices, and the arbitrary nature of financial flows on two-sided markets, create the risk of a significant uncertainty in the evolution of economic relations between the various categories of players and the viability of their economic models. Since Internet access providers are required to provide a sufficient level of quality, we must ensure that their economic model allows them to do so. According to the information collected by the mission, establishing “data call termination,” which would allow the network's variable costs to be covered, could be a good solution. We must continue to study this point since the markets related to the Internet network are still not well understood (proposal n°8) and the appropriateness of implementing such a solution must be evaluated in depth (proposal n°9).

Proposal n°8: Document the economic issues related to the Internet network

The national regulatory authorities and the European Commission should conduct in-depth investigations into Internet-related markets and managed services, financial flows between the various categories of players, and the evolution of their business models.

Position: no proposal of codified legislative provisions.

Arguments:

Rely on objective data

The available data does not establish a precise diagnosis of the costs related to the Internet network and managed services, the sharing of added value, or the accurate financial flows between players. The available economic literature is essentially theoretical, and when theory is no longer applied, no figures are provided. The studies dedicated specifically to neutrality that are essentially legal do not resolve these questions, despite the sophistication of the rationale presented. The purely economic aspects of the available reports were implemented by consulting firms funded by Internet players and contain very few figures. The public authorities' reports on neutrality also provide little economic data and do not allow these economic issues to be objectified. The information collected by the fact-finding mission is only the first step toward what should be a much more detailed work conducted by bodies with the appropriate means at their disposal, such as the ARCEP, the Government, or the European Commission.

Develop a “panoramic” knowledge of the markets

The difficulty in clearly presenting the economic issues related to the Internet network is perhaps due to the market's fragmentation, as it is divided into several intermediation segments in which each player sees only one or two endpoints (hosting, CDN, transit, access, etc.). Given this fragmentation, it is essential to elaborate a comprehensive economic vision of the Internet network.

Demonstrate the necessary caution to avoid disrupting economic models

Finally, data collection on the economy of the Internet network is fundamental, since the debate on neutrality arose out of concerns related to the increase in Internet traffic—specifically the explosion of video flows—the costs generated, and the reaction of Internet access providers. These costs should therefore be fully clarified. More generally, it is essential to have a sufficiently accurate representation of how Internet-related markets function in order to render cautious regulatory decisions that do not destabilize the economic models of the various categories of players.

Proposal n°9: In-depth evaluation of data call termination at the European level

The European Commission should conduct an in-depth analysis on the effects implementation of data call termination would have at the European level.
--

Position: no proposal of codified legislative provisions.

Arguments:

Be at the right level

It is possible to present the idea of data call termination schematically by characterizing it as a mechanism where operators generating traffic pay Internet access providers a sum based on the asymmetrical portion of the traffic exchanged to cover the incremental costs incurred. There are two reasons why the effects of this system should be analyzed at the European level:

– Establishing data call termination only in France seems inappropriate; in effect, players with no interest in submitting to data call termination could easily relocate their interconnection points to circumvent it with a minimum loss of quality if they interconnect elsewhere in Europe;

– It is unlikely that a decision rendered by the ARCEP or the legislator directly implementing this regulation would be compatible with European Law.

Consider the substantial arguments in favor of “data call termination”

Implementation of data call termination would:

– Stabilize the sharing of network costs—which have an arbitrary component on a two-sided market—between final consumers and players generating traffic;

– Provide clarity on the market to improve predictability for the players and enhance the government’s ability to identify discrimination;

– Send a price signal that encourages the best practices, for example for encoding or routing, and reduces unnecessary investments;

– Favor small content providers that cannot currently use market power to negotiate bandwidth.

Precisely evaluate the impact of implementing “data call termination” on the economic models of the various categories of players

However, significant uncertainties remain with regard to:

– What rate would allow the incremental costs assumed by Internet access providers due to an increase in traffic to be covered;

– Data call termination's consequent impact on transit providers and content providers.

Encourage the European Commission to conduct an in-depth analysis on the subject

The European Commission should analyze in depth the appropriateness of implementing data call termination at the European level. This analysis should also elucidate interconnection practices, an urgent need in the current environment. The intensification of interconnection disputes in recent months (e.g., Netflix-Level3-Comcast or Megaupload-Cogent-Orange) indicates that this issue is one of the most controversial surrounding neutrality. France should support these investigations at the European level.