CNCDH
COMMISSION NATIONALE CONSULTATIVE DES DROITS DE L'HOMME
RÉPUBLIQUE FRANÇAISE

Opinion on the fight against online hate speech

(Plenary meeting of 12 February 2015 - Unanimously adopted)

1. In 2004, the CNCDH devoted a significant chapter of its annual report to the fight against racism, anti-Semitism and xenophobia and to dealing with such matters on the Internet[1], placing particular importance on combating hate speech in order to maintain social cohesion and civil peace. Ten years later, the proliferation of hateful content on the web, which is regularly fuelled by social tension and the crisis of citizenship[2], is becoming a matter of great concern, representing a source of growing conflict between groups and communities challenging the democratic notion of 'peaceful coexistence'. Hate speech is not just speech; it can, in fact, trigger violence, in some cases very extreme, as demonstrated by the terrorist crimes committed on 7 and 9 January 2015 in Paris, which were themselves inspired by the death and hate propaganda widely present on the web.

2. This proliferation raises the issues of the effectiveness of the policies and measures implemented and, in more general terms, the effectiveness of existing legal systems, and of weapons designed to repress such activity in particular. As far as the CNCDH is concerned, this worrying situation requires a new assessment of the situation to be carried out as a matter of urgency with a view to outlining new strategies for fighting these issues[3]. With this in mind, a working group was set up in September 2014. It has since held a number of hearings[4], some of which immediately highlighted the inappropriate and above all incomplete nature of reflection focusing primarily on 'fighting racist, anti-Semitic and xenophobic speech on the Internet'[5]. It is for this reason that the CNCDH believes it preferable to use

[1] CNCDH, *Rapport 2004. La lutte contre le racisme et la xénophobie. Le racisme et l'antisémitisme sur internet,* La Documentation Française 2005, p.239 *et seq*. See CNCDH 14 November 1996, *Avis portant sur le réseau Internet et les Droits de l'Homme,* online at: www.cncdh.fr.

[2] See Falque-Pierrotin, I., *Rapport au Premier Ministre. Lutter contre le racisme sur internet*, Paris 2010; Knobel, M., *L'internet de la haine. Racistes, antisémites, néonazis, intégristes, islamistes, terroristes et homophobes à l'assaut du web,* Berg International Editeurs, 2012.

[3] It should be borne in mind that the ECRI strongly recommended that the French authorities continue and reinforce their efforts to fight any form of racist expression posted on the Internet. The CERD (United Nations) also dealt with the issue in its General Recommendation n°35 of August 2013 on the fight against racial hate speech (see CNCDH, *Rapport 2012-2014 sur les droits de l'homme en France. Regards portés par les instances internationales,* La Documentation Française 2014, p.223 and p.225).

[4] See the attached list of people heard.

[5] Mbongo, P., *Audition du 23 octobre 2014*; Dreyer, E., *Audition du 23 octobre 2014.*

the expression 'hate speech', even though there is no universally accepted definition of the concept[6]. This should be perceived as a generic notion that encompasses all forms of expression that are objectively considered to be offensive and to encourage disregard and even hostility or violence towards ethnic groups, religious groups, women and indeed minorities in general (be they based on gender, sexual orientation, etc.)[7]. This includes condoning acts of terrorism, which is often aimed at specific categories of the population, to whom it poses a significant threat. The broad and operational nature of this approach means that it offers the unquestionable advantage of reflecting the reality of the situation in that there is no uniformity in the hate speech expressed on the Internet and that the latter can be structural or transitory[8]. Structural speech requires a very clear distinction to be made between the posting of politicised and well-constructed content corresponding to actual propaganda produced by small groups, sometimes based abroad and with varying degrees of hierarchy, on the one hand, and expressions of a more 'commonplace' type of hatred on the part of Internet-users that see their speech as somewhat legitimated as a result of the relative anonymity the Internet offers, on the other. Transitory hate speech, meanwhile, is based primarily on current affairs. Early indications of racism, anti-Semitism and Islamophobia in comments posted in forums and on discussion platforms regarding the Israeli-Palestinian conflict are a prime example of this[9], as are the very many messages advocating the January 2015 attacks[10].

3. The initial work undertaken by the CNCDH is now unquestionably outdated since it relates to a period in time, the age of Web 1.0, in fact, when the Internet was merely designed as a tool for classifying, consulting and processing information. The user was limited to playing a passive role, content to simply receive information and to share it with others. However, the way in which the Internet works changed completely in the mid-2000s with the 'Web 2.0'[11] revolution that followed the exponential growth of social networks, audiovisual content sharing sites, discussion platforms, blogs and email, providing the Internet-user with various tools that enabled them to play an active role in the Internet and a special part in communications as a powerful vehicle of collective intelligence[12]. Technology enables the user to provide and indeed to share information on a daily basis, thus becoming a writer, journalist, artist or publisher in their own right[13]

---

[6] See Sciences Po - CERI, *Colloque du 17 novembre 2014 : Incitation à la discrimination ou à la haine : perspectives croisées sur une répression problématique*. On the history of this notion and its American origin see Walker, V.S., *Hate Speech: The History of An American Controversy*, Lincoln University of Nebraska Press 1994.

[7] See Recommendation n°R (97) adopted on 30 October 1997 by the Committee of Ministers of the Council of Europe, which defines hate speech as "covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, antisemitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin". See also Committee on the Elimination of Racial Discrimination – CERD, General Recommendation n°35 on Combating racist hate speech (26 October 2013).

[8] On this distinction see Knobel, M., 'Lorsque le racisme tisse sa toile sur le Net en 2009', in CNCDH, *Rapport 2009. La lutte contre le racisme, l'antisémitisme et la xénophobie*, La Documentation Française 2010, p.274; Falque-Pierrotin, I., *op. cit.*, p.18-19.

[9] Falque-Pierrotin, I., *op. cit.*, p.18 *et seq.*; Conseil Supérieur de l'Audiovisuel, *Lutter contre le racisme et l'antisémitisme sur les médias relevant du droit de la communication audiovisuelle,* Paris, November 2009.

[10] See Quinault Maupoil, T., 'Il sera jugé pour avoir fait l'apologie de l'attentat contre Charlie Hebdo', online at www.lefigaro.fr.

[11] See Rebillard, F., *Le Web 2.0 en perspective : une analyse socio-économique de l'internet*, L'Harmattan 2007; Trudel, P. and Abran, F., *Gérer les enjeux et risques juridiques du Web 2.0,* Université de Montréal, January 2012.

[12] See Beaude, B., *Les fins d'internet*, Fyp 2014, p.37 *et seq.*

[13] Achilléas, P., 'Internet et libertés', JurisClasseur Libertés, fasc. n°820, n°27.

should they so choose. As a result of its transition to a participatory tool[14], the Internet has considerably increased the individual's 'capabilities', in the words of Amartya Sen, meaning their actual ability to exercise their liberties[15]. With this in mind, the CNCDH has a duty to duly recognise a major societal development already identified by the Constitutional Council and the European Court of Human Rights, stating that "the Internet has now become one of the principal means by which individuals exercise their right to freedom of expression and information"[16]. Admittedly, prior to the launch of Web 2.0, one could only exercise their right to express their thoughts by means of access to professional media (written press, audiovisual media, publishers, etc.), which were subject to certain ethical standards and therefore served as a filter. Nowadays, however, anyone can create a blog or post a comment or video online. The Internet now enables anyone to circulate and share a wide variety of content with a potentially global audience and with no 'gate-keeper' to monitor the content that is being circulated[17]. If, as stated in Article 11 of the 1789 Declaration, "the free communication of ideas and of opinions is one of the most precious rights of man", then the Internet is currently one of the most precious tools for exercising one of the most precious rights of man[18]. Furthermore, whilst Article 10-1 of the European Convention on Human Rights (ECHR) provides that freedom of expression must be exercised "regardless of frontiers", it is the Internet, and the Internet alone, that has made it possible to effectively remove these frontiers[19].

4. This being the case, the participative Internet has put an end to the monopoly formerly held by the traditional media with regard to the information available to the public[20]. Agathe Lepage worthily points out that "the Internet primarily represents a change of paradigm with regard to public expression in that it enables anyone to express themselves without the filtering and selection processes associated with access to more traditional means of public expression, such as publishing, television, radio (...) With this in mind, it is perfectly reasonable to believe that it is actually the Internet that has enabled the principle of freedom of expression to really come into its own in that, from a public communications perspective, it is now a reality for a significant part of society"[21]. This development shows that prior editorial control (i.e. at the point of accessing traditional media) has given way to *a posteriori* control (that is at the point at which content is selected by the Internet-user)[22], with users sorting through the information themselves once it has been posted on such and such website[23]. This could only

[14] On the participative Internet see Cardon, D., *La démocratie Internet. Promesses et limites.* Seuil 2010, p.46 *et seq.*; Dérieux, E., 'Régulation de l'internet. Libertés et droits fondamentaux', *RLDI* 2012, n°78, p.95.
[15] Sen, A., *L'idée de justice*, Flammarion 2012, p.277 *et seq.* and p.309 *et seq.*
[16] See Const. Coun. 10 June 2009, n°2009-580 DC, considering n°12; ECtHR 18 December 2012, *Ahmet Yildirim v. Turkey* app. n°3111/10, §54.
[17] See Wolton, D., *Internet et après ? Une théorie critique des nouveaux médias*, Flammarion 2000, p.115, which supports the reintroduction of mediators on the Internet, insofar as the latter serve as "garantors of a certain philosophy of information".
[18] Council of State, *Etude annuelle 2014. Le numérique et les droits fondamentaux*, La Documentation Française 2014, p.146.
[19] *Ibid.*, p.145.
[20] Lucas, G., 'Internet pour le meilleur et pour le pire ?', in Lepage, A. (dir.), *L'opinion numérique. Internet : un nouvel esprit public*, Dalloz 2006, p.95 *et seq.*
[21] Lepage, A., 'Internet au regard de la loi du 29 juillet 1881 sur la presse : un mode de communication comme un autre ?', in Lepage, A. (dir.), *L'opinion numérique, op. cit.*, p.141-142. See also Trudel, P. and Abran, F. *op. cit.*, p.11-12, which alludes to the "heightened role of the amateur" in situations that were formerly dominated by professionals.
[22] Council of State, *Etude annuelle 2014, op. cit.*, p.145; Cardon, D., *op. cit.*, p.39 *et seq.*
[23] Cardon, D., *op. cit.*, p.41-42, which states that it is the "principle of the ex-post hierarchisation performed by Internet-users according to their position within the online reputation-based structure (…) Those sites that rank very poorly in the Internet hierarchies are only accessible to Internet-users who deliberately search for

serve to put an end to the notion of speech being governed by certain standards[24] and pave the way for the complete deregulation of affects and subjectivities, since not all Internet-users are media professionals with knowledge and experience of the ethics of public communications[25]. The following factors must also be taken into account:

- the possibility of anonymity and using a pseudonym, which foster a strong sense of impunity[26]. Using the Internet can even create a 'habit of anonymity' among Internet-users who, believing themselves to be invisible and unidentifiable online, allow themselves to behave in a way that is inappropriate to life in society or even unlawful;
- the fact that online communication often breaches some of the most basic rules of politeness and courtesy, even in the absence of anonymity[27].

The Internet brought us into the age of 'interactive solitude'[28] in which many individuals, finding themselves free of any rules or constraints, demonstrate an intense indifference to the fate of their neighbour[29]. As a result, and in spite of themselves, the new technologies associated with Web 2.0 have become a vehicle for the dissemination of speech that previously had no place in the traditional media[30] and that inevitably enjoys heightened visibility thanks to the amplifying effects of the Internet[31]. It is unsurprising, then, that the past ten years have been marked by a worrying proliferation of hate speech[32] and therefore by the normalisation of racist, anti-Semitic, xenophobic, Islamophobic and homophobic speech online[33]. Little is yet known, however, of the true scope of the phenomenon, owing in particular to the fragmented nature of the statistics

---

them, which does nothing to lessen the intolerable nature of anti-Semitic, racist, sexist, homophobic, etc. remarks. The fact remains that, in a spirit resembling that of the First Amendment of the American constitution, the Internet rejects any paternalistic policy that would define for others what it is appropriate to say or to hear. On the other hand, it trusts the self-structured activity of Internet-users to ensure that information that must remain in the dark depths of the Internet does not become visible. Greatness and misery of freedom of speech in the digital era".

[24] Cardon, D., *op. cit.*, p.37-38.

[25] *Ibid.*, p.10-11: "It is now possible for a large number of people who would previously have been considered inept or ignorant to comment on, critique, ridicule and even alter public speech, but the Internet also draws Internet-users' personal expressions into the public sphere. The web has taken possession of conversations that were not previously recognised as belonging in the public domain by taking advantage of the new self-exposure practices adopted by individuals. The dividing line between private social relations and public debate is further complicated by a new tendency that is leading individuals to expose themselves and to forge links between their personal lives and public matters before the eyes of others".

[26] Charpenel, Y., *Audition du 11 septembre 2014.*

[27] Moulard, C., *Mailconnexion. La conversation planétaire*, Au Diable Vauvert 2005; Feral-Schuhl, C., *Audition du 23 octobre 2014.*

[28] See Wolton, D., *Internet et après ?, op. cit.*, p.106; Wolton, D., *Penser la communication,* Flammarion 1997, chapter XIV.

[29] Teyssié, B., 'L'homme et la fourmi. Variations sur l'empire du numérique', in Teyssié, B. (dir.), *La communication numérique, un droit, des droits*, Editions Panthéon-Assas 2012, p.61.

[30] Quéméner, M., *Cybersociété. Entre espoirs et risques*, L'Harmattan 2013, p.170 *et seq.*; Schmidt, P. (INACH), *Audition du 4 septembre 2014.*

[31] The Court of Strasbourg usefully pointed out that "modern means of conveying information and the fact that it was accessible to everyone, including minors, would have multiplied the impact of the poster campaign" (ECtHR, Grand Chamber, 13 July 2012, *Mouvement Raëlien Suisse v. Switzerland*, app. n°16354/06).

[32] See Knobel, M., *L'internet de la haine, op. cit.* See Lepage, A., *Libertés et droits fondamentaux à l'épreuve de l'internet,* Litec 2002, p.91 *et seq.* On the situation in the United States see Bell, J., 'Pour faire barrage à ceux qui n'ont pas de cœur : expressions racistes et droits des minorités', in Zoller, E. (dir.), *La liberté d'expression aux États-Unis et en Europe.* Dalloz 2008, p.52 *et seq.*

[33] Gilles Clavreul (DILCRA) stated during a talk at the CNCDH on 29 January 2015 that the number of reports of hateful online content reached 15,000 in 2014.
For detailed figures for 2014 see the contributions of Quéméner, M. and the Minister of the Interior in CNCDH, *Rapport 2014. La lutte contre le racisme, l'antisémitisme et la xénophobie*, La Documentation Française 2015.

available[34] and the relative lack of scientific knowledge of the matter. With this in mind, the CNCDH recommends that public authorities improve the tools that will make it possible to establish the exact nature of the phenomenon, notably through the introduction of statistical tools, with a specific breakdown of acts committed on or via the Internet, and the funding of research in the field. In this respect, the public and private sectors could join forces and collaborate for the purpose of implementing cross-disciplinary research projects based on innovative scientific methods that recognise and accept the digital 'imperative'[35].

5. Furthermore, the CNCDH regularly reiterates, as do the Constitutional Council[36] and the Court of Strasbourg[37], that freedom of expression, as guaranteed by Article 10 of the ECHR, is one of the key founding principles of a democratic society[38]. This right "is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no "democratic society""[39]. The CNCDH is also fundamentally concerned about the safeguarding and, if need be, extension of the public sphere of free discussion which is consubstantial to democracy and the rule of law[40]. Impertinence, irreverence and disturbing ideas represent an incalculable source of wealth when it comes to raising awareness and all have their place in a public sphere that is not sterilised by means of the harnessing of speech. In this respect, freedom of expression has unquestionably become the 'cornerstone' of Web 2.0 insofar as it represents the very essence of its function, namely to receive and provide information[41]. However, whilst the Internet is a formidable platform for exercising freedoms, it should not be perceived as a 'law-free zone'[42] governed by the 'free flow of ideas' or one in which the State should abstain from any form of intervention so as not to distort the free competition of opinions[43]. Indeed, Article 10-2 of the ECHR states that the exercising of freedom of expression inherently implies certain 'duties and responsibilities' in order to prevent it being used in a way that might be irresponsible or detrimental to the rule of law[44]. This being the case, "democratic society is tolerant but not inert. As a militant democracy, society

[34] See Groupe de Travail Interministériel sur la Lutte contre la Cybercriminalité ('Interministerial Working Group on Fighting Cyber-Criminality'), *Protéger les internautes. Rapport sur la cybercriminalité*, February 2014, p.20 *et seq*.

[35] See Wieviorka, M., *L'impératif numérique*, CNRS-éditions 2013. As far as this author is concerned, human and social sciences should play a role in new information technologies by using Web 2.0 data and social networks to exchange, communicate, collaborate and create 'digital humanities'. With examples to support his claims, he explains exactly how they could benefit from the digital sphere and suggests a new way of structuring research that would overstep the boundaries of a discipline system that has become a real hindrance to intellectual innovation.

[36] Const. Coun. 10 June 2009, n°2008-580 DC.

[37] See notably ECtHR 7 December 1976, *Handyside v. United Kingdom*, app. n°5493/72, §49; ECtHR, 28 June 2012, *Ressiot & Others v. France*, apps. n°15054/07 and 15066/07.

[38] CNCDH 25 April 2013, *Avis sur la réforme de la protection du secret des sources*, *JORF* n°0134 of 12 June 2013, text n°90.

[39] ECtHR 7 December 1976, *Handyside v. United Kingdom, op. cit.*, §49.

[40] See Wachsmann, P. 'Participation, communication, pluralisme', *AJDA* 1998, p.165; Flauss, J.-F., 'La Cour européenne des droits de l'homme et la liberté d'expression' in Zoller, E. (dir.), *op. cit.*, p.102.

[41] Casas, M. et al., *Rapport de recherche - table ronde 2014 Quel(s) droit(s) pour les réseaux sociaux ? La liberté d'expression et les réseaux sociaux*, Aix-Marseille Université / IREDIC, p.5.

[42] Comp. Choné-Grimaldi, A.-S., 'Publicité en ligne et pratiques anticoncurrentielles', in Teyssié, B. (dir.), *op. cit.*, p.233.

[43] In this respect, the United States Supreme Court confirmed that, "under the First Amendment, there is no such thing as a false idea. However pernicious an opinion may seem, we depend for its correction not on the conscience of judges and juries, but on the competition of other ideas" (*Gertz v. Robert Welch* case, 418 US 323 (1974)).

[44] Flauss, J.-F., *op. cit.*, p.98.

must defend its basic principles. Consequently, it also has the duty to fight against abuses, committed in the exercise of freedom of speech, that openly target democratic values"[45]. The Court of Strasbourg very strongly condemns hate speech, maintaining that racist and xenophobic claims are not protected by Article 10 of the ECHR[46]. The same applies to "remarks intended to incite racial hatred in society and to promote the idea of a superior race"[47] and "all forms of expression which spread, incite, promote or justify hatred based on intolerance (including religious intolerance)"[48]. Any speech that is incompatible with democracy and human rights is not a matter of freedom of expression[49] and cannot purport to be covered by the guarantees provided by the Convention in accordance with Article 17 of the ECHR[50]. As a result, States have a positive obligation to fight any speech that contradicts the values of liberties and fundamental rights by encouraging intolerance, hatred and racism. With this in mind, the CNCDH will outline a series of recommendations with the following aims:

- to affirm the digital sovereignty of the State (I.);
- to strengthen existing systems designed to fight hate speech on the Internet (II.);
- to have access to a responsive and innovative Internet regulatory body (III.)
- to adopt a national digital education and citizenship action plan (IV.).

I. AFFIRMING THE DIGITAL SOVEREIGNTY OF THE STATE

A. REINFORCING THE VITAL ROLE OF THE STATE IN GUARANTEEING FUNDAMENTAL RIGHTS AND FREEDOMS ONLINE

6. Once again, the tragic events of January 2015 resulted in a proliferation of incidences of hate speech on the Internet, only a minimal proportion of which resulted in criminal prosecution. The CNCDH can therefore only reiterate its recommendation designed to encourage widespread reflection on the potential definition of a form of 'digital public order'[51] based on the notion that the Internet must remain a platform for exercising freedoms where fundamental rights and liberties are respected and not a platform for impunity. After all, as the European Court of Human Rights has said on the matter, "it is true that the Internet is an information and communication tool particularly distinct from the printed media, especially as regards the capacity to store and transmit information. The electronic network, serving billions of users worldwide, is not and potentially will never be subject to the same regulations and control. The risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than

[45] *Ibid.*, p.124.
[46] ECtHR 23 September 1994, *Jersild v. Denmark*, app. n°15890/89.
[47] ECtHR 10 October 2000, *Ibrahim Aksoy v. Turkey*, app. n°28635/95.
[48] ECtHR 4 December 2003, *Günduz v. Turkey*, app. n°35071/97.
[49] See Goldman, S., 'Le discours de haine raciste et/ou antisémite en France – Aspects juridiques', in CNCDH, *Rapport 2011. La lutte contre le racisme, l'antisémitisme et la xénophobie,* La Documentation Française 2012, p.173, which rightly asserts that "the expression of racism is not an opinion but an offence".
[50] "Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided for in the Convention".
[51] CNCDH 25 September 2014, *Avis sur le projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme, JORF* n°0231 of 5 October 2014, text n°45.

that posed by the press"[52]. However, it is sometimes claimed that the Internet, owing to its immaterial nature, should escape State control both in fact and in form[53], but the advent of the digital society does not represent a return to a new state of nature with no social contract or political sovereignty[54]. With this in mind, the CNCDH wishes to reiterate that the State is at complete liberty to supervise human activity online for the purpose of ensuring that it fully complies with fundamental rights and freedoms[55]. This is particularly true given that such activity, which is virtual only in its appearance, can have very real consequences. As it happens, there is a degree of asymmetry of power between users and associations, on the one hand, and Internet service providers[56], on the other, the latter often being extremely powerful economic players. Furthermore, whilst instances of hate speech online have increased in recent years, this is actually due to a sense of impunity that stems from the fact that public authorities do not have a strong enough online presence[57].

B. UNDERTAKING DIPLOMATIC NEGOTIATIONS LEADING TO THE SIGNING AND RATIFICATION OF ADDITIONAL PROTOCOL N°189 TO THE CONVENTION ON CYBERCRIME

7. It is important to emphasise the specific difficulties associated with the Internet as a cross-border or even borderless tool, given that law is a national concept that is applied primarily on a regional scale[58]. With this in mind, the Council of State rightly points out in its *Etude annuelle 2014* annual study entitled *Le numérique et les droits fondamentaux* ('The digital sphere and fundamental rights') that the notion of territoriality incorporates a strategic dimension: "What is actually being called into question here is the ability of a State to protect the fundamental freedoms of its citizens, along with their right to appeal"[59]. Furthermore, regulating the Internet has unquestionably become a major issue of sovereignty[60]. With regard to the specific issue of abuses of freedom of expression, the French legal system allows for French laws and jurisdiction to prevail in matters of civil and criminal

---

[52] ECtHR 5 May 2011, *Editorial Board of Pravoye Delo and Shtekel v Ukraine*, app. n°33014/05, §63.

[53] See Barlow, J. P., *A Declaration of the Independence of Cyberspace*, Editions Hache 1996: "We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity. Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are based on matter, there is no matter here".
For legal analyses see Frison-Roche, M.-A., 'Les bouleversements du droit par internet', in *Internet et nos fondamentaux*, PUF 2000, p.45-46.

[54] For further information see Beaude, B., *op. cit.*, p.28 *et seq*.

[55] See Council of State, *Etude annuelle 2014, op. cit.*, p.133.

[56] For the purpose of the present opinion this notion is understood in the sense of Article 2 of Directive 2000/31/EC of 8 June 2000 on *certain legal aspects of information society services, in particular electronic commerce, in the internal market*: "For the purpose of this Directive, the following terms shall bear the following meanings: (…) b) 'service provider': any natural or legal person providing an information society service".
Furthermore, paragraph 17 of Article 1 of Directive 2000/31/CE *modifying Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations* defines an information society service as "any service normally provided for remuneration, at a distance, by means of electronic equipment (...) and at the individual request of the recipient of a service".

[57] See Walter, E. (HADOPI), *Audition du 20 novembre 2014* : "Upstream, we must be wary of the notion of trust with regard to self-regulation. It is not because the State is unable to fulfil its role that it must delegate certain functions to private players. It is a dangerous slope, particularly since it is due to the fact that the forces of law and order have failed to adapt in order to apply the laws that such an idea exists".

[58] See Vivant, M., 'Cybermonde : Droit et droits des réseaux', *JCP gen. ed.* 1996, I., 3969; Marchadier, F., 'Le web ignore les frontières et l'internationalité lui est consubstantiel', in Pailler, L. (dir.), *Les réseaux sociaux sur internet et le droit au respect de la vie privée*, Larcier 2012, p.6.

[59] Council of State, *Etude annuelle 2014, op. cit.*, p.240.

[60] Bellanger, P., *La souveraineté numérique*, Stock 2014.

liability[61]. This being the case, the principle of extended territoriality, according to which "the offence is deemed to have been committed within the French Republic as long as one of its component acts has taken place in the country" (Article 113-2 paragraph 2 of the French Criminal Code), makes it possible, at least in theory, for French criminal law and the ruling of a French judge to prevail, provided that the unlawful content is accessible within France[62]. In practice, however, if a company has relocated its activities to 'Internet havens', prosecution and the implementation of measures designed to suppress such activity will be destined to fail[63]: "the deterritorialised world of the Internet is largely understood by those who encourage racism as a terrific way of escaping repression. They use both differences in legislation and the power of communication that the Internet offers"[64]. Some of the hearings held at the CNCDH notably highlighted that some hosting service providers with head offices located in the United States do not consider themselves to be bound by the provisions of French criminal law regarding the abuse of freedom of expression[65]. Referring to the First Amendment of the American Constitution, they maintain that hate speech is nothing more than the expression of an opinion since they are not directly or immediately encouraging anyone to commit an act of violence[66]. With this in mind, the CNCDH believes there is an urgent need to strongly reaffirm its profound attachment to European democratic values. It can therefore only encourage the French State once again to implement strong diplomatic measures to have those States hosting sites that publish hate speech sign and ratify Additional Protocol n°189 of the Council of Europe's Convention on Cybercrime dealing specifically with racism and anti-Semitism[67].

C. ESTABLISHING THE TERRITORIAL SCOPE OF ARTICLE 6 OF THE FRENCH LAW ON TRUST IN THE DIGITAL ECONOMY (LCEN)

8. A number of the hearings conducted at the CNCDH highlighted the fact that the majority of sites hosting hate speech are hosted by companies with head offices located in Ireland or the United States and which consequently claim legal alien status. As a result, major American companies such as Facebook, Twitter and YouTube do not consider themselves to be bound by the provisions of Article 6 II. of

[61] For futher information see notably Dérieux, E. and Granchet, A., *Réseaux sociaux en ligne. Aspects juridiques et déontologiques*, Lamy 2013, p.34 *et seq.*; Dérieux, E., 'Règles de procédure applicables à la poursuite des abus de la liberté d'expression. Garantie de la liberté d'expression ou privilège des médias ?', *RLDI* 2013, n°89, p.61 *et seq.*; Francillon, J., 'Le droit pénal face à la cyberdélinquance et la cybercriminalité', *RLDI* 2012, p.103; Martin-Hocquenghem, E., 'Le principe de la territorialité de la loi pénale et les infractions commises sur internet', in Teyssié, B. (dir.), *op. cit.*, p.495 *et seq*.

[62] Court of Cassation, Criminal Division, 9 September 2008, n°07-87.281, which states that French criminal law applies to sites aimed at a French audience, the offence then being considered to have been committed on French soil. On this matter see also Lepage, A., 'Réflexions sur l'adaptation du droit pénal à l'internet', in Teyssié, B. (dir.), *op. cit.*, p.493; Groupe de Travail Interministériel sur la Lutte contre la Cybercriminalité ('Interministerial Working Group on Fighting Cyber-Criminality'), *op. cit.*, p.211; Council of State, *Etude annuelle 2014*, *op. cit.*, p.325.

[63] In the case of an American hosting service provider being sentenced by default by a French judge on the grounds of Article 113-2 paragraph 2 of the Criminal Code, for example, the American courts will refuse to enforce the decision in the absence of any similar default procedure in American law. Indeed, the United States Supreme Court considers the proof of the accused party to be a constitutional right in accordance with the 6th Amendment (the case of the *United States v. Gagnon* 470 US 522 (1985); see also Pradel, J., *Droit pénal comparé,* Dalloz 2002, n°472, p.592 *et seq.*).

[64] Falque-Pierrotin, I., *op. cit.*, p.27.

[65] Schmidt, P. (INACH), *Audition du 4 septembre 2014*; Louvet, B. (LICRA), *Audition du 4 septembre 2014.*

[66] For further information on United States law see Preuss-Laussinotte, S., *La liberté d'expression*, Ellipse 2014, p.27 *et seq.*; Zoller, E., 'La Cour suprême des Etats-Unis et la liberté d'expression', in Zoller, E. (dir.), *op. cit.*, p.253 *et seq*.

[67] See CNCDH, *Rapport 2010. La lutte contre le racisme, l'antisémitisme et la xénophobie*, La Documentation Française 2011, p.166; CNCDH, *Rapport 2013. La lutte contre le racisme, l'antisémitisme et la xénophobie*, La Documentation Française 2014, p.215.

law n°2004-575 of 21 June 2004 *on confidence in the digital economy* (hereafter referred to as the LCEN) that requires players in the Internet sector to cooperate with legal and administrative authorities to help identify individuals who have contributed to the creation of unlawful content[68]. In cases where Internet-user anonymity is combined with the absence of any cooperation on the part of the service providers (hosters) concerned, it is extremely difficult for the judicial authority to quickly obtain the information required to identify those suspected of having committed a criminal offence (IP address, etc.). Furthermore, it is regrettable that many foreign companies no longer consider themselves bound by Article 6 I. 7 of the LCEN enabling the judicial authority to ensure that hosting service providers and access providers are bound by a special (targeted and temporary) surveillance obligation regarding certain illegal behaviours, it being reiterated that, with regard to clamping down on offences relating to abuses of freedom of expression, these service providers must also promptly inform the public authorities of any unlawful activity of which they are aware and publicise the resources they devote to fighting such activity[69].

9. In light of the aforementioned, the CNCDH laments the fact that, owing to a failure on the part of foreign companies to fulfil their obligations, the French public authorities are all too often rendered powerless with regard to implementing a policy designed to fight hate speech on the Internet. As far as the CNCDH is concerned, the fact that the effectiveness of a law can be dependent upon the specific interests of an industry and indeed on economic and even political interests in general simply cannot be tolerated. It would call for the State not to abdicate its sovereignty and consequently recommend that the territorial scope of Article 6 of the LCEN, the provisions of which should apply to any company conducting any form of economic activity in France, be clearly established[70].

10. Furthermore, protecting public interest and the principle of equality before the law require a guarantee that service providers will fulfil their obligations and that any failings observed will be punished, bearing in mind that the criminal sanctions provided for in the LCEN have never previously been enforced[71]. This situation is all the more unfortunate given that it results in a distortion of competition that is detrimental to French companies that do comply with the law[72], the economic weight of which is far inferior to that of the American Internet and computer giants. It is for this reason that the CNCDH is firmly convinced that achieving digital sovereignty must also be concurrently supported by the following:
    - renewed stimulation of the French digital industry and support for innovation in the field for the purpose, as recommended by the Economic, Social and Environmental Council, of "creating an ecosystem that is conducive to the emergence and growth of start-ups with the potential to become the digital champions of tomorrow"[73]. The major French economic players must also make a

[68] Council of State, *Etude annuelle 2014, op. cit.*, p.245; Dérieux, E., 'Diffusion de messages racistes sur Twitter. Obligations de l'hébergeur', *RLDI* 2013, n°90, p.27 *et seq.*
[69] Groupe de Travail Interministériel sur la Lutte contre la Cybercriminalité ('Interministerial Working Group on Fighting Cyber-Criminality'), *op. cit.*, p.185 *et seq.* See Falque-Pierrotin, I., *op. cit.*, p.59.
[70] See Council of State, *Etude annuelle 2014, op. cit.*, p.245.
[71] Groupe de Travail Interministériel sur la Lutte contre la Cybercriminalité ('Interministerial Working Group on Fighting Cyber-Criminality'), *op. cit.*, p.187-188.
[72] *Ibid.*, p.185-186.
[73] Economic, Social and Environmental Council (ESEC) 13 January 2015, *Données numériques, un enjeu d'éducation et de citoyenneté* (reporter: E. Peres), p.96.

stronger commitment to developing the digital industry in order to promote the values of the Republic and indeed of human rights[74];

- a policy designed to hold companies accountable with regard to respecting human rights[75], and the French understanding of freedom of expression in particular.

II. STRENGTHENING EXISTING SYSTEMS DESIGNED TO FIGHT HATE SPEECH ON THE INTERNET

A. INCREASING THE EFFECTIVENESS OF SYSTEMS RESULTING FROM THE LAW OF 29 JULY 1881 ON THE FREEDOM OF THE PRESS

1. Upholding the crimes of opinion and abuses of freedom of expression outlined in the law of 29 July 1881

11. On a preliminary basis, the CNCDH believes that existing incriminations outlined primarily in the law of 29 July 1881 *on the freedom of the press* and in a few rare cases in the French Criminal Code are sufficient[76]. In a multi-party democracy based on freedom of opinion and of expression, offences relating to the abuse of public expression must be strictly outlined and defined and be based on violations or a proven risk of violation of individuals (libel, slander, provocation, advocacy or negationism). The scope of this repression cannot be extended without disproportionately affecting the freedom of expression guaranteed under Article 10-1 of the ECHR.

12. The law of 29 July 1881 subtly and progressively outlines the balance that must be maintained between the freedom of expression that it protects and its limits, which is why violations that incriminate hate speech and abuses of freedom of expression are so specific in their nature that they are not permitted to be incorporated in the French Criminal Code. Furthermore, the specific system that governs press offences demonstrates both to the Court of Strasbourg and to the European bodies concerned that, even in the event that our right to communication is not decriminalised – a decriminalisation of which the Council of Europe is in favour[77] –, French law on the matter complies, both in letter and in spirit, with Article 10 of

---

[74] See Lemoine, P., *Rapport au Gouvernement. La nouvelle grammaire du succès. La transformation numérique de l'économie française,* November 2014, p.15: "It is time that the major French groups turned the page on the disappointments and humiliation that some of them experienced when they came a cropper during the Internet bubble. That was 10 years ago and the context has since changed. They need to start again with strong, original and motivational plans for the future. We can cite examples of such projects in the banking sector ('Secure anonymous payment'), in commerce ('The bookseller of the future'), in the manufacturing industry ('A car for the young, including multiple designs and prototyped in the FabLab), in the transport sector ('A tailored universal mobility pass'), in the health sector ('Digital life, chronic conditions') and in the administrative sphere ('Territorial innovation network for local services'). Particular emphasis is placed on projects with the potential to contribute to our growth model, including the acceleration of professional mobility (the 'Emploi Store', the 'Public cross-functional mobility platform'), ecological issues and the energy transition (Green Button *à la française*'), the living link between the public interest approach and the shared asset approach supported by major foundations (Wikipedia, Mozilla, OpenStreetMap, etc.)".

[75] CNCDH 24 October 2013, *Business and human rights: report on the issues associated with the application of the United Nations' Guiding Principles in France*, JORF n°0266 of 16 November 2013, text n°56.

[76] See Groupe de Travail Interministériel sur la Lutte contre la Cybercriminalité ('Interministerial Working Group on Fighting Cyber-Criminality'), *op. cit.*, p.152; Knobel, M., *Audition du 4 septembre 2014*; Mbongo, P., *Audition du 23 octobre 2014*; Quéméner, M. and Ferry, J., *Cybercriminalité. Défi mondial,* 2nd ed., Economica 2009, p.155.

[77] See Bechtel, M.-F., *Rapport n° 409 au nom de la Commission des lois (…) sur le projet de loi (…) relatif à la sécurité et à la lutte contre le terrorisme,* French National Assembly, 14 November 2012, p.54.

the ECHR[78]. As a result, the CNCDH is in principle opposed to the inclusion of offences relating to freedom of expression in the French Criminal Code. Where the legislator wishes to specifically incriminate certain behaviours that are more or less closely related to communication, however, and to firmly repress such behaviours, it is preferable that they do so in the framework of the Criminal Code and not that of the law of 1881, which loses some of its meaning here[79].

13. The CNCDH implemented these guidelines concerning offences relating to public incitement to commit acts of terrorism and the public condoning of such acts in its opinion of 25 September 2014 on the bill designed to reinforce provisions regarding the fight against terrorism[80]. Indeed, law n°2014-1353 of 13 November 2014 *reinforcing provisions regarding the fight against terrorism* anticipated them being removed from the law of 29 July 1881 and incorporated by means of a new Article, Article 421-2-5, into the French Criminal Code[81] on the grounds that it is not a matter of an "abuse of freedom of expression (…) but rather of actual facts that are directly responsible for terrorist acts". These new provisions, which make no distinction between provocation that has an effect and provocation that has no effect (as Articles 23 and 24 of the law of 29 July 1881 currently do[82]), encompass both types of provocation[83]. In the event of provocation having an effect (namely the commitment of acts of terrorism), the matter is no longer one of freedom of expression but rather one of personal protection. The issue of fighting terrorism has become all the more pressing since it relates, as stated in the new Article 421-2-5 of the French Criminal Code, to a 'direct' provocation leading to written and spoken remarks that explicitly define the acts for which the provocation calls. In the event of provocation that does not have an effect, however, the reprehensible act remains a matter of freedom of expression. In light of the aforementioned, whilst the CNCDH is not opposed to public provocation that has an effect being incorporated into the French Criminal Code, it does believe that public provocation that does not have an effect should continue to be governed by the law of 29 July 1881. This is all the more applicable with regard to the public condoning of terrorism, which must continue to be governed by specific provisions of the law on the press. Indeed, the CNCDH fears that the move to remove a number of offences relating to abuses of freedom of expression from the law of 29 July 1881 will also

[78] CNCDH 20 December 2012, *Avis sur la loi relative à la sécurité et à la lutte contre le terrorisme*, online at www.cncdh.fr. CNCDH 25 September 2014, *Avis sur le projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme, op. cit.*

[79] *Ibid.*

[80] See CNCDH 25 September 2014, *Avis sur le projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme, op. cit.*

[81] Article 421-2-5 of the French Penal Code: "Directly provoking acts of terrorism or publicly condoning such acts is punishable by five years' imprisonment and a €75,000 fine.
These penalties are increased to seven years' imprisonment and a €100,000 fine in the event that the acts are committed using an online public communication service.
In the event that the acts are committed through the written or audiovisual press or by means of online public communication tools, the specific provisions of the laws governing such matters apply with regard to identifying people responsible"

[82] The distinction between provocation that has an effect (Article 23 of the law of 29 July 1881) and provocation that does not have an effect (Article 24 of the law of 29 July 1881) is meaningful in that the former, in short, 'particularises' a case of complicity with the advantage that the judge is exempt from the obligation to provide proof with regard to any of the adminicles of Article 121-7, paragraph 2 of the French Criminal Code (donation, pledge, etc.). The latter, meanwhile, makes a case of complicity that would not otherwise be considered to be independent for lack of a primary offence ("that does not have an effect") punishable by making it an independent offence.

[83] In this respect, French law complies with Framework Decision 2008/919/JAI of the Council of the EU dated 28 November 2008 *which amends Framework Decision 2002/475/JAI of 13 June 2002 on combating terrorism*. According to this document, incitement to commit acts of terrorism must be suppressed, regardless of whether or not it has an effect.

rid this great law of its substance by depriving it of any coherence and at the risk of marginalising it and eventually seeing it disappear altogether.

14. Furthermore, certain emergency procedures, which notably include immediate appearance and plea-bargaining, are not appropriate to disputes regarding abuses of freedom of expression, the complexity and values of which require them to be dealt with in a firm but considered manner. Proof of this came in the wake of the January 2015 attacks in the form of a burst of convictions resulting from immediate appearances for condoning terrorism, this legal process having been made possible as a result of the reform of 13 November 2014[84]. As the texts currently stand, in order to guarantee the principle of the equality of citizens before the law, as well as the principles of proportionality and legality, it would appear important for the legislator to accurately define the notion of condoning terrorism as a matter of urgency[85]. Furthermore, the CNCDH reiterates the fact that it is in favour of the introduction of alternatives to prosecution in the least serious cases of abuse of freedom of expression provided that they are well thought out and appropriate to this form of delinquency. Finally, extending the statute of limitations stemming from the incorporation of such offences in the French Criminal Code to three years is not appropriate. Indeed, reopening the public debate on an incident of slander or libel 3 years after it was potentially committed may contradict the pacifying function of the criminal proceedings.

2. Improving the procedural framework of the law of 29 July 1881

15. Since it was introduced in the 19th Century, the law of 29 July 1881 has been a symbolic cornerstone of French democracy and its basic standard of protection for freedom of expression[86]. Over time it has demonstrated its power, its influence, its adaptability and its ability to maintain a delicate balance between the fundamental right to freedom of expression and its necessary limits. Nevertheless, a number of the procedural provisions of this law are now clearly out of step with the increase in public expression following the 'Web 2.0' revolution, which resulted in the exponential growth of social networks, audiovisual content sharing sites, discussion platforms, blogs and email. Whilst the law of 29 July 1881 does, in some respects, apply to online communications, it is no longer appropriate to the mass disputes that the Internet is likely to generate[87]. It is a complex law, the content of which is not easily accessible, and one that can be judicially interpreted with a great deal of nuance, in a way of which only specialist legal practitioners have a sound command[88]. It was originally aimed at communications professionals (press, publishers, media, etc.) in an attempt to monitor their activity and result in a sophisticated dispute before highly specialist magistrates (and the 17th correctional chamber of the TGI Paris in particular). It was not originally intended to apply to all Internet-users, who have now become potential public publishers in their own right. In other words, the law of 29 July 1881 was not designed with widespread public expression in mind, the latter no longer being filtered upstream by responsible professional media players or subject to ethical controls. Nevertheless, the room for interpretation of which the judge avails with this law largely allows for the law

[84] See Alix, J., 'La répression de l'incitation au terrorisme', *Gaz. Pal.* 2015, yet to be published.
[85] See Godeberge, C. and Daoud, E., 'La loi du 13 novembre 2014 constitue-t-elle une atteinte à la liberté d'expression ? De la nouvelle définition de la provocation aux actes de terrorisme et de l'apologie de ces actes', *AJ Pénal* 2014, p.563-564.
[86] See CNCDH 25 April 2013, *Avis sur la réforme de la protection du secret des sources,* online at www.cncdh.fr.
[87] See Dreyer, E., *Audition du 23 octobre 2014*; Philippe, A., *Audition du 11 septembre 2014.*
[88] For a general overview see Mallet-Poujol, N., 'La liberté d'expression sur internet : aspects de droit interne', *Rec. Dalloz* 2007, p.591 *et seq*.

to be manoeuvred in a way that reflects the contexts and expectations of a certain age. With this in mind, the CNCDH recommends that certain improvements be made to the procedural provisions of the law of 29 July 1881 in order to more effectively combat the proliferation of hate speech posted on the Internet by non-professional Internet-users and with a view to facilitating victims' access to justice. These include the following:

- improving the intelligibility and understanding of the provisions of the law of 29 July 1881[89], particularly defining and updating the notions of public space and private space in Web 2.0 to reflect new types of digital communities and networks;
- considering the digitisation of procedures (and of summons and notifications in particular); simplifying and facilitating summary procedures through the introduction of a digital summary judgement (rather than maintaining various summary judgements on the matter); introducing the possibility of lodging complaints online[90];
- introducing an effective right to reply online in favour of anti-racism associations[91];
- giving the judge the power to order that a site cease to operate, in the same vein as the possibility of suspending a newspaper for 3 months in the event of incitement to racial hatred;
- giving the judge the power to order the cessation of an online communication service for any offence relating to abuses of freedom of expression[92];
- initiating reflection on the relevance of increasing and standardising statutes of limitations[93];
- considering the possibility of holding legal entities criminally liable[94], aside from press organisations[95].

16. Furthermore, a new major difficulty arose with the introduction of Web 2.0 in the form of an increase in speech published anonymously or under pseudonyms, making it difficult to identify the author of contentious remarks. Verbal and written remarks are then all the more uninhibited since the author has a strong sense of impunity[96]. In addition to the difficulty of identifying the authors of racist remarks, which is largely dependent on the cooperation of service providers, and hosting service providers in particular[97], the law of 29 July 1982 *on audiovisual communication* - which requires authors to be identified within a very short time frame and in the restrictive framework of an exhaustive list of cascading responsibility (director of publication, author, producer, etc.) - does not appear to

[89] Derieux, E., *Audition du 27 novembre 2014*; Lepage, A., *Audition du 3 décembre 2014*.
[90] See Féral-Schuhl, *C., Audition du 23 octobre 2014*.
[91] See Dreyer, E., *Audition du 23 octobre 2014,* which states that Article 13-1 of the law of 29 July 1881 does not currently provide for any specific right to reply with regard to the Internet.
[92] See Dreyer, E., *Audition du 23 octobre 2014,* which states that Article 50-1 of the law of 29 July 1881 does not currently apply to all racist remarks. It does, however, add that it is important that this authority be withdrawn from the judge hearing applications for interim measures (the *juge des référés*) and given to the freedom and detention judge (the *juge des libertés et de la détention*).
[93] For food for thought see Dreyer, E., 'L'allongement du délai de prescription pour la répression des propos racistes ou xénophobes. Commentaire de l'article 65-3 de la loi du 29 juillet 1881', *LEGICOM* 2006/1, n°35, p.107 *et seq*.; Dreyer, E., 'La Constitution ne s'oppose pas à l'abandon de la prescription trimestrielle en matière de presse', *Rec. Dalloz* 2013, p.1526.
[94] See ECtHR 10 October 2013, *Delfi AS v. Estonia*, app. n°64569/09.
[95] Comp. Dreyer, *E., Audition du 23 octobre 2014*, which suggests that racism-related offences be incorporated in the Criminal Code. This would notably make it possible to hold legal entities criminally liable.
[96] Dérieux, E., 'Réseaux sociaux et responsabilité des atteintes aux droits de la personnalité', *RLDI* 2014, n°100, p.79.
[97] See *infra*.

still be appropriate[98]. When a site relies on the anonymity of its director of publication and article authors, for example, the CNCDH believes that it is important to consider potentially extending the list of participants in the offence to include those responsible for managing the association or organisation behind the publishing website[99].

B. INCREASING THE EFFECTIVENESS OF SYSTEMS RESULTING FROM THE LAW ON TRUST IN THE DIGITAL ECONOMY (LCEN)

17. At the end of his magisterial work on cybercriminality, Public Prosecutor Robert clearly stated that the LCEN was "suffering from a general lack of effectiveness"[100]. This law, which is nevertheless largely considered to be of a high quality, could be adapted in order to more effectively fight hate speech on the Internet[101].

18. First and foremost, the LCEN guarantees the principle of 'network neutrality'[102] in global terms in that it establishes a system of limited service provider liability (access providers and hosting service providers)[103]. At the same time, the latter are under no general obligation to monitor content (Article 6 I., 7 LCEN)[104]. Firstly, it is important to point out that increasing liability on the part of service providers would present the risk of the 'privatisation of censorship': indeed, holding them responsible for content could, in reality, indirectly lead to them being delegated to undertake a surveillance and sanctioning mission, which would mean entrusting them with too central a role with regard to establishing digital public order. In any case, the rules governing the liability of service providers, as major players in the circulation of hate speech on the Internet, are unsatisfactory in that they are a major source of impunity owing to their complexity[105] and the corresponding lack of enforcement[106]. This being the case, it would appear necessary to clarify and to

[98] Article 93-3 of law n°82-652 of 29 July 1982 *on audiovisual communication*, which outlines the so-called 'cascading' responsibility system, states that "the director of publication or (...) the assistant director of publication will be pursued as the primary perpetrator in the event that the incriminated message has been approved prior to being communicated to the public". It adds that, "failing this, the author, and in the absence of the author, the producer will be pursued as the primary perpetrator" and that "in the event that the blame is placed with the director or assistant director of publication, the author will be pursued as an accomplice". It even states that "anyone else to whom Article 121-7 of the French Criminal Code may apply may also be pursued as an accomplice".

[99] See Philippe, A., *Audition du 11 septembre 2014.*

[100] Robert, M. *Audition du 3 décembre 2014.*

[101] On the loopholes in the French Law on Trust in the Digital Economy (LCEN), see notably Bossan, J., 'Le droit pénal confronté à la diversité des intermédiaires de l'internet', *RSC* 2013, p.295 *et seq.*

[102] On the principle of network neutrality see Huet, J. and Dreyer, E., *Droit de la communication numérique*, LGDJ 2011, p.16 *et seq.*; Dérieux, E., 'Entre esprit libertaire et nécessaire réglementation. A propos de la neutralité de l'internet. Un atout pour le développement de l'économie numérique', *RLDI* 2010, n°64, p.6 *et seq.*

[103] On reducing the responsibility of access providers and hosting service providers see Huet, J. and Dreyer, E., *op. cit.*, p.121 *et seq.*; Dérieux, E., 'Réseaux sociaux et responsabilité des atteintes aux droits de la personnalité', *op. cit.*, p.82 *et seq.* Comp. Castets-Renard, C., *Droit de l'internet : droit français et européen*, Montchrestien 2012, p.289 *et seq.*, which alludes to the '*conditioned irresponsibility*' of hosting service providers and Internet access providers.

[104] Article 6 I., 7 LCEN: "Those referred to in 1 and 2 (access providers and hosting service providers) are bound neither by a general obligation to monitor the information they publish or store nor a general obligation to monitor circumstances revealing any signs of unlawful activity.
The previous paragraph is without prejudice to any targeted and temporary monitoring activity requested by the judicial authority".

[105] On this matter see Bossan, J., *op. cit.*, n°33 *et seq.* See also Monfort, J.-Y., *Audition du 25 septembre 2014*, which suggests that Internet-users are 'unarmed' against hosting service providers, who can only be held responsible under the tightest of conditions, with an 'LCEN notification' system being difficult to implement in practice.

[106] See Groupe de Travail Interministériel sur la Lutte contre la Cybercriminalité ('Interministerial Working Group on Fighting Cyber-Criminality'), *op. cit.*, p.185.

more clearly distinguish those service providers that play 'an active role'[107] in the content published online, notably by means of referencing and classification services or even personalised recommendations sent to Internet-users[108]. As far as the CNCDH is concerned, the latter should be governed by a system of increased liability in the event that the content in question is ubiquitous in nature[109], and consequently bound by a series of obligations, themselves reinforced, such as the following:

- an obligation to preventively (proactively) detect content that is likely to constitute an offence relating to the abuse of freedom of expression[110] since service providers are technically better equipped than Internet-users to identify unlawful content, notably by means of algorithms based on semantic vectors and context[111];
- a corresponding obligation to quickly inform and cooperate with the public authorities to enable the perpetrators of offences relating to the public expression of hatred to be identified.

19. Secondly, it is worth reiterating that the civil and criminal liability of the hosting service provider is currently dependent upon their actual awareness of the unlawful activity or information in question (Articles 6 I., 2 and 6 I., 3 of the LCEN[112]). With regard to abuses of freedom of expression, they are, of course, obliged to put in place an "easily accessible and visible" reporting system for Internet-users (article 6 I., 7 paragraph 3 of the LCEN[113]), which is not always the case in practice[114].

---

[107] This is the criterion applied by the Court of Justice of the European Union on the grounds of Article 14 of Directive 2000/31/EU *on electronic commerce* (see notably CJEU, 12 July 2011, *L'Oréal & others v. E-Bay,* n°C-324/09).

[108] See Council of State, *Etude annuelle 2014, op. cit.* p.272 *et seq.*, which suggests defining the legal classification of platforms.

[109] In this respect, the EUCJ states that the role played by search engines renders data 'ubiquitous' since it can be consulted "instantly by an unlimited number of internet users throughout the world, irrespective of any intention on the part of the person who placed it in regard to its consultation beyond that person's Member State of establishment and outside of that person's control", (EUCJ 25 October 2011, *eDate Advertising GmbH & Others*, n°C-509/09 and C-161/10, §45; EUCJ 13 May 2014, *Google Spain SL, Google Inc v. AEDP M. Costeja Gonzales*, n°C-131/12, §80.

[110] Comp. Groupe de Travail Interministériel sur la Lutte contre la Cybercriminalité ('Interministerial Working Group on Fighting Cyber-Criminality'), *op. cit.*, p.185, which recommends that service providers (and hosting service providers, search engine providers and access providers in particular) be bound by a legal obligation with regard to preventive monitoring in order to detect unlawful content that is considered to be of a particularly serious nature and that technically lends itself to such detection. With this in mind, it is recommended that the offences listed in Article 6 I., 7 of the LCEN be targeted.

[111] See Berthier, T., *Haines numériques, Tribune publiée le 28 novembre 2014*, online at www.crif.org.; Corchia, D., (Concileo), *Audition du 16 décembre 2014.*

[112] Article 6 I., 2 of the LCEN provides that: "Both individuals and legal persons storing signals, written remarks, images, sounds or messages of any kind provided by the recipients of such services for the purpose of public information by means of online public communication services, even free of charge, cannot be held civilly liable for the activities or information stored at the request of a recipient of such services if they were not, in fact, aware of their unlawful nature or of any events and circumstances that might highlight this nature or if they have acted promptly to have the information in question removed or make it inaccessible as soon as they became aware of the aforementioned".
In accordance with Article 6 I., 3 of the LCEN, those acting as hosting service providers cannot be held criminally liable "owing to the information stored at the request of a recipient of such services if they were not, in fact, aware of the unlawful activity or information or if they have acted promptly to have the information in question removed or make it inaccessible as soon as they became aware of the aforementioned".

[113] Article 6 I., 7 paragraph 3 of the LCEN: "In light of the general interest associated with repressing the condoning of crimes against humanity, incitement to racial hatred and child pornography, those referred to above (hosting service providers and access providers) must contribute to fighting the spread of the offences listed in the fifth and eighth paragraphs of Article 24 of the law of 29 July 1881 on the freedom of the press and Article 227-23 of the French Criminal Code.
With this in mind, they must put in place an easily accessible and visible system enabling any individual to bring this type of information to their attention".

However, failure to comply with this obligation, which is criminally sanctioned[115], rarely results in criminal prosecution[116]. Moreover, it should be pointed out that such reporting has no direct impact on the hosting service provider being held liable for unlawful content since only a notification, governed by a very demanding protocol (see Article 6 I., 5 of the LCEN[117]), leads to the presumed acquisition of knowledge of the unlawful nature of the content on the part of the service provider[118]. As far as the CNCDH is concerned, it is important that reflection on the legal consequences of reporting be initiated. With this in mind, it might be useful to consider increasing the civil and criminal liability of the hosting service provider in the event of failure on their part to respond to a significant number of reports of obviously unlawful hateful content[119]. These new obligations are not, of course, intended to hinder freedoms of expression, innovation or enterprise.

20. Thirdly, as stated above and in addition to reporting, users have the option of notifying the hosting service provider of contentious facts. Furthermore, only in the event of regular notification can the hosting service provider be presumed aware of unlawful content and consequently held liable (article 6 I., 5 of the LCEN)[120]. This formality, which notably requires legal characterisation of the contentious facts and accurate identification of the hosting service provider, is difficult for often resourceless non-legal practitioners to complete[121]. As a result, associations generally step in and take over, whereas in actual fact, all citizens should be in a position to issue an 'LCEN notification' by themselves and with ease. As far as the CNCDH is concerned, it is therefore important that these different systems (reporting and notification)[122], which should not only be used to create a 'receipt acknowledgement' mechanism[123] but more importantly to enable users to liaise with the approved associations, be simplified and standardised as a matter of urgency.

---

[114] The Court of Appeal of Paris ruled that the system put in place for bringing unlawful content to the attention of Twitter is not sufficiently visible or accessible (CA Paris 12 June 2013, *UEJF c. Twitter Inc. (Sté),* n°13/06106, *Rec. Dalloz* 2013, p.1614, C. Manara note; *RSC* 2013, p.566, obs. J. Francillon).

[115] In accordance with Article 6 VI., 1 of the LCEN, the penalty incurred is one year's imprisonment and a €75,000 fine.

[116] Huet, J. and Dreyer, E., *Droit de la communication numérique, op. cit.,* p.130.

[117] Article 6 I., 5 of the LCEN: "Those referred to in 2 (hosting service providers) are presumed aware of the contentious facts in the event that they are notified of the following:
- the date of the notification;
- if the notifier is an individual: their surname, forename(s), profession, home address, nationality and date and place of birth; if the petitioner is a legal entity: its form, its name, the address of its head office and the body that represents it in legal matters;
- the name and address of the recipient or, in the case of a legal entity, its name and its head office address;
- a description of the contentious facts and their precise location;
- the reasons for which the content should be removed, including reference to legal provisions and evidence of the facts;
- a copy of the correspondence addressed to the author or publisher of the contentious information or activity requesting that it be halted, removed or modified, or evidence that it was not possible to contact the author or publisher".

[118] See TGI Paris 3rd Chamber 13 January 2011, *Légipresse* 2011, p.213.

[119] See Souffron, J.-B. (General Secretary of the French National Digital Council), *Audition du 3 février 2015.*

[120] See Cass. 1st Civ., 17 February 2011, *Rec. Dalloz* 2011, p.1113, C. Manara note, which states that "notification issued by virtue of the law of 21 June 2004 must include all of the elements outlined in the present text". It goes on to claim that "the Court of Appeal, which has noted that the information stated on the formal notice was insufficient under the terms of Article 6-1-5 of the law to fulfil the notifier's obligation to describe and locate the contentious facts (…), has consequently concluded that the hosting service provider could not be blamed for any breach of the obligation to promptly remove the unlawful content or prohibit access thereto".

[121] Lefranc, C. (LICRA), *Audition du 4 septembre 2014*; Monfort, J.-Y., *Audition du 25 septembre 2014.*

[122] See Conseil National du Numérique ('French National Digital Council') 17 December 2013, *Avis n° 2013-6 sur les contenus et les comportements illicites en ligne,* online at www.cnumerique.fr.

[123] See Falque-Pierrotin, I., *Audition du 21 janvier 2015.*

21. Fourthly and finally, Article 6 II. of the LCEN regarding the identification of those who have contributed to the creation of unlawful content does not provide for any legal procedure in favour of the user as the victim. Article 6 I., 8 of the LCEN does, of course, provide that the judicial authority may order the hosting service provider or, failing this, the access provider, by means of summary or ex-parte proceedings, to take any measures likely to prevent or put an end to any damages caused by the content of an online public communication service, but no such provision exists in paragraph II. This situation is extremely unfortunate since obtaining identification details can be essential to issuing an LCEN notification or implementing substantive measures. The CNCDH would therefore immediately recommend an extension of Article 6 II. of the LCEN in this respect.

C. OUTLINING AND IMPLEMENTING AN AMBITIOUS AND PROACTIVE PROSECUTION POLICY

22. The high cost and complexity of investigative acts[124] combined with the lack of resources allocated to the PHAROS platform are a significant hindrance to the effectiveness of the criminal response to online hate speech. With this in mind, it is essential that the State outline an ambitious and proactive criminal policy and allocate sufficient resources thereto if the situation is to be remedied, which will require a number of improvements, including the following, to be made:
    - more widespread use of inquiries under aliases[125] by surrounding it with all of the safeguards guaranteeing the protection of fundamental rights for the purpose of being able to identify the authors of unlawful content in the absence of cooperation on the part of hosting service providers or the circulation of such content on the Tor network or on the 'dark net';
    - reinforced European and international cooperation for the purpose of tracing and identifying those that host sites that circulate unlawful content;
    - an increase in the human, technical and material resources allocated to the PHAROS reporting platform[126] and the structuring of report traceability, with the obligation to inform the reporter of the legal action taken as a result of their report;
    - ensuring consistency between reporting platforms with a view to improving the accessibility, visibility and functionality thereof;
    - structuring the sharing of information at both national and local levels by means of regular meetings involving institutional players, Internet companies and civil society with a view to taking coordinated action in order to combat hate speech and improve understanding of public action[127];
    - calling Public Prosecutor's offices to action by means of general instructions and circulars outlining a clear strategy for public action with regard to prosecuting racist, anti-Semitic and xenophobic offences[128], notably requiring prosecutors to call for convictions to be legally published online [129];
    - the use of alternatives to prosecution with the creation of special modules incorporating hate speech on the Internet as part of community rehabilitation programmes[130] and the use of alternatives to imprisonment with the creation of

[124] See on this matter Falque-Pierrotin, I., *op. cit.*, p.52.
[125] See on this matter the contribution of Quéméner, M. in CNCDH, *Rapport 2014. La lutte contre le racisme, l'antisémitisme et la xénophobie, op. cit.* See also Groupe de Travail Interministériel sur la Lutte contre la Cybercriminalité ('Interministerial Working Group on Fighting Cyber-Criminality'), *op. cit.*, p.237-238.
[126] See CNCDH, *Rapport 2010, op. cit.*, p.165.
[127] See Falque-Pierrotin, I. *op. cit.*, p.48; Charef, L. (CCIF), *Audition du 16 décembre 2014.*
[128] See Charpenel, Y., *Audition du 11 septembre 2014.*
[129] See CNCDH, *Rapport 2010, op. cit.*, p.165-166.
[130] Article 41-1 2° of the French Code of Criminal Procedure.

such modules as part of programmes designed to prevent perpetrators from reoffending and aimed notably at those sentenced to criminal restraint[131];
- the creation of special modules incorporating hate speech on the Internet as part of so-called compensation-sanction measures[132];
- extending the scope of jurisdiction of the *Commission d'Indemnisation des Victimes d'Infraction* ('Criminal Injuries Compensation Board', CIVI) and the guarantee fund to all offences relating to abuses of freedom of expression[133].

D. SUPPORTING AND PROMOTING THE EXPERTISE OF ASSOCIATIONS

23. The CNCDH would recommend greater involvement on the part of the public authorities in order to more effectively fight hate speech that represents a criminal offence or is likely to be a matter of civil liability. Associations are currently overwhelmed owing to a lack of engagement on the part of the State and have too few resources available to initiate complex and costly procedures[134]. They are not, therefore, in a position to rectify the asymmetry of power that exists between resourceless victims and the commercial corporations that provide Internet services. As a result, the CNCDH must salute the considerable efforts and exemplary devotion on the part of associations. It can only ask that the public authorities promote the expertise of associations and provide funding that would enable such bodies to fulfil their missions under proper conditions. Finally, cultural mediation and specialist prevention must be encouraged and supported by the public authorities.

III. HAVING ACCESS TO A RESPONSIVE AND INNOVATIVE INTERNET REGULATORY BODY

24. The State must fully commit to the issue of fighting hate speech on the Internet by establishing a strong, specialist and coherent presence as the only body that can regain sovereignty on the matter. This is all the more essential given that the proliferation of hate speech online has the ability to give rise to mass litigation. It is therefore vital that there be a body that can take preventive action and provide a fast and appropriate response. With this in mind, the CNCDH would recommend that either an existing independent administrative authority (IAA)[135] or one established for this purpose be entrusted with the general mission of protecting rights and freedoms in the digital sphere. Such a body should be responsive and innovative, as is its target, the digital world. Whilst it is perfectly aware of the current leaning towards the need on the part of IAAs to make savings and streamline their activities[136], the CNCDH is nevertheless convinced that such an

[131] Article 131-8-2 of the French Criminal Code and Articles 713-42 and following of the French Code of Criminal Procedure.
[132] Articles 131-3, 8° of the French Criminal Code and 12-1 of ruling n°45-174 of 2 February 1945 regarding childhood delinquency.
[133] See Goldman, S., *op. cit.*, p.177.
[134] It is worth remembering that authors of unlawful content and hosting service providers are often located abroad, which requires legal procedures to be followed in the country in which they are based or in which they have their head office. Furthermore, a screenshot is not considered to be sufficient proof. In order to initiate a legal procedure it is necessary to have a bailiff's report on the unlawful online content drawn up (see Goldman, S. *op. cit.*, p.176).
[135] There are at least three administrative authorities whose field of jurisdiction could be extended, these being the CSA, the HADOPI and the CNIL.
[136] See *Rapport d'information du Comité d'évaluation et de contrôle des politiques publiques de l'Assemblée nationale sur les autorités administratives indépendantes*, Volume I., October 2010; *Rapport d'information de*

institution would be entirely justified. The aim, of course, is to restore the online presence of the public authorities by means of a decriminalisation approach, with the judicial authority having to intervene only in the secondary instance, in the event that the solution provided by the IAA fails to achieve the desired effect[137]. In this respect, it must be pointed out that prioritising the effectiveness of the administrative response in this way does not result in any decriminalisation since an element of criminal offence remains. Indeed, as has already been stated, the issue here is not one of repealing offences relating to abuses of freedom of expression.

A. PUTTING AN END TO INSTITUTIONAL UNREST BY APPOINTING A SINGLE, INDEPENDANT AND IMPARTIAL REPRESENTATIVE

25. There is currently neither an interministerial delegation nor an independent administrative authority that serves as a reference body in the field of cyber-criminality[138]. Following on from the Robert report, the CNCDH can only observe the fragmented nature of the organisations, initiatives and partnerships established between the public authorities and certain private service providers[139]. This fragmentation of State intervention plays into the hands of commercial corporations claiming alien status, to the detriment of those who willingly comply with the legal obligations by which they are bound. It is unacceptable for purely economic factors to take precedence over the public interest, which demands that cyber-criminality and therefore the proliferation of online hate speech be effectively combated[140]. With this in mind, the CNCDH believes there is an urgent need to establish a single point of contact for all Internet players, both institutional and non-institutional. Public regulation, in the form of a single independent representative responsible for protection and prevention where Internet-users are concerned and for ensuring that a series of obligations common to both users and companies are fulfilled, would appear to be the most appropriate solution.

26. Above and beyond this, the CNCDH wishes to reiterate that the protection of the public interest could not permit the introduction of a 'private censorship' system whereby the technical service provider would be the only party with the power to remove content with no possible recourse[141]. Clearly, neither should it be a matter of establishing a State system for initially monitoring content posted online, as is the case with authoritarian and dictatorial regimes[142]. Such an option, which would disproportionately violate freedom of expression and the right to privacy, would

---

la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale du Sénat sur les autorités administratives indépendantes, June 2014.

[137] On the matter of decriminalisation see Lazerges, C., *Introduction à la politique criminelle*, L'Harmattan 2000; Jung, H., *Was ist Strafe ?*, Nomos 2002, p.68 *et seq*.

[138] See Groupe de Travail Interministériel sur la Lutte contre la Cybercriminalité ('Interministerial Working Group on Fighting Cyber-Criminality'), *op. cit.*, p.138 *et seq*.: "Whilst, with regard to developing the digital economy and fighting the digital divide, such matters are the responsibility of a specific ministerial department, the Interministerial Delegation of Economic Intelligence and the Delegation for Internet use, with regard to cyber defence the matter is entrusted to the General Secretariat for Defence, under the direct command of the Prime Minister, and with regard to technological security and the technical response to cyber attack such matters, at least in the case of companies deemed to be sensitive, fall within the jurisdiction of the French Network and Information Security Agency (ANSSI), also under the command of the Prime Minister, there is no comparable organisation for fighting cyber criminality, which is a matter that is dealt with jointly by the police and the justice system, along with various specialist administrative bodies, whilst the existing independent administrative bodies, the jurisdiction of which is often limited to a particular sector (personal data protection, online gaming, copyright protection, etc.), are not intended to play a unifying role".

[139] See Robert, M., *Audition du 3 décembre 2014*.

[140] Article 6 I., 7 of the LCEN.

[141] See Council of State, *Etude annuelle 2014, op. cit.*, p.225 *et seq*.

[142] See Achilléas, P., 'Internet et libertés', *op. cit.*, n°38.

inevitably result in the demise of the Internet[143]. This being the case, establishing a balance between protecting freedom of expression and protecting the public interest calls for impartial and analytical control on the part of an independent body as the only party with the ability to maintain a subtle balance between these two principles. The appearance of impartiality and independence could be guaranteed by an IAA with a more pluralist composition, combining representatives of civil society (associations and NGOs), representatives of commercial service providers and justice professionals.

B. INTRODUCING AN ANNUAL MISSION TO EVALUATE PUBLIC POLICIES DESIGNED TO COMBAT THE PROLIFERATION OF HATE SPEECH ON THE INTERNET

27. The proposed IAA could easily establish itself in the institutional landscape alongside an interministerial delegation, be this a new delegation that would be created to have general jurisdiction in the field of cyber criminality[144] or even the Interministerial Delegation for the Fight Against Racism and Anti-Semitism (DILCRA), which is already developing innovative missions as part of the fight against online racism[145]. As far as the CNCDH is concerned, the IAA could provide an independent appraisal of the public policies that the interministerial delegation would be responsible for implementing. The traditional separation of the functions of player and appraiser requires a bicephalous organisation. This appraisal of public action could notably give rise to the annual publication of a report.

C. CREATING AN ONLINE HATE SPEECH OBSERVATORY

28. The IAA could, owing to its special position and as a result of a dialogue established and maintained with companies, Internet-users and the public authorities, serve as an observatory for the purpose of better understanding manifestations of hatred on the Internet, as well as developments therein and systems for combating such manifestations. Such observation would notably be fuelled by the qualitative and quantitative reports produced by the PHAROS platform, by the conducting of victimhood surveys and studies and research carried out by a scientific college, and by the creation of a monitoring unit. In order for the work undertaken by the observatory to be operational, the various players concerned, both public and private, would be required to produce a report on the measures and systems put in place. In this respect, the IAA could centralise information provided by private service providers in relation to unlawful activities and the resources devoted to fighting the latter, as is required by Article 6 of the LCEN[146]. This monitoring on the part of the independent authority would offer the advantage of capitalising on an intricate knowledge of the phenomena in question and examining in depth the systems put in place by commercial enterprises to fight such phenomena. As a result, the CNCDH recommends that an annual assessment of the fulfilment on the part of private service providers of their legal obligations, which would serve to increase both the visibility and, *in fine*, by means of 'brand image' and the upward levelling effect, the effectiveness of the system designed to fight hate speech.

[143] See Mbongo, P., *Audition du 23 octobre 2014.*
[144] See Recommendation n°7 of the *Rapport Robert* regarding the creation of an Interministerial Delegation for the Fight Against Cyber-Criminality (Interministerial Working Group on Fighting Cyber-Criminality, *op. cit.*, p.141).
[145] See on this matter the contribution of the DILCRA in CNCDH, *Rapport 2014. La lutte contre le racisme, l'antisémitisme et la xénophobie, op. cit*.
[146] See *supra*.

There are also plans to certify those sites that do respect fundamental rights and freedoms[147].

D. DEVELOPPING PARTNERSHIPS WITH THE AIM OF PRODUCING A CONSISTENT AND COHERENT NORMATIVE FRAMEWORK

29. The IAA could implement a joint regulation initiative where private service providers are concerned as part of an approach that encourages partnership and dialogue rather than confrontation[148]. The outlining of a series of mutually accepted rules is a measure of greater effectiveness, provided that they are negotiated with a single representative.

30. First and foremost, partnerships could focus on outlining a series of general conditions of use that comply with the laws in force and respect fundamental rights and freedoms[149], which are unfortunately often somewhat abstruse and difficult to access. In order to better guarantee freedom of expression, it is essential that the criteria for removing content be clarified and explicitly outlined in a series of clear and accessible general conditions of use. The CNCDH must reiterate the fact that the Committee of Ministers of the Council of Europe adopted a Recommendation on a Guide to human rights for Internet users, which states that "human rights, which are universal and indivisible, and related standards, prevail over the general terms and conditions imposed on Internet users by any private sector actor"[150].

31. Secondly, partnerships could be established to encourage the adoption of charters focusing on outlining editorial rules for websites or even increasing coherence between the various unlawful content reporting platforms that are currently being developed in an entirely uncoordinated manner. The CNCDH would emphasise the importance of working on producing a consistent and coherent normative framework that applies to all digital professions, contrary to the current situation that has arisen as a result of fragmented State intervention. Indeed, the idea that certain companies should be able to take advantage of their economic power to negotiate reduced obligations or even avoid any obligation whatsoever when others are obliged to comply is not only incomprehensible and counter-productive but also anti-competitive. Under no circumstances should this partnership-based approach be allowed to resemble any resignation on the part of the State towards any of the economic players concerned.

E. DIVERSIFYING AND INDIVIDUALISING RESPONSES TO HATE SPEECH ON THE INTERNET

32. Soft law has limits that the restrictive rules of law must then compensate for, most notably in the case of abuses of freedom of expression. The CNCDH cannot emphasise too strongly the dangers associated with blind and 'standardised'

[147] Take, for example, the 'net+sûr' certification launched by the AFA in 2005 with the aim of guaranteeing a parental control tool, access to information designed to protect children and one-click access to a form for reporting abuse (see http://www.afa-france.com/netplussur.html).

[148] See Dérieux, E., 'Régulation de l'internet', *op. cit.*, p.98, who writes: "Is there any form of self-regulation or reference to ethics or morality that might serve to control the shared use of the Internet by professionals and amateurs alike? Would it not primarily facilitate self-defence and self-justification for some? Are economic concerns and industrial interests not likely to take precedence over all else?".

[149] In this respect we might refer to the online hosting service and Internet access provider charter on combating certain content produced by the French Access Providers Association (AFA), the so-called 'undesirable content charter', signed in June 2004 at the same time as the promulgation of the LCEN (see http://www.afa-france.com/charte_contenusodieux.html).

[150] Committee of Ministers of the Council of Europe 16 April 2014, *Recommendation CM/Rec (2014) 6 on a Guide to human rights for Internet users.*

suppression in relation to hate speech. Indeed, the response has to be appropriate to the offender's profile, since a case of mere negligence on the part of the technical service provider will not call for the same reaction as the characterised defiance of a foreign company that refuses to comply with French obligations; likewise, an inappropriate use of language on the part of an Internet-user should not result in as harsh a punishment as would befit a considered and recurrent hate speech activist. With regard to mass disputes, the CNCDH believes it essential to diversify the responses provided with the emphasis on adopting a graded approach that takes into account the gravity and recurring nature of hateful remarks, ranging from decriminalisation to the initiation of criminal prosecution. With this in mind, the IAA could be entrusted with a range of powers, thus combining the obligations by which both private service providers and Internet-users are bound, and mechanisms designed to prevent and, in the event of failure only, suppress breaches thereof. In this respect, the CNCDH firmly believes that the response should be individualised, something that would require greater diversity in the range of tools available to the IAA which could result in the following:

- service providers who fail to fulfil their legal obligations, and those outlined in Article 6 of the LCEN in particular, being warned that this is the case, with the possibility of such a warning being published online if need be, thus encouraging the service provider to comply with the requirements of the law in order to protect their brand image;
- users being warned of any breach of obligations, this warning consisting of informing the Internet-user of the offence committed and the potential sanctions. At the same time, the IAA could develop an initiative designed to formulate counter-discourse, along the lines of the copyright protection initiative developed by the HADOPI, thus offering Internet-users, when the situation arises, alternatives to simplistic arguments, notably by means of the circulation of quantitative indicators[151];
- mediation between private service providers and Internet-users, be they authors or victims of unlawful content. In a relationship that all too often resembles the battle between David and Goliath, it is important that the economically weaker party be protected. It is currently difficult for the Internet-user to assert their observations in the event of a refusal to remove the unlawful content, silence on the part of the duly notified private service provider or even any removal of content that is considered to be abusive;
- the hosting service provider being issued with a formal notice demanding that they remove any obviously unlawful content or that they repost any lawful content;
- the hosting service provider being issued with a formal notice informing them of the information required to identify the author of unlawful content. In the absence of any response from the service provider, the IAA could refer the matter to the judge ruling on applications for interim measures.

33. Furthermore, a number of the hearings conducted at the CNCDH revealed that hosting service providers sometimes have difficulty assessing the 'obviously unlawful' nature of content[152], despite the fact that they are required by constitutional case law to remove such content[153]. Furthermore, the IAA could be entrusted with a legal intelligence mission, asked by hosting service providers to

[151] Such as the '*10 chiffres clés sur l'immigration en France*' published on the Government's website to mark the opening of the Museum of History and Immigration in December 2014, which discredits preconceived ideas regarding the number of immigrants in France, their origin and even their level of qualification (see http://www.gouvernement.fr/10-chiffres-qui-vont-vous-surprendre-sur-l-immigration-en-france).
[152] See Gay, C. and d'Arcy, N. (AFA), *Audition du 9 octobre 2014.* See also Roux, O., 'Le contenu manifestement illicite…n'est pas toujours évident', *RLDI* 2013, n°95, p.36 *et seq.*
[153] Const. Coun. 10 June 2004, n°2004-496 DC, considering n°9.

give its opinion and be responsible for managing a 'wastebin' designed to hold dubious content, that is a space reserved for the temporary storage of such content pending a court decision. It could, at the same time, be authorised to order the temporary delisting of dubious content.

34. With regard to the potential sanctioning power that could be granted to the IAA, this must be exercised in accordance with constitutional requirements. The Constitutional Council has asserted on a number of occasions that an administrative authority can be granted sanctioning power by law provided that it does not involve any deprivation of liberty and that it is exercised in combination with measures designed to safeguard constitutionally guaranteed rights and freedoms[154]. This sanctioning is all the more restricted, particularly with regard to freedom of expression and communication, since it "is a condition of democracy and one of the guarantees of respect for other rights and freedoms; (…) any impediment to the exercising of this freedom must be necessary, appropriate and proportionate to the objective being pursued"[155]. The Elders, reiterating the fact that Internet access is an integral part of freedom of expression, have consequently nullified the system with which the HADOPI Rights Protection Commission was entrusted, authorising it to suspend the offending Internet-user's access to the Internet having implemented the appropriate warning procedure. It is essential that the judicial authority be responsible for such a power[156]. With regard to our hypothesis, a judge could very well limit a subscriber's Internet access, whilst ruling without undue delay upon referral to the IAA following the unsuccessful issuing of formal notification.

35. As for the removal of content by the hosting service provider, this is considered to hinder both the free circulation of information and freedom of expression. This is particularly true with regard to an access provider blocking a site[157]. Indeed, any prior restriction on online expression will result in a heavy presumption of

[154] Const. Coun. 17 January 1989, n°88-248 DC: "the law may (...) grant the independent authority responsible for guaranteeing the exercising of freedom of audiovisual communication certain sanctioning powers deemed necessary to the fulfilment of its mission without detriment to the principle of the separation of powers", (considering n°27); Const. Coun. 28 July 1989, n°89-260 DC: "the principle of the separation of powers does not stand in the way of an administrative authority, acting in accordance with the prerogatives of public authority, exercising any sanctioning power any more than any principle or rule of constitutional value, provided, on the one hand, that the sanction that is likely to be imposed does not involve any deprivation of liberty, and on the other hand, that the exercising of sanctioning power is combined by law with measures designed to safeguard constitutionally guaranteed rights and freedoms" (considering n°6).

[155] Const. Coun. 10 June 2009, n°2008-580 DC: "Bearing in mind that the sanctioning powers introduced by the provisions criticized authorise the Rights Protection Commission, which is not a jurisdiction, to restrict or to withdraw subscribers' Internet access, as well as that of those who benefit from it; that the recognised expertise of this administrative authority is not limited to a particular category of person but rather extends to the population as a whole; that its powers can result in a restriction on the exercising by any person of their right to express themselves and to communicate freely, particularly from their own home; that, this being the case, and in light of the nature of the freedom guaranteed by Article 11 of the 1789 Declaration, the legislator could not, regardless of the guarantees governing the imposition of sanctions, entrust such powers to an administrative authority for the purpose of protecting the rights of copyright holders and related rights".

[156] Law n°2009-1311 of 28 October 2009 *on the criminal protection of literary and artistic property on the Internet*.

[157] The Constitutional Council has approved a system for the administrative blocking of a site for the purpose of fighting child pornography (Const. Coun. 10 March 2011, n°2011-625 DC: "the disputed provisions only give the administrative authority the power to restrict, in order to protect the Internet-user, access to online public communication services when and insofar as they are circulating images of child pornography; that the decision of the administrative authority is likely to be contested at any time and by any interested party before the competent court, or, if necessary, by means of summary proceedings; that, this being the case, its provisions provide for a conciliation that is not disproportionate between the aim of the constitutional value 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").

incompatibility with Article 10 of the ECHR[158], which is why the CNCDH believes it necessary for a judge to intervene to order and monitor the removal of unlawful content and the blocking of websites[159], since such measures are considered to seriously interfere with freedom of expression and communication[160]. More specifically, a magistrate could rule on summary proceedings within a short time frame of 48 or 72 hours, upon referral to the IAA. As previously stated, it is important that the judge intervene only in the secondary instance and that the matter be referred to them only after the publisher or hosting service provider has been formally notified by the IAA of the need to remove or republish the contentious content.

36. As far as the CNCDH is concerned, a site should only be blocked as a last resort since this measure is not technically reliable[161], owing to the risk of over-blocking and of the issue being circumvented by means of the consequent duplication of unlawful content from one site to another. This being the case, it is essential that the appropriate action be taken first and foremost with the hosting service provider. Only in the event that the latter is unknown or difficult to get hold of as a result of them being based abroad should action be taken against the access provider[162].

37. Finally, the IAA could be given a role to play in the enforcement and monitoring of conviction decisions – of both service providers and Internet-users - that it could be responsible for posting online. In order to prevent content that has been deemed unlawful from being recirculated, it could primarily be given the power to order any service provider to prevent such content from being reposted or duplicated. Still, as part of its mission to enforce and monitor court rulings, the IAA could be authorised to produce a list of sites to be blocked subject to the approval of the judicial authority whilst ensuring that said list is updated on a regular basis[163]. This option offers the significant advantage of avoiding multiple reports, LCEN notifications[164] and, where applicable, costly and complex proceedings.

---

[158] See the concurring opinion of judge Paulo Pinto de Albuquerque (under ECtHR 18 December 2012, *Ahmet Yildirim v. Turkey*, *op. cit.*), which refers to the case of *Banatan Books, Inc. v. Sullivan* (372 U.S. 58 (1963): "*Any system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity*").

[159] See French National Assembly, Commission *ad hoc* de Réflexion et de Propositions sur le Droit et les Libertés à l'Age du Numérique ('Ad hoc Commission on Law and Liberties in the Digital Age'), *Recommandation sur l'article 9 du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme*, which reiterates the fact that the "prerequisite to a court ruling would appear to be a vital principle with regard to respecting all of the interests represented when there are plans to block access to unlawful content on digital networks. Not only does this prerequisite constitute a strong guarantee of freedom of expression and communication but it is also designed to maintain neutrality in networks".

[160] See Const. Coun. 10 March 2011, n°2011-625 DC.

[161] See Esper, O., Maganza, F., and Guiroy, T. (Google France), *Audition du 25 septembre 2014.* The *Conseil National du Numérique* ('French National Digital Council') defended an identical position in its opinion on Article 9 of the bill designed to reinforce provisions regarding the fight against terrorism (*Avis n° 2014-3 sur l'article 9 du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme*, online at www.cnumerique.fr).

[162] Comp. Cass. 1st Civ., 19 June 2008, n°07-12.244, which claims that the prescription of measures designed to put an end to any discord is not conditional upon the preliminary implication of the hosting service provider. However, Article 6 I., 8 of the LCEN provides that the judicial authority may order the hosting service provider "or, failing this", the access provider, by means of summary or ex-parte proceedings, to take "any measures likely to prevent or put an end to any damages caused by the content of an online public communication service".

[163] See Imbert-Quaretta, *M., Les outils opérationnels de prévention et de lutte contre la contrefaçon en ligne. Rapport à Madame la Ministre de la culture et de la communication,* May 2014, p.23 *et seq.*

[164] It should be noted that the Court of Cassation has ruled, by virtue of Articles 6 I., 2, 6 I., 5 and 6 I., 7 of the LCEN, that a new notification that complies with the formalities outlined in the aforementioned Article 6 I., 5 must be issued every time the unlawful content reappears. In the event that the hosting service provider were

IV. ADOPTING A NATIONAL DIGITAL EDUCATION AND CITIZENSHIP PLAN

38. A truly inclusive information society should enable all citizens to acquire the skills they need to be able to understand and interact online, as outlined in the requirements of the fundamental right to education, recognised notably by Article 13 of the International Covenant on Economic, Social and Cultural Rights[165]. Online communication is a fundamental freedom, but also a responsibility that requires a certain amount of learning[166]. The CNCDH believes that it is essential that a national action plan[167], focusing notably on digital education and citizenship, be implemented and involve the main ministries concerned (the Secretary of State for Digital Affairs, the Ministry of National Education, the Ministry of the Interior, the Ministry of Justice and the Secretary of State for Family Affairs), the *Conseil National du Numérique* ('French National Digital Council'), representatives of the education sphere and of family life, associations and Internet players and users. This action plan could focus on the following:
    - promoting 'digital humanities' by means of support for innovation with regard to creating new participation and deliberation procedures designed to reinforce a sense of citizenship[168];
    - promoting free and responsible speech by outlining a series of codes of conduct aimed at Internet-users;
    - conducting universal information campaigns (TV/Internet) on the issue of preventing hate speech[169];
    - the implementation of initiatives designed to raise awareness among and provide information for parents to encourage them to be vigilant with regard to both their educational role in the field of digital citizenship and to their own responsibilities in terms of their child's use of the Internet[170]. The CNCDH wishes to emphasise this recommendation in particular since younger generations often have a much better command of computing tools and new technologies than older generations[171];
    - incorporating an element of specific training relating to the Internet and the civic use thereof, as well as the more general codes of practice that should be adopted, into national education curricula[172];
    - encouraging national education and players in civil society to promote an informed use of the Internet that will enable both young and old alike to distinguish between good and bad information so that they may independently form their own opinion;
    - producing educational tools designed for all of the audiences concerned (users, parents, children, teachers, etc.);

---

to act promptly by removing the unlawful content in question (in this instance an offending image) or making it inaccessible without further notification, this would result in them being bound by a general obligation to monitor content (Cass. 1st Civ., 12 July 2012, n°11-151.165 and 11-151.188).

[165] Achilléas, P., 'Une société mondiale de l'information inclusive comme préalable à la formation des opinions publiques' in Lepage, A. (dir.), *L'opinion numérique, op. cit.*, p.121.

[166] See Schmidt, P. (INACH), *Audition du 4 septembre 2014.*

[167] See Economic, Social and Environmental Council (ESEC) 13 January 2015, *op. cit.*, p.72, which calls for the Government to make digital education the 'major national cause for 2016'.

[168] See Wieviorka, M., *op. cit.*, p.41.

[169] See Falque-Pierrotin, I., *op. cit.*, p.54.

[170] See Falque-Pierrotin, I., *op. cit.*, p.55.

[171] See Octobre, S. (French Minister of Culture and Communication/General Secretariat/Department of Studies, Forecasting and Statistics), *Deux pouces et des neurones. Les cultures juvéniles de l'ère médiatique à l'ère numérique*, La Documentation Française 2014.

[172] See Falque-Pierrotin, I., *op. cit.*, p.54.

- increasing both the ability of associations involved in fighting racism, anti-Semitism and xenophobia to take action and the synergies that exist between such associations, notably by means of a special purpose grant[173];
- outlining and developing, in conjunction with civil society, 'counter-discourse' aimed at both young and old alike[174]. In this respect, the CNCDH must salute dynamic and innovative initiatives such as the *Pousse ton cri* campaign, whereby a group of associations (the LICRA, the MRAP, SOS Racisme and the UEJF) invited both younger and older Internet-users to spontaneously express their intolerance of hatred in videos that were then posted online.

SUMMARY OF PRIMARY RECOMMENDATIONS

Recommendation n°1: The CNCDH recommends that public authorities improve the tools making it possible to establish the extent of the proliferation of hate speech on the Internet, notably through the introduction of statistical tools, with a specific breakdown of offences committed on or via the Internet, and the funding of research in the field.

Recommendation n°2: The CNCDH recommends that the French State implement strong diplomatic measures to have those States hosting sites that publish hate speech sign and ratify Additional Protocol n°189 of the Council of Europe's Convention on Cybercrime dealing specifically with racism and anti-Semitism.

Recommendation n°3: The CNCDH recommends outlining the territorial scope of Article 6 of the French law on trust in the digital economy (LCEN), the provisions of which should apply to any company conducting any form of economic activity in France.

Recommendation n°4: The CNCDH recommends that the State stimulate the French digital industry and support innovation in the field. A policy designed to hold companies accountable with regard to respecting human rights, and the French understanding of freedom of expression in particular, is also crucial in the current context.

Recommendation n°5: The CNCDH recommends that the public authorities promote the expertise of associations and provide funding that would enable such bodies to fulfil their mission of fighting racism, anti-Semitism and xenophobia under proper material conditions.

Recommendation n°6: The CNCDH solemnly recommends that any offences relating to abuses of freedom of expression continue to be governed by the law of 29 July 1881 *on the freedom of the press*.

Recommendation n°7: The CNCDH recommends that certain legislative improvements be made in order to more effectively combat the proliferation of hate speech posted on the Internet by non-professional Internet-users and facilitate victims' access to justice, including the following:

- improving the intelligibility and understanding of the provisions of the law of 29 July 1881, particularly defining and updating the notions of public space and

[173] See Falque-Pierrotin, I., *op. cit.*, p.57.
[174] Over the course of the hearings conducted at the CNCDH, the *La Quatradure du Net* ('Squaring of the Net') association (J. Zimmermann, *Audition du 2 octobre 2014*; F. Tréguer, *Audition du 9 octobre 2014*) and *Renaissance Numérique* ('Digital Renaissance') (G. Buffet, *Audition du 2 octobre 2014*) in particular emphasised the need to outline such 'counter-discourse'. This matter was also addressed by P. Cartes (Twitter) and D. Reyre (Facebook France) during the hearings of 2 October 2014.

private space in Web 2.0 to reflect new types of digital communities and networks;
- considering the digitisation of procedures (and of summons and notifications in particular); simplifying and facilitating summary procedures, notably through the introduction of a digital summary judgement (rather than maintaining various summary judgements on the matter). Generally speaking, it is important that the procedural chain, beginning with LCEN reporting and notification systems (standardisation of said systems/enabling users to liaise with the approved associations/improving the quality of the reports filed/acknowledging receipt), right through to the possibility of lodging complaints online, be clarified and simplified as a matter of urgency;
- introducing a right to reply on the Internet in favour of anti-racism associations;
- giving the judge the power to order that a site cease to operate, in the same vein as the possibility of suspending a newspaper for 3 months in the event of incitement to racial hatred;
- giving the judge the power to order the cessation of an online communication service for any offence relating to abuses of freedom of expression;
- initiating reflection on the relevance of increasing the statute of limitations;
- considering the possibility of holding legal entities criminally liable, aside from press organisations.

Recommendation n°8: The CNCDH recommends clarifying and more clearly distinguishing those Internet service providers that play 'an active role' in the content published online, notably by means of referencing and classification services or even personalised recommendations for Internet-users. As far as the CNCDH is concerned, the latter should be governed by a system of increased liability in the event that the content in question is ubiquitous in nature, and consequently bound by a series of obligations, themselves reinforced, such as the following:

- an obligation for such service providers to preventively (proactively) identify unlawful acts since they are technically better equipped to identify unlawful content;
- a corresponding obligation to quickly inform and cooperate with the public authorities to enable the perpetrators of offences relating to the public expression of hatred to be identified.

Recommendation n°9: The CNCDH recommends that reflection on the legal consequences of reporting based on Article 6 I., 7 of the LCEN be initiated. With this in mind, it might be useful to consider increasing the civil and criminal liability of the hosting service provider in the event of failure on their part to respond to a significant number of reports of obviously unlawful hateful content. These new obligations are not, of course, intended to hinder freedoms of expression, innovation or enterprise.

Recommendation n°10: The CNCDH recommends that Article 6 II. of the LCEN sanction the possibility of the user requesting that the judge, by means of summary or ex-parte proceedings, provide information relating to the identification of those who have contributed to the creation of unlawful content.

Recommendation n°11: The CNCDH recommends that the public authorities outline and implement a proactive policy designed to suppress hate speech on the Internet, which will require a number of improvements, including the following, to be made:

- an increase in the use of inquiries under aliases by surrounding it with all of the safeguards guaranteeing the protection of fundamental rights for the purpose of being able to identify the authors of unlawful content in the absence of

cooperation on the part of hosting service providers or the circulation of such content on the Tor network or on the 'dark net';
- reinforced European and international cooperation for the purpose of tracing and identifying those that host sites that circulate unlawful content;
- an increase in the human, technical and material resources allocated to the PHAROS reporting platform and the structuring of the traceability of reports, with the obligation to inform the reporter of the legal action taken as a result of their report;
- ensuring consistency between reporting platforms with a view to improving the accessibility, visibility and functionality thereof;
- structuring the sharing of information at both national and local levels by means of regular meetings involving institutional players, Internet companies and civil society with a view to taking coordinated action in order to combat hate speech and improve understanding of public action;
- calling Public Prosecutor's offices to action by means of general instructions and circulars outlining a clear strategy for public action with regard to prosecuting racist, anti-Semitic and xenophobic offences, notably requiring prosecutors to call for convictions to be legally published;
- the use of alternatives to prosecution with the creation of special modules incorporating hate speech on the Internet as part of community rehabilitation programmes and the use of alternatives to imprisonment with the creation of such modules as part of programmes designed to prevent perpetrators from reoffending and aimed notably at those sentenced to criminal restraint;
- the creation of special modules incorporating hate speech on the Internet as part of so-called compensation-sanction measures;
- extending the scope of jurisdiction of the *Commission d'Indemnisation des Victimes d'Infraction* ('Criminal Injuries Compensation Board', CIVI) and the guarantee fund to all offences relating to abuses of freedom of expression.

Recommendation n°12: The CNCDH recommends that an independent administrative authority (IAA) be created and that such a body be flexible, responsive and innovative, as is its target, the digital world. This IAA would be responsible for the following:

- providing an initial individual response following reports of unlawful content;
- developing partnerships with private service providers to encourage the production of charters (focusing notably on editorial rules for websites and increasing coherence between reporting platforms) and the outlining of a series of general conditions of use that comply with the laws in force and respect fundamental rights and freedoms;
- serving as an observatory for the purpose of better understanding manifestations of hatred on the Internet, as well as developments therein and systems for combating such manifestations;
- performing a legal intelligence role. The IAA could therefore be asked by hosting service providers to give its opinion in the event of any doubt regarding the unlawful nature of any content and be responsible for managing a 'wastebin' designed to hold dubious content, that is a space reserved for the temporary storage of such content pending a court decision;
- providing an appraisal of the public policies implemented for the purpose of fighting hate speech on the Internet by means of the annual publication of a report;
- certifying those sites that do respect fundamental rights and freedoms.

Recommendation n°13: The CNCDH recommends that responses be graduated and is particularly keen that they should be individualised, something that would require greater

diversity in the range of tools available to the IAA, which could then result in the following:

- service providers who fail to fulfil their legal obligations, and those outlined in Article 6 of the LCEN in particular, being warned that this is the case, with the possibility of such a warning being published online if need be, thus encouraging the service provider to comply with the requirements of the law in order to protect their brand image;
- users being warned of any breach of obligations by informing the Internet-user of the offence committed and the potential sanctions;
- mediation between private service providers and Internet-users;
- the hosting service provider being issued with a formal notice demanding that they remove any obviously unlawful content or that they repost any lawful content;
- the hosting service provider being issued with a formal notice informing them of the information required to identify the author of unlawful content. In the absence of any response from the service provider, the IAA could refer the matter to the judge ruling on applications for interim measures;
- the temporary delisting of any dubious content once it has been reported;
- the matter being referred to the judge ruling on applications for interim measures with a view to suspending the offending Internet-user's access to the Internet following the unsuccessful issuing of formal notification;
- the matter being referred to the judge ruling on applications for interim measures with a view to having the unlawful content removed by the hosting service provider following the unsuccessful issuing of formal notification;
- the matter being referred to the judge ruling on applications for interim measures with a view to having a website blocked by an access provider, it being specified that, owing to technical complications, this measure should be adopted only as a last resort.

Recommendation n°14: The CNCDH recommends that the IAA have a role to play in the enforcement and monitoring of conviction decisions that it could be responsible for posting online. In order to prevent content that has been deemed unlawful from being recirculated, it could primarily be given the power to order any service provider to prevent such content from being reposted or duplicated. Still as part of its mission to enforce and monitor court rulings, the IAA could be authorised to produce a list of sites to be blocked subject to the approval of the judicial authority whilst ensuring that said list is updated on a regular basis.

Recommendation n°15: The CNCDH recommends adopting a national action plan, focusing notably on digital education and citizenship and involving the main ministries concerned (the Secretary of State for Digital Affairs, the Ministry of National Education, the Ministry of the Interior, the Ministry of Justice and the Secretary of State for Family Affairs), the *Conseil National du Numérique* ('French National Digital Council'), representatives of the education sphere and of family life, associations and Internet players and users. This action plan could focus on the following:

- promoting 'digital humanities' by means of support for innovation with regard to creating new participation and deliberation procedures designed to reinforce a sense of citizenship;
- promoting free and responsible speech by outlining a series of codes of conduct aimed at Internet-users;
- conducting universal information campaigns (TV/Internet) on the issue of preventing hate speech;

- the implementation of initiatives designed to raise awareness among and provide information for parents to encourage them to be vigilant with regard to both their educational role in the field of digital citizenship and to their own responsibilities in terms of their child's use of the Internet;
- incorporating an element of specific training relating to the Internet and the civic use thereof, as well as the more general codes of practice that should be adopted, into national education curricula;
- producing educational tools designed for all of the audiences concerned (users, parents, children, teachers, etc.);
- increasing the ability of associations involved in fighting racism, anti-Semitism and xenophobia to take action, as well as the synergies that exist between such associations, notably by means of a special purpose grant;
- outlining and developing, in conjunction with civil society, 'counter-discourse' aimed at both young and old alike.

LIST OF PEOPLE HEARD

Mr Christopher Abboud, Head of Communications at Twitter France (2 October 2014);

Mr Nicolas d'Arcy, Legal Adviser and Content Analyst at the *Association des Fournisseurs d'Accès et de Services Internet* ('Association of Access and Internet Service Providers') (9 October 2014);

Mr Anton'Maria Battesti, representative of Facebook France (2 October 2014);

Mr Guillaume Buffet, Chairman of the *Renaissance Numérique* ('Digital Renaissance') think tank (2 October 2014);

Mrs Patricia Cartes, Global Head of Online Safety Outreach at Twitter (2 October 2014);

Mrs Lila Charef, Legal Officer at the *Collectif Contre l'Islamophobie en France* ('Anti-Islamophobia in France Collective') (16 December 2014);

Mr David Corchia, founder of CONCILEO (16 December 2014);

Mr Yves Charpenel, First Advocate-General at the Court of Cassation (11 September 2014);

Mr Thomas Dautieu, Assistant Director of Programmes at the *Conseil Supérieur de l'Audiovisuel* ('French Higher Council for the Audiovisual Sector') (20 November 2014);

Mr Emmanuel Derieux, Professor of Information and Communication Sciences at the University Paris 2 (27 November 2014)

Mrs Nadia Doghramadjian, Human Rights League of France (4 September 2014);

Mr Emmanuel Dreyer, Professor at the University Paris 1 (23 October 2014);

Mr Olivier Esper, representative of Google France and of the *Association des Services Internet Communautaires* ('Association of Community Internet Services', ASIC) (25 September 2014);

Mrs Isabelle Falque-Pierrotin, President of the CNIL (21 January 2015);

Mrs Christiane Féral-Schuhl, former President of the Bar of Paris, co-president of the *Commission de Réflexion et de Propositions sur le Droit et les Libertés à l'Age Numérique* ('Commission on Law and Liberties in the Digital Age') at the French National Assembly (23 October 2014)

Mrs Carole Gay, Head of Legal Affairs at the *Association des Fournisseurs d'Accès et de Services Internet* ('Association of Access and Internet Service Providers') (9 October 2014);

Mrs Sabrina Goldman, lawyer, LICRA (4 September 2014);

Mr Thibault Guiroy, representative of Google France and of the *Association des Services Internet Communautaires* ('Association of Community Internet Services', ASIC) (25 September 2014);

Mr Yvan Kagan, CFDT (4 September 2014);

Mr Marc Knobel, researcher at the CRIF (4 September 2014);

Police Commander Pierre-Yves Lebeau, Head of the PHAROS Division of the sub-directorate for fighting cyber criminality / OCLCTIC (Ministry for the Interior) (25 September 2014);

Mrs Charlotte Lefranc, Head of Legal Affairs at LICRA (4 September 2014);

Mr Benoît Louvet, lawyer, LICRA (4 September 2014);

Mr Florian Maganza, representative of Google France and of the *Association des Services Internet Communautaires* ('Association of Community Internet Services', ASIC) (25 September 2014);

Mr Pascal Mbongo, Professor at the University of Poitiers (23 October 2014);

Mr Jean-Yves Monfort, Counsellor of the Court of Cassation, member of the CNCDH (25 September 2014);

Mrs Annabelle Philippe, Vice-Prosecutor responsible for matters relating to the press and the protection of liberties at the District Court of Paris (11 September 2014);

Mr Guillaume du Puy-Montbrun, Special Adviser to the President of the *Conseil Supérieur de l'Audiovisuel* ('French Higher Council for the Audiovisual Sector') (20 November 2014);

Mrs Myriam Quéméner, Advocate-General at the Court of Appeal of Versailles (11 September 2014);

Mrs Delphine Reyre, Director of Public Affairs at Facebook for France and Southern Europe (2 October 2014);

Mr Philippe Schmidt, lawyer, President of the International Network Against Cyber Hate (4 September 2014);

Mr Jean-Baptiste Souffron, General Secretary of the *Conseil National du Numérique* ('French National Digital Council') (3 February 2015);

Mr Felix Treguer, founding member of the *La Quadrature du Net* ('Squaring of the Net') association and doctoral candidate in political studies at the EHESS (9 October 2014)

Mr Éric Walter, Secretary-General of the High Authority for the Distribution of Works and the Protection of Rights on the Internet (HADOPI) (20 November 2014);

Mr Jérémie Zimmermann, founding member of the *La Quadrature du Net* ('Squaring of the Net') association (2 October 2014);

Mr Marc Hecker, researcher at the IFRI (27 November 2014)