FOLLOW-UP TO THE COMPARATIVE STUDY ON "BLOCKING, FILTERING AND TAKE-DOWN OF ILLEGAL INTERNET CONTENT"

Stéphanie De Dycker

LL.M., Legal Adviser, Swiss Institute of Comparative Law

REPORT

The present research provides an update to this study and reflects the developments in law and practice of France that have taken place from October 2015 till October 2020.

FRANCE

1. Sources

In December 2015 the Council of Europe published a Comparative study on blocking, filtering and take-down of illegal internet content, as carried out by the Swiss Institute of Comparative Law (the 2015 Comparative study). The present research provides an update to this study and reflects the developments in law and practice of France that have taken place from October 2015 till October 2020.

France is party to all Council of Europe conventions in the field of internet governance, namely: the Cybercrime Convention, as well as its Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems; the Convention on the Prevention of Terrorism; the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse; and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, as well as its Additional Protocol regarding supervisory authorities and transborder data flows.[1] More recently, France has been among the first signatories of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[2] Also, as a member state of the Council of Europe and of the European Union, France has been involved in the adoption of two standard-setting documents of relevance for online content moderation: Recommendation of the Council of Europe Committee of Ministers

[1] Decree No. 2006-580 of 23 May 2006 promulgating the Convention on Cybercrime, drawn up in Budapest on 23 November 2001, Official Gazette of the French Republic (JORF), 24 May 2006; Decree No. 2006-597 of 23 May 2006 promulgating the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, drawn up in Strasbourg on 28 January 2003, JORF, 27 May 2006; Decree No. 2008-1099 of 28 October 2008 promulgating the Council of Europe Convention on the Prevention of Terrorism (together with the appendix), adopted in Warsaw on 16 May 2005, signed by France on 22 May 2006, JORF, 30 October 2008; Decree No. 2011-1385 of 27 October 2011 promulgating the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (together with a declaration and a reservation), signed in Lanzarote on 25 October 2007, JORF, 29 October 2011; Law No. 82-890 of 19 October 1982 promulgating the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted in Strasbourg on 28 January 1981, JORF, 20 October 1982, 3163; Law No. 2007-301 of 5 March 2007 authorising the approval of the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, adopted in Strasbourg on 8 November 2001, JORF, 7 March 2007.

[2] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS.223, open for signature by the Contracting States to Treaty ETS 108 in Strasbourg on 10 October 2018.

CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries[3] and Recommendation (EU)2018/334 on measures to effectively tackle illegal content online, adopted by the European Commission on 1 March 2018.[4]

Matters related to blocking, filtering and take-down/removal of illegal internet content are governed in France by different **laws and regulations** which vary depending on the grounds for application of these restrictive measures. Law 575-2004 of 21 June 2004 on ensuring confidence in the digital economy (LCEN)[5] remains the main legislative text governing blocking and removal of illegal content from the internet. It provides that both judicial and executive authorities may order blocking, filtering or removal of certain types of internet content, subject to certain requirements. Since its amendment by Law 2011-267 of 14 March 2011 on domestic security guidance and planning, known as LOPPSI 2, and Law 2014-1353 of 13 November 2014 on scaling up counter-terrorism provisions, the LCEN has undergone several additional legislative revisions which will be discussed in this update report.

In particular, between 2015 and 2020 several laws have been adopted to extend the internet hosting services and internet service providers' (ISP) obligation to cooperate in cases involving specific types of illegal content. These include, notably, content related to proxenitism, human trafficking[6] and sexual harassment.[7] Law 2016-731 of 3 June 2016 reinforced the mechanism for blocking and take down of internet content by criminalising hindrance to the implementation of the relevant provisions of the LCEN.[8]

In addition, the widely debated new legislation regarding fight against hateful content on the internet has simplified the requirements for notification of illegal content by users and has laid basis for the establishment of a monitoring body to follow and analyse the developments regarding hateful online content.[9] Other measures initially intended by the Government (see sections 2.1.1. and 5) have not passed the constitutionality test due to augmented risks that they carried for freedom of expression.[10]

Also, in response to the terrorist attacks in France on 13 November 2015, the Government had declared the state of emergency, which was lifted on 30 October 2017. Law 2015-1501 of 20 November 2015[11] specified the measures applicable throughout this period, including those related to the blocking of certain types of illegal websites.

Other relevant sources have remained largely without change since 2015. In the field of intellectual

---

[3] Recommendation CM/Rec (2018)2 of the Committee of Ministers to member states on the roles and responsibilities of internet intermediaries, adopted by the Committee of Ministers on 7 March 2018 at the 1309th meeting of the Ministers' Deputies, available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14

[4] Recommendation (EU) 2018/334 on measures to effectively tackle illegal content online, available at: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_1170

[5] Law 575-2004 of 21 June 2004 on ensuring confidence in the digital economy, J.O., nr. 0143, 22 June 2004, 11168.

[6] Law 2016-444 of 13 April 2016 reinforcing the fight against the system of prostitution and to accompany prostitutes, J.O., 14 April 2016, available at: www.legifrance.gouv.fr (in French only)

[7] Law 2018-703 of 3rd August 2018 reinforcing the fight against sexual and sexist violence, J.O., 4 August 2018, available at: www.legifrance.gouv.fr (in French only)

[8] Law 2016-731 of 3 June 2016 reinforcing the fight against organized crime, terrorism and its financing and ameliorating the efficiency and guarantees of the criminal procedure, J.O., 4 June 2016, available at: www.legifrance.gouv.fr (in French only)

[9] Law 2020-766 of 24 June 2020 on fighting against hateful content on the internet, JORF, 25 June 2020, available at: www.legifrance.gouv.fr (in French only)

[10] Decision of the Constitutional Council no.2020-801 DC of 18 June 2020, available at: https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm

[11] Law 2015-1501 of 20 November 2015 prolonging the application of Law 55-385 of 3 April 1955 regarding the state of emergency and reinforcing the effectivity of its provisions, JORF, 21.11.2015, available at: www.legifrance.gouv.fr (in French only)

property rights, the Intellectual Property Code contains provisions enabling courts to order the removal of content from websites that breach intellectual property rights. With regard to the protection of privacy, the Civil Code entitles civil courts to order any appropriate measures to prevent or halt the violation at issue.

Administrative or semi-administrative blocking mechanisms exist, as before, in the areas of personal data protection and online gambling regulation. In particular, the French Data Protection Agency (CNIL) has the authority to ensure the cessation of processing of personal data carried out on the internet in the circumstances set out in Law 78-17 of 6 January 1978 on Information Technology, Data Files and Individual Liberties. Similarly, the **National Gaming Authority (NAG)**, which replaces as of 1 January 2020 the Online Gaming Regulatory Authority, is entitled to request a court order for blocking access to an online gaming service which does not comply with legal requirements.

2. Applicable regulations

2.1. Blocking and/or filtering of illegal internet content

2.1.1. The protection of national security and morality

French law provides for both judicial and administrative blocking and/or filtering of illegal internet content.

In line with Article 12.3 of the Directive 2000/31/EC on e-commerce, article 6.I.8 LCEN provides that internet intermediaries can be requested **by a court** to terminate or prevent an infringement caused by online content. In practice, such measures are ordered by civil courts and consist of requiring from hosting services companies that they remove illegal online content or, alternatively, from ISPs that they make specific online content inaccessible, as a provisional measure or as a final decision. This provision applies **irrespective of the ground for unlawfulness** of the content found by the court.

A procedure for **administrative blocking** was introduced into the LCEN[12] in 2014 within the framework of action taken against child sexual abuse and fight against terrorism and has not undergone significant change up to date**.** Administrative blocking can be requested by the Directorate General of the **National Police**, the Central Office for Combating ITC-related Crime (OCLCTIC) with regard to websites featuring images the dissemination of which constitutes a criminal offence related to **child sexual abuse**[13] or to **incitement or condonement of acts of terrorism** [“*le fait de provoquer directement ou de faire publiquement l’apologie”*].[14] Internet hosting services must remove illegal content within 24 hours of notification, failing which will lead to blocking of related websites, which ISPs must implement without delay upon OCLCTIC’s request (Article 6-1 LCEN).

In order to avoid disproportionate interference by this measure, the law assigns control over administrative blocking/removal of internet content to an expert appointed by the CNIL. The expert checks the merits of the blocking/removal requests made by the OCLCTIC and also ensures maintenance of the list of blocked or dereferenced websites.[15]

[12] Law 2014-1353 of 13 November 2014 on scaling up counter-terrorism provisions, available (in French only) on www.legifrance.gouv.fr. See also: Decree 2015-125 of 5 February 2015 on the blocking of sites inciting or condoning terrorism and sites circulating pornographic images and representations of minors, JORF, 6 February 2015, available at: www.legifrance.gouv.fr (in French only); Decree 2015-253 of 4 March 2015 on delisting of sites inciting or condoning terrorism and sites circulating pornographic images and representations of minors, JORF, 5 March 2015, available at: www.legifrance.gouv.fr (in French only)

[13] See Article 227-23 of the Criminal Code.

[14] See Article 421-2-5 of the Criminal Code.

[15] For further information, please see CNIL’s official website at: https://www.cnil.fr/en/node/22532

Since his appointment in January 2015, the CNIL expert has made several recommendations to the OCLCTIC regarding the assessment of questionable online content. In particular, on various occasions he has warned against blocking or removal of webpages which, despite containing images of terrorist attacks, did not incite or apologise terrorism. This was the case, for example, with respect to a video showing the terrorist attack of 14 July 2017 in Nice. In response to the blocking request by OCLCTIC, the CNIL expert submitted that **the mere fact of showing terrorist attacks was not sufficient** to trigger blocking or removal of a webpage. Stating that the substance of the video was neutral, the expert recommended not to block the webpage at issue. The OCLCTIC followed this recommendation.

Another noteworthy case concerns the OCLCTIC's request for removal and delisting of four videos showing police and gendarmerie vehicles set on fire (several such instances occurred in September 2017 in different locations). The CNIL expert warned against the measures requested because the videos at issue were not related to terrorist acts and therefore did not fall within the scope of the LCEN provisions on administrative blocking/removal of online content. As the OCLCTIC did not follow this recommendation, the CNIL expert initiated proceedings before the administrative tribunal. In its decision of 4 February 2019, the administrative tribunal ruled that the videos did not concern terrorist acts because: (i) the instances of arson did not have a nation-wide significance, nor affect a substantial part of the population, and (ii) the culprits were not part of a group activity aimed at destabilisation of the State and its institutions by installing a climate of fear and insecurity. As a result, the tribunal confirmed that the administrative blocking/removal procedure provided for by LCEN was not applicable in this case.[16]

In view of the continuing public debate on the inefficiency of blocking/removal measures, in 2016 the French legislator reinforced the respective mechanism. Law 2016-731 of 3 June 2016[17] created a new criminal offence that consists in willingly impeding or hindering the efficiency of the procedures of blocking and removal of illegal internet content as provided for by the LCEN or by article 706-23 of the Criminal Procedural Code. This offence is punishable by five years' imprisonment and a €75,000 fine.

The same Law also criminalised **repeated consultation of websites** disseminating images or messages directly inciting the commission of terrorist acts or apologising such acts. This provision was however declared unconstitutional by the Constitutional Council's decision of 10 February 2017.[18] An amended legal provision introducing the same criminal offence adopted at a later date[19] was also quashed by the Constitutional Council's decision.[20] Hence, the criminal offence of repeated consultation of terrorist websites no longer exists.

Most recently there has been a wide public debate[21] around **draft legislation** concerning the fight against hateful content on the internet.[22] This draft legislation, in parallel with the already existing "notice and take down" procedure (see section 2.2.1), was to impose on online platforms (social media) and web search engines **an obligation to remove/block/delist hateful content within 24 hours**

---

[16] Administrative Tribunal, Cergy-Pontoise, 4 February 2019, available (in French) at: http://cergy-pontoise.tribunal-administratif.fr/A-savoir/Communiques/Internet-premier-jugement-rendu-sur-saisine-de-la-personnalite-qualifiee-designee-par-la-CNIL

[17] Law 2016-731 of 3 June 2016 reinforcing the fight against organised crime, terrorism and its financing and ameliorating the efficiency and guarantees of the criminal procedure, J.O., 4 June 2016, available at: www.legifrance.gouv.fr (in French only)

[18] Constitutional Council, Decision 2016-611 QPC, 10 February 2017, available at: www.conseil-constitutionnel.fr

[19] Law 2017-258 of 28 February 2017 on public safety, J.O., 1st March 2017, available at: www.legifrance.gouv.fr (in French only)

[20] Constitutional Council, Decision 2017-682 QPC, 15 December 2017, available at: www.conseil-constitutionnel.fr

[21] See Section 5 for further information about the human rights debate around this draft legislation.

[22] Draft Law regarding the fight against hateful content on the internet, adopted by the National Assembly (nr. 419) on 13 May 2020, available at: http://www.assemblee-nationale.fr/dyn/15/textes/l15t0419_texte-adopte-provisoire.pdf

as of receipt of a notification containing a limited list of relevant information. The procedure was supposed to apply to **manifestly illegal** online content that may qualify under the following criminal offences: condonement of crimes against humanity; incitement or condonement of acts of terrorism; incitement to hatred, violence, discrimination as well as public insult against a person or a group of persons on the grounds of their origin, alleged race, religion, ethnicity, nationality, gender, sexual orientation or identity, disability; child sexual abuse.

The draft legislation further intended to impose on online platforms (social media) and web search engines an obligation to cooperate in the fight against hateful content encompassing, among others: acknowledging the receipt of notifications of hateful content and notifying the decisions taken on such notifications to the relevant parties; engaging the necessary means and resources for a smooth treatment of each notification, as well as ensuring proper assessment of the notified internet content so as to prevent unjustified removals; making available a recourse mechanism; taking measures to prevent repetitive spread of hateful content that has previously been blocked/removed/delisted. In fulfilling these obligations, internet intermediaries were to follow the recommendations issued by the *Conseil Supérieur de l'Audiovisuel*, the latter being entitled to impose fines for non-compliance of up to 4% of the annual worldwide turnover of respective companies.

Soon after adoption in the final reading by the National Assembly on 13 May 2020 and further submission to the Senate, the draft law regarding fight against hateful content on the internet was referred by a group of 60 senators to the Constitutional Council. In their application, the senators argued that some of the proposed amendments to the LCEN were not in line with the Constitution and carried serious risk to freedom of expression. In the decision of 18 June 2020, the Constitutional Council fully endorsed these arguments.[23]

In particular, with regard to the new obligation to remove/block/delist hateful content, the Constitutional Council considered the following: (i) the assignment of assessment of the notified content solely to internet intermediaries, regardless the complexity of such assessment that might require special expertise; (ii) the insufficiency of the 24-hour time limit for such assessment, bearing in mind the number of notifications; (iii) €250.000 fines being due per notification not processed within the deadline; (iv) the absence of exemptions from liability and (v) the lack of judicial or other review. It arrived at the conclusion that in sum the provisions at issue were conducive to over-removal/blocking. The procedure proposed by the draft law therefore interfered with the exercise of freedom of expression in a way that was neither necessary, nor proportionate and did not conform with the Constitution. The same conclusion was drawn regarding the new obligation to cooperate in the fight against hateful content which was inseparably linked with the new procedure for removal/blocking/delisting hateful content.

This draft legislation, in the part that has stood the constitutionality test, was finally adopted on 24 June 2020 (**Law 2020-766 regarding fight against hateful content on the internet**). Among amendments to the LCEN introduced by this Law, fines for physical persons and directors of legal entities for failure to comply with the LCEN provisions regarding moderation of child sexual abuse content or content inciting or apologising terrorism, have been augmented from €75,000 to €250,000.[24]

Apart from amendments to the LCEN, there has been little change in law and practice related to blocking and filtering of illegal online content. Following the terrorist attacks in France on 13 November 2015, the Government declared the **state of emergency**. The Law 2015-1501 of 20 November 2015 confirmed the state of emergency and specified the ensuing measures. In particular, this Law entitled the Ministry of the Interior to block certain types of illegal websites, i.e. websites featuring images the

[23] Constitutional Council, Decision 2020-801 DC, 18 June 2020, available at: https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm (in French only)

[24] Law 2020-766 of 24 June 2020 regarding fight against hateful content on the internet, available at: www.legifrance.gouv.fr (in French only)

dissemination of which constitutes a criminal offence under the legislation related to child sexual abuse or incitement or condonement of acts of terrorism. However, the **Ministry of the Interior has never used this power in practice,** as in parallel the procedure for administrative blocking/filtering was introduced by the LCEN. France lifted the state of emergency on 30 October 2017.

Lastly, in the field **of online gaming**, the **Online Gaming Regulatory Authority** (ARJEL) which has previously been in charge of monitoring online gaming sites, was replaced as of 1 January 2020 by the **National Gaming Authority (NAG)**, with its mandate reinforced.[25]

The NAG can act of its own motion or on cases referred to it by the public prosecution service or by any natural or legal person having a legitimate interest. The NAG sends **a formal notice** (by any means that allows for a confirmation of its receipt) to unauthorised online gaming or betting operators (i.e. operators which have not been granted an exclusive right or a licence as required by law) and to any individual offering online gambling or games of chance not in conformity with the law, giving them eight days to ensure compliance with the law and send their observations. At the same time, a formal notification is sent to the hosting services to prevent access to the illegal gaming website at issue.

Past the deadline, if the operator fails to terminate the betting, gambling or games of chance activity, or if the illegal gaming website is still accessible, the president of the NAG may **refer the matter to the president of the Paris Regional Court** for the latter to issue an injunction ordering the **website hosting services and ISPs to terminate access to this service.** Users whose access to the illegal website has been prevented are re-directed to a webpage containing information on the grounds for the blocking/removal measure. The president of the NAG may also refer the matter to the president of the Paris Regional Court for the latter to issue an injunction ordering any other necessary measure to **ensure that the website at issue can no longer be indexed** by a search engine or directory.[26]

2.1.2. Protection of intellectual property rights

The Intellectual Property Code (IPC) contains provisions that allow for blocking of websites whose activities violate intellectual property rights. Despite some changes of minor importance, the system for the protection of intellectual property rights from infringement caused by the content of online public communication services has remained essentially the same in the recent years.

Regarding copyright and related rights, article L.336-2 IPC provides that where there is an **infringement of copyright or a related right** caused by the content of an online public communication service, the president of the regional court, by means of an accelerated procedure, may order, at the request of copyright holders, or of the beneficiaries of the said holders, or of companies responsible for the collection and apportionment of copyright fees, or professional defence organisations **all measures to prevent or put an end to such infringement**. These measures may include blocking, filtering or removal from the internet of the infringing items.

In the field of **trademark protection** too, measures may be taken to prevent or put an end to an infringement. For instance, courts may order internet intermediaries, such as online trading site operators, to ensure that offers of counterfeit products are no longer accessible, as well as any other urgent measures.[27]

[25] Ordinance 2019-1015 of 2 October 2019 reforming the regulation of online gambling, JO, 3 October 2019, available on www.legifrance.gouv.fr (in French only)

[26] Law 2010-476 of 12 May 2010 regarding online gambling websites, Art. 61, J.O., 13 May 2010, available on www.legifrance.gouv.fr (in French only)

[27] Article L.716-6 IPC.

Concerning the protection of **domain names**, where the infringing item is a domain name, the owner of the infringed trademark may apply for cancellation of registration of the domain name or even request that the domain name at issue be transferred to his/her ownership,[28] which entails blocking of the website corresponding to the domain name in question.

2.1.3. Protection of privacy and personal data

Measures to end violations of privacy on the internet, i.e. violations of the right to one's image and to an individual's personal data, focus in the first place on removing the unlawful content from the internet (see section 2.2.3). In line with Article 9 of the Civil Code, the civil courts may order, including in summary proceedings, any appropriate measures to prevent or put an end to an infringement of the right to privacy. However, other legal bases for action are more appropriate for digital materials. For example, under the LCEN internet intermediaries may be requested **by court** to put an end to or to prevent the violation caused by the content of a website (see section 2.1.1).

2.2. Removal of unlawful internet content

2.2.1 Protection of national security and morality

As stated above (see section 2.1.1),the French law provides for the possibility for **civil courts**, upon summary or *ex parte* application, to order ISPs or hosting services to **take any appropriate measures to prevent or halt harm or damage** resulting from the content of an online public communication service, including ordering hosting services to remove a webpage.

In addition, the LCEN provides for a system for removal of unlawful internet content by hosting services, known as "**notice and take-down**". According to this system, there can be no removal of internet content if the hosting service has no **actual knowledge of the unlawful nature** of the content.[29] The law lays down a **rebuttable presumption of knowledge** of the unlawful nature of the content by the hosting service if the latter had received a **notification containing all relevant information as listed in the LCEN**. The list of items included in the notification has been reduced by the Law 2020-766 of 24 June 2020 and is currently limited to the identity of the notifying person (physical or legal), the category of online content, description of the content, the reasons for removal/blocking/delisting and the relevant web address(es). Awareness of the unlawful nature of the content, apart from the presumption, can also be proven by other means. In addition, the hosting service has a **margin of appreciation** in the decision whether to remove the content at issue: where there is no court order, hosting services are not obliged to disable access to unlawful content on the internet unless such content is of **manifestly unlawful nature**.

As mentioned above, the LCEN also provides for **administrative removal** of child sexual abuse content and content inciting or condoning terrorism **upon the decision of the OCLCTIC** (see section 2.1.1.). In addition, with regard to the same types of content, according to the LCEN the OCLCTIC may request the operators of search engines or directories of the electronic addresses to take all appropriate steps to **stop indexing** the websites in question.

The largely debated amendments to the LCEN that intended to introduce a procedure for removal of hateful online content have not passed the constitutionality test (see section 2.1.1.), leaving legislation in this part without significant change.

[28] Article L.45-6 of the Post and Electronic Communications Code.

[29] Article 6, I, 2 LCEN.

2.2.2. Protection of intellectual rights

Measures for removing online content that is in violation of intellectual rights are based on the same provisions as the blocking measures discussed above (see section 2.1.2).

In addition, as the "notice and take-down" procedure mentioned above (see section 2.2.1) is of general application, it also applies to websites breaching intellectual rights. A user may inform the web host of the existence of unlawful content; once notified, the host must remove the manifestly unlawful content, but has discretion when it comes to removing content which is not *manifestly* unlawful.

Other provisions in the IPC authorise courts to order specific measures such as the **confiscation or destruction** of counterfeit products or products that infringe copyright and the **withdrawal of such products from commercial circulation**.[30] Accordingly, insofar as they can oblige the hosting service or the editor of the website to remove respective items concerned from the online sales website, these equal to measures for removal of unlawful internet content.

2.2.3. The protection of privacy-related rights

With regard to violations of privacy, Article 9 of the French Civil Code provides that the **civil courts** may, without prejudice to the right to compensation for any injury suffered, order any measures to prevent or put an end to a violation of privacy. In urgent cases, these measures may be ordered in summary proceedings. In this respect, the Court of Cassation has stated that the finding of a violation is in itself sufficient to warrant urgent proceedings.

Nonetheless, other bases for legal action are more appropriate for digital materials. For example, in civil matters courts may require, upon a summary or *ex parte* application, the hosting services or ISPs to take any measures necessary to prevent or halt harm or damage resulting from the content of an online public communication service (see section 2.1.3). As stipulated in Article 6.I.8 LCEN, the courts shall first indicate these measures to the hosting services and only if the latter are unknown, turn to the ISPs.

In addition, as **the "notice and take-down" procedure** referred to above (see section 2.2.1) is of general application, it also applies to websites violating the privacy of third parties. A user may inform the web host of the existence of unlawful content; once notified, the host must remove the manifestly unlawful content, but has discretion when it comes to removing content which is not *manifestly* unlawful. However, in the field of protection of the right to privacy (e.g., defamation cases, etc.) it will often be difficult to establish the *manifestly* unlawful nature of the content.

2.2.4. Protection of personal data

In the field of personal data protection, the **French Data Protection Agency** (CNIL) has exceptional powers to halt any processing of personal data which fails to comply with the conditions laid down in Law 78-17 of 6 January 1978 on Information Technology, Data Files and Individual Liberties.[31] This Law was amended by the Law of 20 June 2018 regarding the protection of personal data, ensuring implementation of the General Data Protection Regulation[32] and other related European regulations

[30] See for instance, Article L.331-1-4 and L 716-13 IPC.

[31] Law 78-17 of 6 January 1978 on Information Technology, Data Files and Individual Liberties, available on www.legifrance.gouv.fr. According to Article 2, the law applies to automatic processing of personal data, as well as to non-automatic processing of personal data that are or may be contained in a personal data filing system, with the exception of processing carried out by individuals for the exercise of exclusively private activities.

[32] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJL, 119, 04.05.2016.

and directives. Accordingly, the CNIL's Restricted Committee can **order the data controller to cease data processing** where such processing is subject to a notification requirement, or withdraw authorisation given by the CNIL prior to the processing. This decision is made after hearing all parties and in cases where the data controller has failed to comply with the notice served on him or her by the CNIL.[33] In addition, if processing of personal data leads to a violation of privacy rights, such as the right to identity, the CNIL may initiate an urgent procedure, following which it may decide to i**nterrupt the processing for a maximum period of three months**, lock the data in question for the same maximum period or, where the processing in question is carried out by the state, inform the Prime Minister so that the necessary measures could be taken to end the violation identified. Lastly, in the event of serious and immediate violation of the above rights and freedoms, the Chair of the CNIL may request, by means of an urgent application, the competent court to order any appropriate measures for the protection of these rights and freedoms, if necessary also applying a daily penalty.[34]

3. Procedural matters

3.2. Administrative blocking and removal

The procedure for administrative blocking of websites disseminating images constituting a criminal offence under the child sexual abuse legislation or the legislation relating to incitement to or condonement of acts of terrorism, as provided for by the LCEN and specified in the Decree of 5 February 2015, **has remained without change since its adoption** (see section 2.1.1).[35]

The amendments contained in the draft law regarding fight against hateful content on the internet[36] seeking to reduce to one hour the time limit for hosting services and/or content editors to remove illegal content indicated to them have not passed the constitutionality test. In its decision of 18 June 2020, the Constitutional Council pointed out that such a short deadline, coupled with the lack of guarantees for freedom of expression, posed disproportionate risk for the latter.

3.3. Court-ordered blocking and removal

The procedure to obtain a court-ordered measure of blocking or removal **has not been subject to change**. Courts can order, upon summary or *ex parte* applications, any measures necessary to prevent or halt the harm caused by the content of a website (Article 6, I, 8 LCEN).[37] This is equally valid in respect of copyright and neighbouring rights (Article 336-2 IPC)[38] and violations of privacy (Article 9 Civil Code).[39]

[33] Article 20 of Law 78-17 of 6 January 1978 on Information Technology, Data Files and Individual Liberties, available on www.legifrance.gouv.fr

[34] Article 21 of Law 78-17 of 6 January 1978 on Information Technology, Data Files and Individual Liberties, available on www.legifrance.gouv.fr

[35] Further information on this procedure can be found in the 2015 Comparative study.

[36] Draft Law regarding the fight against hateful content on the internet, adopted by the National Assembly (nr. 419) on 13 May 2020, available at http://www.assemblee-nationale.fr/dyn/15/textes/l15t0419_texte-adopte-provisoire.pdf

[37] See Sections 2.1.1 and 2.1.2.

[38] See Sections 2.1.2 and 2.2.2.

[39] See Sections 2.1.3 and 2.2.3.

4. General Internet monitoring

As before, under the LCEN, **hosting services and ISPs are not subject to a general duty to monitor** the information they transmit or stock, nor to actively seek out facts or circumstances indicating unlawful activities. The LCEN nevertheless provides that internet intermediaries may be required by the courts to engage in **targeted and temporary monitoring**.

Internet intermediaries are also required to **establish a procedure whereby anyone is able to bring to their attention** any relevant information for combating crimes against humanity, inciting or condoning acts of terrorism, incitement to racial hatred, hatred of persons on the grounds of their gender, sexual orientation or gender identity, disability, child sexual abuse, incitement to violence, especially incitement to violence against women and abuse of human dignity. As a result of legislative reforms in 2016 and 2018, the same obligation now applies to internet intermediaries with respect to content relating to human trafficking, prostitutes' exploitation and related facts as well as sexual harassment.[40] **Internet intermediaries are also obliged to inform the competent public authorities of any unlawful activities notified to them** that may be conducted by the recipients of their services.[41]

The findings of the 2015 Comparative study as regards internet monitoring by the **OCLCTIC** remain valid, and the provisions of the Homeland Security Code (CSI)[42] regarding intelligence gathering with the help of internet operators in order to protect national security have also remained without significant change.

In addition, Law 2020-766 of 24 June 2020 on fighting against hateful content on the internet has laid basis for establishment of a new internet monitoring body – an online hate observatory that would monitor and analyse the evolution of hateful content on the internet. The observatory is supposed to bring together operators, associations, administrations and researchers concerned with the fight against and prevention of relevant offenses, taking into account the diversity of audiences, in particular the minors. The *Conseil Supérieur de l'Audiovisuel* will provide secretariat services to this body.

5. Evaluation in the light of the case law of the European Court of Human Rights

The introduction of a procedure for administrative blocking of child sexual abuse websites and websites inciting or condoning terrorism has given rise to a lively debate, which culminated in the initiation before the **French *Conseil d'Etat*** of an annulment procedure against the Decrees of 4 February 2015 and of 4 March 2015 regulating this procedure. On 15 February 2016, the Conseil d'Etat] **confirmed the compatibility of the two decrees with Article 10 of the European Convention of Human Rights** (ECHR). In its decision, the *Conseil d'Etat* stated that the measures of blocking and removal as provided by the two decrees have a justified objective of (i) preventing access by good faith users to websites featuring child sexual abuse content and content inciting or condoning terrorism, and (ii) preventing voluntary access to these websites. It further confirmed that **Article 10 of the ECHR did not require the measures of blocking and/or removal to be ordered by courts only**. Lastly, in the opinion of the French *Conseil d'Etat*, the two decrees offer a **range of guarantees against disproportionate interference with freedom of expression.** Notably, one of such guarantees is monitoring of the application of administrative measures of blocking and/or removal of illegal internet

[40] Art. 6, I, 7, sub-paragraphs 3 and 4 LCEN. See also Law 2016-444 of 13 April 2016 reinforcing the fight against the system of prostitution and to accompany prostitutes, J.O., 14 April 2016, available at www.legifrance.gouv.fr (in French only) ; Law 2018-703 of 3rd August 2018 reinforcing the fight against sexual and sexist violence, JO, 4 August 2018, available on www.legifrance.gouv.fr (in French only)

[41] Art. 6, I, 7, sub-paragraph 4 LCEN.

[42] See, in particular, Articles L. 851-1 and L. 851-2 CSI.

content by the CNIL expert, with the possibility of intervention and the power to challenge the administrative measures at issue before the administrative court.

In the recent past however, most of the attention had been focused on the **draft legislation regarding fight against hateful content on the internet**.

The National commission on human rights (NCHR) rendered a negative opinion on this draft legislation. In a report published on 9 July 2019, it stated that the draft legislation, and in particular its procedural aspects, posed a **disproportionate risk to freedom of expression**. **Assessment of the (il)licit nature of internet content shifted from the judicial authorities to privately owned online platforms** (the so-called "privatisation of the judicial function"), as foreseen by the draft law, was one of the main reasons for concern. In the NCHR's view, the fact that the draft legislation intended to limit the obligation to remove/block/delist to "manifestly" illegal online content was not a sufficient guarantee.

The **United Nations Special Rapporteur for the promotion and the protection of the freedom of opinion and expression** in a letter to the Government of France dated 20 August 2019 echoed the above opinion. He further expressed concern about the fact that, according to the draft legislation, online platforms shall be obliged to comply with the recommendations made by an administrative authority, the *Conseil supérieur de l'audiovisuel* (CSA), entitled to impose, in case of non-compliance, fines of up to 4% of their worldwide annual turnover. **The CSA being not a judicial authority** but an administrative authority, the Special Rapporteur also raised the issue of freedom of expression guarantees.

Both at the early stage of the debate around this draft legislation and in the course of proceedings before the Constitutional Council, the French Government provided detailed response to the arguments advanced.[43] Regarding criticism against the **privatisation of the judicial function**, the French Government referred to the fact **the original version of the LCEN** contained similar provisions regarding certain types of "manifestly" illegal internet content, which had been **accepted by the Constitutional Council**. The Government further argued that with the adoption of the draft legislation, the judicial authorities will continue being involved in legal assessment of the **nature of internet content, including upon appeals against decisions on content** blocking/removal/delisting. The government further contended that the **CSA will not interfere with the powers that are reserved for the judiciary,** as it is not mandated to assess the manifestly illegal nature of specific internet content. In addition, the **draft legislation imposes on online platforms a series of obligations**, which shall ensure that there is no overblocking, e.g., to engage the necessary human, technological and other resources, with a report on the measures taken, and to introduce procedures to ensure prompt treatment of the notification as well as appropriate assessment of the notified internet content to limit the risk of unjustified removal.

As discussed above (see section 2.1.1.), the Government's arguments have not been accepted by the Constitutional Council which has **found freedom of expression guarantees embedded in the draft legislation to be insufficient**. The version of the Law 2020-766 that entered into force on 1 July 2020 therefore only features very few provisions as compared to the initial draft, all provisions found to carry risk to freedom of expression having been left out after the constitutionality test.

On 16 October 2020, Mr Samuel Paty, a schoolteacher in Conflans-Sainte-Honorine in France, was murdered and beheaded after having shown Charlie Hebdo's 2012 caricatures of Mahomet to his students in the framework of a class on the topic of freedom of speech. This attack, which occurred following a campaign on social media against Mr Paty for his class, is likely to trigger new political and legislative developments with respect to the blocking and taking down of illegal internet content.

[43] See, for instance, Government observations on the law to combat hateful content on the internet, submitted to the Constitutional Council on 9 June 2020, available at: https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/decisions/2020801dc/2020801dc_obs.pdf