CRIMINAL PROTECTION FOR PRIVATE LIFE RIGHTS IN THE DIGITAL AGE

Nicolas Bonnal
Conseiller à la Cour de cassation (chambre criminelle)

The two faces of the digital revolution, the generalisation of electronic communication and the digitisation of most restocking processes and of data, have become indissolubly linked. 'There is less and less data handling without communication and reciprocity'.[1] In these circumstances, if criminal law is to retain its effectiveness in the areas which we are considering during this round table, that is to say, the protection of the private rights of individuals, it can rarely be spared the trouble of undergoing profound change.

Nevertheless, that fact is not to be imposed out of hand, and the reality of this development is complex and multi-faceted. It would be more accurate to distinguish, within this adaptation process, two main parallel trends.

The first trend consists of applying the existing concepts to the new purposes with which the digitisation of our society presents the judge, either simply because such development always outpaces the legislator, or because the legislator assumes that digitisation has no effect on the definition and prosecution of the classic criminal offences.

But such an approach is quickly seen to be limited, because the combination of data handling and of electronic communication radically changes reality, modifies behaviour and creates new risks. We come, therefore, to the moment of novation, whether by the judge, developing the scheme of existing offences, or the legislator, creating new offences, a delicate exercise because it requires the criminal judge to become involved in an area which is highly technical, and in addition, constantly changing.

In all stages of this process, such development cannot take place without respecting the overriding principles of human rights guaranteed by the Constitution, the European Convention on Human Rights, and the law of the European Union. These principles have developed to take account of this new reality, as shown by the important decision of the French Constitutional Council,[2] which included free public access to online communication among the

1 Alain Bensoussan, *Informatique Télécoms Internet,* Francis Lefebvre
2 Constitutional Council, 10 June 2009, decision no 2009-580 DC, Law promoting the spread and protection of the internet

rights protected by Article 11 of the 1789 Declaration of the Rights of Man and the Citizen.[3]

This subject is inexhaustible, having regard to the scale of digital change. We will therefore consider just a few recent examples illustrating the difficulties facing both the legislator and the judge, and the responses they have tried to make. We will examine three areas: (I) the application of French criminal law concerning the press, when the offence is capable of having been committed on the internet; (II) the creation of a series of new offences to deal with attacks on personal rights arising out of digital files or data processing; and (III) the creation of new delicts which criminalise not only the publication of prohibited content, but also accessing such content on the internet. We will thus consider successively the protection of reputation, of personal information, and of freedom of communication.

The application to the internet of French criminal law on the press

The law of 29 July 1881 on the freedom of the press has been extended and modified from time to time over the last 150 years, but, before the existence of the internet, it had not seen any great change to its overall balance. This is not the moment for an exhaustive study of that law, of the effect on the abundant and fairly stable jurisprudence of that ancient text, nor how it has adapted to the new support for press offences arising from the internet: the freedom of the press was the principal topic of your last meeting. It suffices to say that the list of types of publicity covered by Article 3 of that law has been extended, successively, to include audio-visual communications,[4] and then to public online communication.[5] And, applying roughly similar steps,[6] the list of those legally responsible for press offences has been adapted to include audio-visual and online communications, so that it includes intermediaries who provide access to and hosting of data.

Legislative adaptation ends there. Judicial interpretation of these new provisions has not been easy and will require lengthy development,[7] particularly for those provisions, created for audio-visual communication, which have substituted the producer for the online communication, but those have no place in the present discussion.

3 "The free communication of thoughts and opinions is one of man's most precious rights: thus, every citizen may speak, write, and print freely, save for the limitations imposed by law on abuse of that freedom"

4 Law of 13 December 1985 containing various provisions relating to audio-visual communication.

5 Law of 21 June 2004 on confidence in the digital economy

6 Law of 29 July 1982 on audio-visual communication; Law of 21 June 2004, op.cit.

7 See Cour de Cassation Criminelle, 16 feb 2010, *Bull.criminal.* 2010, nos 30 and 31 ; Conseil Constitutionnel, 16 sept 2011, decision no 2011-164 QPC

On the other hand, the internet poses a new problem, the jurisdiction of the French judge. That question is indissolubly linked to the application of French law, applying the 'traditional and seemingly universal'[8] idea of the solidarity or coincidence of judicial and legislative skills in criminal matters, according to which the criminal judge of any State applies its national criminal law.

This question is particularly difficult to solve because of the well-established jurisprudence holding that, in press matters, it is the publication itself which constitutes the offence or delict. Since the 19th century, the Criminal Chamber of the Cour de Cassation has regularly held that 'in press cases, it is the publication of the offending text which constitutes the delict: proceedings may therefore be brought in any court in whose jurisdiction the text in question has been published.'[9]

The Cour de Cassation has recognised no exception to that rule in any prosecution based on the provisions of the law of 29 July 1881 concerning the freedom of the press. The courts have therefore held that in applying that rule, the plaintiff's choice of jurisdiction is 'arbitrary, artificial, and by its nature, harmful to the interests of the defence'.[10] This rule applies equally to television programmes: '… defamation perpetrated by publication in the written press is held to be committed wherever the publication has been published, distributed or sold; …'.[11]

The rule has been applied to the internet by some first instance Courts.[12] However, the limit of such a mechanical application of existing jurisprudence is apparent when applied to the internet, which is by its nature universally accessible. For this reason, other Courts have chosen to derogate from the rule: thus, in a case where an accused, prosecuted for conspiracy to public defamation, by publication of an article on an internet site situated abroad, disputed the jurisdiction of the French Courts, a French judge refused to apply the exception, observing that the site in question was aimed at the French public, written in French, and had been visited in France on several hundred occasions.[13] However, that decision was not the subject of an appeal.

A particularly good example of the totally artificial application of French law to the press presented itself in a case which came before the Poitiers Cour d'Appel: two sisters, one of Japanese nationality and the other an American citizen, both

8 André Huet et Renée Koering-Joulin, Droit pénal international, 3rd edition., PUF, 2005, no117
9 Cour de Cassation Criminelle, 5 January 1894, *Bull. criminal.* 1894, no5
10 Cour de Cassation Criminelle, 28 November 2006, *Bull. criminal.* 2006, no298
11 Cour de Cassation Criminelle, 5 December 2000, Appeal no 99-85.361
12 CA Limoges, 8 June 2000 : *BICC* 2001, 210 ; CA Paris, 17 March 2004, *Digital Communication and Commerce* 2005, Comm. 72, obs. Agathe Lepage ; CA Paris, pôle 1, ch. 2, 30 September 2009, RG no 09/09773, cited in *Digital Communication and Commerce* no 3, March 2010, chron. 3, Christophe Bigot
13 CA Paris, Ch.2-7, 6 September 2012, JurisData: 2012-021933

domiciled in Japan, sued a South African citizen before the Niort Criminal Court (Deux-Sèvres) for public defamation of an individual, for having uploaded to an American internet site two documents in the English language. The plaintiff was writing a book on Japanese video games, on which one of the sisters was an expert: the disputed passages in the online documents challenged the situation where the other sister had advised the plaintiff to use an incompetent Japanese interpreter, and, on the other hand, the campaign of denigration which the sisters had led against him.

Why, you ask, should such a case have been brought before the court in Niort? The reason given was that, several years earlier, the accused had lived within the jurisdiction of that Court, where his parents still lived. But he himself no longer lived there and had moved his domicile to London, long before the index events. The court could not derive jurisdiction from the residence of the defendant. There remained the place of commission of the offence, because, within the jurisdiction of the Niort court, one could connect to the internet and read there the disputed texts.

The accused applied to the Tribunal to recuse itself for lack of jurisdiction, and the Court entertained that application. It held that neither the internet site, nor the disputed publications were 'oriented towards the French public'. How, indeed, could a South African, writing in English on an American website about a situation which occurred in Japan, concerning two sisters who were Japanese and American citizens respectively, be expected to anticipate the application of French law and its eventual consequences to his actions?

The sisters appealed. The Cour d'Appel upheld the judgment. One of the sisters appealed to the Cour de Cassation. The Criminal Chamber[14] dismissed the appeal, holding that 'in the absence of any criterion linking the disputed words to the territory of the French Republic, the mere circumstance of their being available in that territory, by reason of their publication on the internet, was not of itself capable of being characterised as an act of publication on that territory, giving a French judge jurisdiction to decide thereon'.

The Court thus made an important exception to a fundamental principle of French law concerning the press. In so doing, the Court was able to rely on numerous precedents, but from other areas of criminal law. The Court had previously ruled, long ago, when dealing with counterfeit products available on

14 Cour de Cassation Criminelle, 12 July 2016, to be published shortly in the Bulletin ; *Dalloz* 2016, p. 1848, note Emmanuel Dreyer; *Gazette du Palais*, 2016, no.34, p. 45, note Stéphane Detraz, et no.38, p. 35, note François Fourment ; *Contrats Concurrence Consommation* 2016, comm. No.83, note Agathe Lepage ; *Légipresse*, October 2016, p. 532, note Stéphane Detraz

line, that a conviction for counterfeiting could not be made unless the judges were satisfied that the disputed site 'was directed towards the French public'.[15]

The Court was also able to draw upon decisions of the Court of Justice of the European Union, dealing with the interpretation of Community law regarding the jurisdiction of civil Courts,[16] which, while reserving the possibility for a victim of defamation to obtain compensation 'before the courts of each Contracting State in which the publication was distributed and where the victim claims to have suffered injury to his reputation, which have jurisdiction to rule solely in respect of the harm caused in the State of the court seised', interpreted the Regulation to mean ' before the courts of the Contracting State of the place where the publisher of the defamatory publication is established, which have jurisdiction to award damages for all the harm caused by the defamation'.[17] The court later added, this time dealing with an attack on private life, taking into account the specificity of the internet and reserving expressly at least the possibility of obtaining, in the place where the harm was caused, damages only for the harm caused in that place, that ' … given that the impact which material placed online is liable to have on an individual's personality rights might best be assessed by the court of the place where the alleged victim has his centre of interests, the alleged victim may choose to bring an action in one forum in respect of all of the damage caused'.[18]

Although this civil law approach is not the obvious route, having regard to the overlap between judicial and legislative jurisdiction in criminal matters, it has nevertheless supported the analysis in the 12 July 2016 decision. Thus, the elusive character of the internet leads us, on the question of jurisdiction, to favour not the author or the editor, difficult to discern in the background, but the private individual whose interests are harmed by an online publication.

New offences punishing attacks on personal rights resulting from digital files or data processing.

We know that French law, fairly early in the European context,[19] took into account the reality of attacks capable of causing prejudice to private individuals, by reason of the digital processing of personal data, formally establishing the principle that digitalisation 'should do no harm either to human identity, or to

15 Cour de Cassation Criminelle, 14 December 2010, appeal no 10-80.088; and earlier, to the same effect, Cour de Cassation Criminelle, 22 May 2007, appeal no 06-87.520; 9 September 2008, appeal no 07-87.281

16 Article 5(3) of Regulation 44/2001(EU) of the Council, 22 December 2000, concerning judicial jurisdiction, recognition and execution of civil and commercial decisions.

17 CJEU, *Fiona Shevill & Ors v Presse Alliance SA.* (Convention on jurisdiction and the enforcement of judgments) [1995] EUECJ C-68/93, which responded to a reference from the House of Lords, regarding defamation proceedings in the United Kingdom against the editor of a French publication.

18 CJEU, *eDate Advertising GmbH v O. et R. Martinez,* C-509/09 et C-161/10 (25 October 2011), as explained by the Luxembourg court in a later decision (*Peter Pinckney v KDG Mediatech AG* [2013] EUECJ C-170/12 (03 October 2013))

19 Law of 6 January 1978 regarding digitalisation, digital files and freedoms

human rights, or to private life, or to individual or public freedoms', and in parallel, created an independent, multi-mission administrative authority, the Commission Nationale Informatique et Libertés (CNIL). The Constitutional Council,[20] after considering a law which had been referred to it and which provided that ' the legislator has not contemplated any derogation from the protective measures protecting individual freedoms set out in legislation regarding data processing, data files or freedoms', included this text in the 'Constitutional bloc'. Then, applying Community law,[21] French law substituted for personal data the notion of data with a personal character.[22] All of this took place before the coming into force of the new Community rules, [23] applicable from 25 May 2018.

It is the criminal dimension of this text which we will discuss here. The offences created in law have been greatly recast and completed over the years, and they are now integrated into the Criminal Code.[24] This is not the place to deliver an exhaustive study of these offences, which would be tedious and irrelevant. I now propose to illustrate how this law of the digital age leads, inevitably and perhaps more than any other, to a dynamic link between administrative and penal law, and to explain why criminal penalties are not always the most apt method of assuring the most effective protection of data with a personal character.

The limits of criminalisation

An example of what legal doctrine describes as 'criminal law sanctions',[25] this criminalisation of some of the Rules under the Law of 1978 operates by reference to other provisions. Instead of defining offences *in extenso*, these criminal provisions penalise failure to meet legal obligations, and refer to those texts for the definition of the said obligations. Thus, the delict defined at article 226-16 of the Criminal Code penalises 'the fact, including by negligence, of either proceeding, or causing other to proceed to process data with a personal character without respecting the legal formalities for so doing'. The law does not specify, by reference to precise Articles, for what formalities breach will be so penalised, although the punishments are far from being symbolic, 5 years in prison and 300,000 Euro fines.

20 Constitutional Council, 20 January 1993, decision no93-316 DC, Law regarding the prevention of corruption and transparency in economic life and public procedures

21 Directive 95/46/EEC of the European Parliament and the Council of 24 October 1995, regarding the protection of physical persons relating to the treatment of personal data and the free circulation of such data

22 Law of 6 August 2004 regarding the protection of physical persons regarding the treatment of personal data, modifying Law no.78-17 of 6 January 1978 relating to digitalisation, digital files, and freedom

23 Regulation 2016/679 (EU) of the European Parliament and the Council of 27 April 2016 regarding the protection of physical persons relating to the treatment of personal data and the free circulation of such data, and repealing Directive no 95/46/CE

24 Articles 226-16 to 226-24 of the said Code

25 Patrick Maistre du Chambon, Agathe Lepage, Renaud Salomon, *Droit pénal des affaires,* LexisNexis, 2015

Now, the preliminary requirements in question are complex, to the extent that the law does define them, as set out in Chapter IV (at Articles 22-31, which sometimes also proceed by way of reference to other legal provisions), which distinguishes the system of declaration, normal or simplified, from which certain data processing is purely and simply excepted, from the system of authorisation, and fixes the ways, communal or individual, in which such declaration or authorisation must be made. The duties which the law imposes are completed by a regulatory text,[26] which is equally dense and detailed.

In these circumstances, the material element of the offence can take multiple forms. The most obvious situation is the absence of the formality which the law requires, and therefore, of what we might call clandestine data processing, which should have been declared and authorised, but has been conducted without any formal application, so that it remains unknown.[27] But it has been held that the delict was committed where a declaration was made, not in the form required by law (and spelled out in detail in the Decree), but by a simple letter.

One particular dimension of this offence appears in Article 226-16-1A of the Law which penalises failure to respect the CNIL norms for simplified declarations, or dispensation from declaration, for ' the most common categories for processing data with a personal character, the implementation of which is incapable of causing harm to private life or freedoms'.[28] Heavy penalties (the same as those set out in Article 226-16) are imposed for the failure to respect rules set by an independent administrative authority, which is also given power to define the scope of such rules (it is for CNIL to determine what types of data processing come within the definition just set out, and also, which data processing is dispensed from any declaration), rules for which the law only states that CNIL will publish them.

A recent case illustrates[29] the difficulty of implementing the criminal penalties which the law contemplates, in the context of proceedings based on Article 226-19 of the Criminal Code, which penalises data processing of the most sensitive personal facts, when it is done 'outside the cases covered by the law', and in particular, those which reveal racial or ethnic origin, political, philosophical or religious opinions, or which relate to health or to a person's sexual orientation. A man wanted to give blood, but was refused twice, by reason of his presumed homosexuality, and in conditions which led him to believe that his digital record was so marked. His civil action for breach of Article 226-19 was dismissed, because such treatment of his data was authorised by Article L. 1223-3 of the

26 Articles 7 to 41-1 of the Decree of 20 October 2005 for the application of Law no.78-17 of 6 January 1978 regarding electronic data, files and freedoms.
27 Cour de Cassation Criminelle, 3 November 1987, appeal no.87-83.429, *Bull. criminal.* 1987, no.382
28 Article 24, Law of 6 January 1978
29 Cour de Cassation Criminelle, 8 July 2015, appeal no.13-83.267, *Bull. criminal.* 2015, no.175 ; *Droit pénal* 2015, comm. 109, noted by Michel Véron

Public Health Code, which in its relevant guidance imposed on blood transfusion centres the obligation to 'introduce good practices', and by the 10 September 2003 Order of the Minister of Public Safety, regarding good practice in blood transfusion matters, which included a contraindication to the giving of blood in such circumstances.

The Cour de Cassation made an urgent reference to Conseil Constitutionnel of the question whether, by reason of the combination of these two instruments, the existence of a criminal penalty depended' on 'good practices' defined by reference to a regulation promulgated by a public establishment'.[30] The Conseil Constitutionnel[31] said that Article 226-19 did not infringe the legality of either delicts or penalties, that the provisions of Article L. 1223-3 of the Public Health Code 'do not have the object of defining an exception to such incrimination; that such exceptions are specifically defined in Article 8 of the Law of 6 January 1978', and considered that both instruments were in conformity with the Constitution.

The case then came back before the Cour de Cassation, which upheld the dismissal, taking account of the recast guidance of the Conseil Constitutionnel, because it considered that, if data handling could not be authorised by the instruments on which the investigatory chamber of the Cour d'Appel based its decision, then the matter ' falls [...] within the provisions of Article 8(II)(6) of Law no 78-17 of the 6 January 1978, according to which, pursuant to paragraph 1 of that Article, the prohibition on collecting or handling data with a personal character, relating, in particular, to health or the sexual life of individuals, does not apply to necessary treatments for preventive medicine, medical diagnosis, the administration of care or treatments, or the management of health services, or by another person bound by doctor-patient privilege'.

The relationship between administrative sanctions and criminal prosecutions.

Despite the diversity, and the wide field of offences assembled in Articles 226-14 and following of the Criminal Code, of which the examples above give a brief overview, it does not seem that the criminal route is often used. The technicality, and the lack of clarity of certain ideas are sufficient to explain this caution by the prosecuting authorities. In addition, there is the no doubt decisive factor that an administrative route exists, as a result of the power of CNIL to impose penalties, under the conditions set out in chapter VII of the Law of 1978. Any disrespect for the legal obligations can give rise to penalties. The penalties provided include warnings, pecuniary penalties up to 3 million Euros, and an injunction to cease handling electronic data.

30 Cour de Cassation Criminelle, 17 June 2014, QPC no13-83.267
31 Constitutional Council, 17 September 2014, decision no.2014-412 QPC

The behaviours which attract criminal penalties, as well as those which do not, are punishable under the CNIL's power to impose penalties. Without straying here into a discussion of questions linked to the application of the rule of *non bis in idem*, we remind ourselves only that the law provides that when a pecuniary penalty has become final, a criminal judge dealing elsewhere with the same facts, or linked facts, may decide that such pecuniary sanction counts against the penalty which he will impose.

We will look at an interesting link between administrative and criminal penalties: Article 226-16(2) imposes the same penalty as Article 226-16(1) for proceeding to handle data electronically despite CNIL having granted an injunction to cease processing (if it arises out of a declaratory scheme) or having withdrawn authorisation (when authorisation is required and had been granted). Thus, if the administrative penalty is not respected, a criminal prosecution can take over. The interest of this provision must be kept in proportion: in 2016, among the 13 penalties imposed by the special panel of the CNIL,[32] there was not one injunction or withdrawal of authorisation (but four pecuniary penalties and nine warnings).

The same CNIL annual report for 2016, from which this information is taken, gives another example of an interesting link between the administrative and judicial authorities. The President of the CNIL used his power of giving formal notice before commencing proceedings which could lead to an administrative penalty[33] to a company which produced an application called 'Gossip, anonymous rumours', used by hundreds of millions of people, permitting an internaut to circulate to all his contacts who used the application a rumour aimed at the said contacts (who, if they did not use the application, would remain unaware of that circulation). The formal notice had the effect of leading the company to close down the application, following which, as the law provides, the administrative procedure ended. The CNIL then reported the circumstances to the Public Prosecutor, pursuant to Article 40 of the Criminal Procedure Code, having regard to the deficiencies identified and the risks involved, particularly to minors.

Criminalising access to prohibited content on the internet

Article 421-2-5-2 of the Criminal Code illustrates the difficulties of penalising access to internet links, when it is combined with a recasting such as that which we have considered on the question of the jurisdiction of the criminal libel judge dealing with text uploaded online.

32 *Activity Report* 2016, Conseil National de l'Informatique et des Libertés, La Documentation française
33 Article 45, Law of 6 January 1978, and Article 73 Decree of 20 October 2005

The initial version of that Article[34] prohibited ' the fact of habitually accessing an online public communication service, which hosts messages, images, or representations, or directly provokes the commission of acts of terrorism, or glorifies such acts when, to that end, the service includes images or representations showing the commission of such acts, consisting in voluntary attacks on life', except ' when such accessing is undertaken in good faith, results from the normal practice of a profession having for its purpose to inform the public, or takes place in the context of scientific research, or is undertaken in order to serve as evidence in legal proceedings'.

Criminalising accessing internet content which is itself criminally prohibited[35] is neither natural nor frequent.[36] The logic of the law on the freedom of the press, is that it is the editors, and the authors, of prohibited content who must answer for it. This classic device has been expanded by special regulations, regulating technical intermediaries on the internet, who benefit from a system of conditional protection from responsibility, but are required to contribute to the struggle against the dissemination of the offences of provocation and glorification of acts of terrorism, in ways which the law sets out.

The fact remains that, for the Public Ministry, it is practically impossible to suppress such content, broadly diffused by individuals who can easily take steps to ensure that they are safe from attack. It is, therefore, that inability of the national prosecution authorities to ensure respect for their own law on the network which has led to the criminalisation of the act of accessing the said content.

Of course, that is not the only reason: it has been observed that habitual accessing of such content becomes a type of apprenticeship,[37] substantially, the foundation of a possible transition to the act itself. Such habitual accessing has been retained as one of the elements constituting the delict of individual terrorist offence.[38]

On the other hand, according to the Conseil d'État, which, in the context of an earlier attempt by the Government to create a delict of habitual accessing of prohibited material, had expressed clear reservations as to the compatibility of

34 Law of 3 June 2016 strengthening the fight against organised crime, terrorism, and their financing, and improving the effectiveness and guarantees in criminal procedure.
35 In this case, Article 23, Law of 29 July 1881 on the freedom of the press for provocation having for effect the commission of an act of terrorism, et Article 421-2-5 of the Criminal Code, for direct provocation and advocating terrorism
36 Law of 5 March 2007 regarding the prevention of delinquency, of which Article 29 inserted, in Article 227-7(7) of the Criminal Code, a delict of habitual accessing of a paedo-pornographic site, which regularly gives rise to prosecutions, and of which the constitutionality has never been challenged.
37 Senate, 2 February 2016, Senator Mercier, Rapporteur for the draft law on reinforcing the effectiveness of the fight against terrorism.
38 Article 421-2-6 of the Criminal Code, inserted by the Law of 13 November 2014 reinforcing provisions relative to the fight against terrorism.

such a provision with the French constitution and/or the ECHR,[39] the Cour de Cassation, when dealing with a preliminary reference on constitutionality, and considering ' the necessity and proportionality of this attack on the principle of freedom of communication' as well as the precise definition of the notion of habitual accessing in good faith, referred the question to the Conseil Constitutionnel.[40]

One must remember that this Court, seised of the law giving to an administrative authority charged with protection of online copyright, the possibility of imposing penalties, including the prohibition of internet access for the offender (known as Hadopi 1), held that ' in the present state of means of communication, and having regard to the general development of public online communication services, as well as the importance which those services have acquired in the participation in democratic life, and the expression of ideas and opinions, such right implies freedom of access to these services; ...that the power to impose sanctions given by the contested provisions empower the Commission for the Protection of Rights, which is not a court, to restrict or prevent internet access by subscription holders, as well as the persons whom they benefit; that the jurisdiction given to such administrative authority is not limited to one particular category of persons, but extends to the totality of the population; that its powers could lead to restricting access, by anyone, to their right of expressing and communicating freely, particularly from their own home; and that, in these circumstances, regard being had to the freedom guaranteed by Article 11 of the Declaration of 1789, the legislator cannot, whatever guarantees surround the pronouncement of such sanctions, give powers of this kind to an administrative authority, with the purpose of protecting the owners of copyrights and associated rights'.[41]

On the question raised under Article 421-2-5-2 of the Criminal Code, la Constitutional Court[42] held that ' administrative and judicial authorities have, independently of the contested Article, numerous prerogatives, not only to supervise online public communications services tending to provoke or glorify terrorism and to repress their authors, but also to keep under surveillance an individual who accesses such services and to question and punish them when such access is accompanied by behaviour indicating a terrorist intention, even before such a project enters its execution phase', but that ' the disputed provisions do not require that a person concerned in habitual accessing of public online services should have the will to commit terrorist acts, nor even evidence that such accessing is accompanied by demonstration of adherence to the ideology expressed on such services' and that, since the scope of the exception

39 Notice no 386618 of 5 April 2012, *Activity Report* 2013, pp. 202 and 203
40 Cour de Cassation Criminelle, 29 November 2016, QPC no16-90.024
41 Constitutional Council, 10 June 2009, op.cit.
42 Constitutional Council, 10 February 2017, decision no 2016-611 QPC

for good faith remains uncertain, they 'impose a lack of certainty as to the legality of accessing certain public online communication services, and, therefore, of using the internet to research information', held the provisions to be contrary to the Constitution, because they 'comprise an attack on the exercise of the freedom of communication which is neither necessary, suitably adapted, or proportionate'.

Parliament, almost immediately, enacted a new version of the legislation;[43] habitual accessing is now punishable only 'when such accessing is accompanied by a demonstration of belonging to the ideology expressed on the service' and when it is effected ' without legitimate motive'. Such motive can be demonstrated by the three exemptions defined in the first version of the legislation (public information, scientific research, judicial investigation) or by 'the fact that such accessing is accompanied by reporting of the content of the service to the competent public authorities'. It is not impossible that the constitutionality of the latest draft could be raised again in Courts vested with prosecutions undertaken on the basis of facts which predated its entry into force, but punishing access to content on the internet remains subject to the respect of the personal right, recognised by the Conseil Constitutionnel, of access to online communication services.

Over and above their own specific features, the three themes I have just dealt with illustrate various faces of the same difficulty, for criminal law, in understanding the digital age. The universal character of the internet is in conflict with the national essence of penal law. In consequence, it is broadly inevitable that the internet occupies a space, not, as is sometimes said, of non-law, but one where national law struggles to impose itself, even when it would be legitimate to do so. The effect is that the national criminal law, which long ago ceased to pursue those who owned a banned book, now that the content can be uploaded, is led to incriminate those who become aware of it, in conditions which may lead to excessive harm to their rights. The cardinal principal of the legality of delicts and punishments is impaired by the technicality of the data processing world, even though that technical complexity allows for numerous derivatives, which endanger, in particular, personal data and private life.

The legislator and the judge are thus required to assess, albeit in a new field and under special conditions, the well-known balance between the objectives of protecting public order and respecting fundamental rights, in the context of offences which they define, or punish. This is classic: properly analysed, the criminal protection of private rights threatened by digitalisation does not raise any really new issues.

43 Law of 28 February 2017 regarding public security