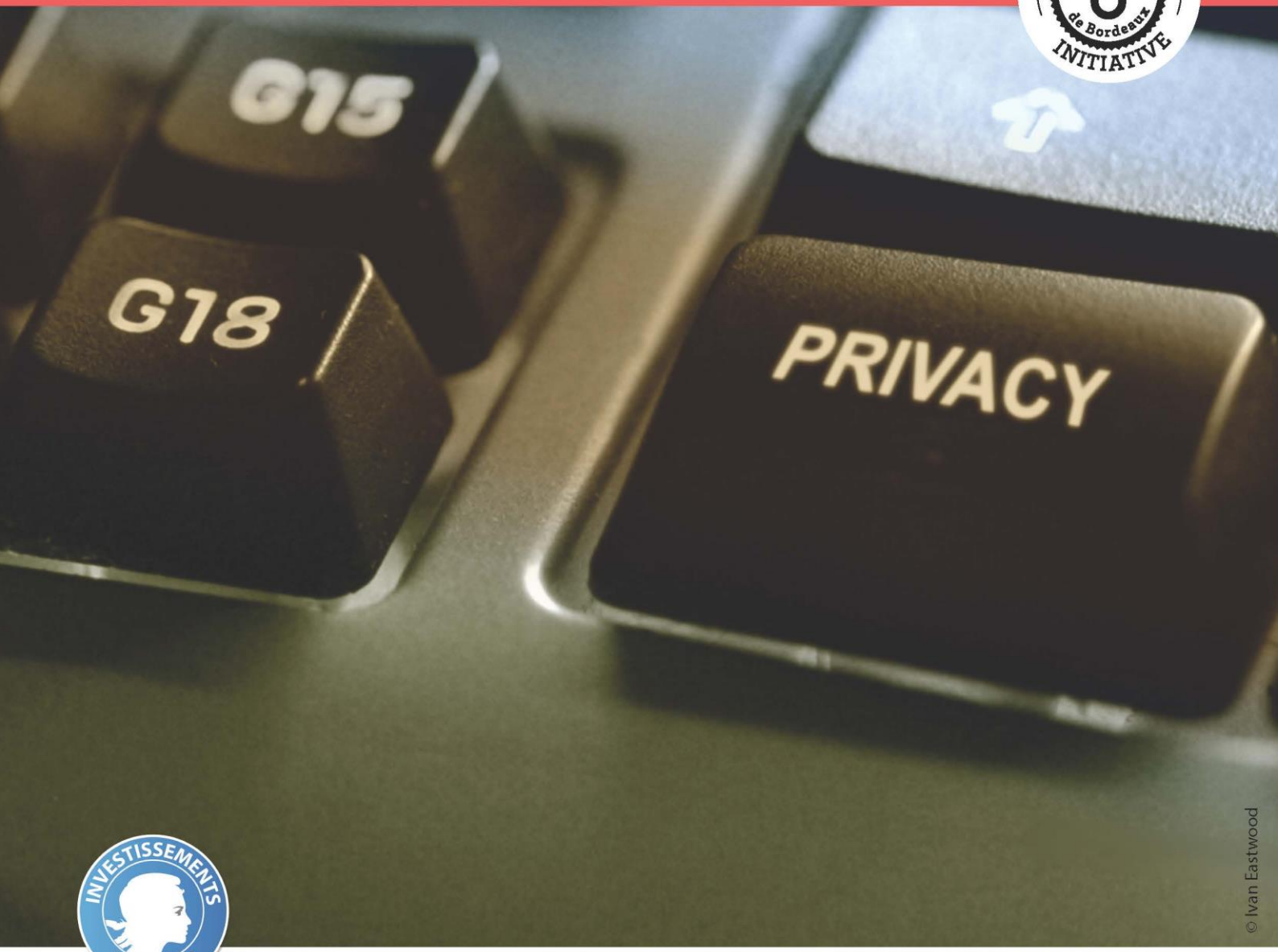
Issue | July 2015
No.2 | Special Issue: Privacy

Montesquieu Law Review

Criminal provisions for the protection of privacy: between the archaic and the ineffective

Mikaël Benillouche, Associate Professor, Faculty of Law and Political Science, Amiens



© Ivan Eastwood

Program supported by the ANR
n°ANR-10-IDEX-03-02

Faculté de droit et science politique

université de BORDEAUX

Criminal provisions for the protection of privacy: between the archaic and the ineffective

Mikaël Benillouche, Associate Professor, Faculty of Law and Political Science, Amiens

Suggested citation: Mikaël Benillouche, Criminal provisions for the protection of privacy: between the archaic and the ineffective, 1 Montesquieu Law Review (2015), issue 2, available at http://www.montesquieulawreview.eu/review.htm

In the words of Voltaire, *"[t]he pettiness of privacy can ally with the heroism of public life"* (1).

However, in positive law, the right to privacy benefits everybody and is even subject to a double level of protection, both civil and criminal, under French national law. Thus, in civil law, it is possible to combat all privacy violations. In criminal cases, only the most serious violations are punishable. This dichotomy is immediately duplicated insofar as the right to private life is proclaimed by the European Convention on Human Rights (2) and the French Civil Code (3).

The topic is at the heart of public debate, as demonstrated by various news stories about harassment on social media, done by assuming a child's identity before using their personal data.

In order to curb such abuses, criminal law has the delicate task of naming that which is forbidden. On that basis, an initial look at the development of positive law shows that the legislature meets social needs by adapting criminal law, including the creation of an offence of identity theft under Law No. 2011-267 of 14 March 2011 on guidance and programming for the performance of domestic security. This trend in positive law seemed essential as invasions of privacy have multiplied with the development of new technologies. However, a second glace leads us to qualify the above statement, by noting that the shortcomings of existing criminal provisions have not been fully addressed and that the new law is not as effective as had been hoped, particularly owing to a special type of dishonesty that is difficult to establish and also to relatively light penalties.

It would therefore appear that the French legislature is reluctant to reinforce the punishments to be imposed for invasions of privacy; this is certainly due to the risk of infringing other fundamental rights and freedoms, such as freedom of expression (4). Positive law therefore cannot give precedence to the right to private life over freedom of expression but must instead attempt to reconcile the two. Legislation protecting these fundamental rights and freedoms also provides for the possibility of restricting and establishing a framework for them.

The fact remains that the resulting balance is a shifting and fragile one: shifting because if infringements are not addressed, the right to private life becomes ineffective; fragile because existing criminal provisions need to be adjusted regularly in order to adapt them – and this, as Montesquieu put it, "with trembling hand" (5).

Lastly, it is tempting for the legislature to have, alongside traditional positive law as included in the Penal Code since 1970, more specific provisions that are more effective in combatting infringements of "digital identity", given that such infringements and the modalities thereof are

frequently encountered. How then can a specific right to the internet be established? And above all, how can its effectiveness be guaranteed in a field where it seems so difficult to legislate?

These are the questions that the legislature wishes to answer, the general consensus being that the conventional system is obsolete (section I) and to such an extent that its renewal seems inevitable (section II).

I) An outdated conventional system

Positive law was overhauled in 1970 as a response to a legitimate expectation of protection (section A), but that overhaul is now outdated (section B).

A) The initial expression of "legitimate expectation of protection"

The concept of privacy or private life is difficult to define. Thus, for the European Court of Human Rights, *"[...] the term "private life" must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings; furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life""* (6).

Law No. 70-643 of 17 July 1970 on strengthening the guarantee of individual rights of citizens nevertheless enshrined a subjective right to privacy (7): *"[e]veryone regardless of his rank, birth, fortune, functions present or future, has the right to respect for his private life"* (8).This protection is applicable to any person, on condition of being born. Moreover, any person, even widely known to the general public, must have a legitimate expectation of protection and respect for his or her private life (9).

Additionally, according to the provisions of Article 9, paragraph 2 of the Civil Code, *"[w]ithout prejudice to compensation for injury suffered, the court may prescribe any measures, such as sequestration, seizure and others, appropriate to prevent or put an end to an invasion of personal privacy; in case of emergency those measures may be provided for by interim order*".

In criminal law, only the most serious invasions of privacy are criminally punishable. The various offences are grouped together under Articles 226-1 and subsequent of the Penal Code, which sanction individual espionage, be it visual or auditory, and the exploitation thereof (10). The words or images concerned must necessarily have been intercepted in a private place. This is defined negatively as not being a public place, i.e. as a place that is not accessible to all (11). In derogation to ordinary law in this field, a prosecution may only be brought further to a complaint filed by the victim. Consequently, invasions of privacy fall within the scope of the narrow category of private crimes (12).

The offence is characterised where remarks made in a private place are recorded without the consent of the speaker (13). The clandestine aspect is the essential element of the offence (14). A prosecution may therefore only be brought when the offences have been characterised in all their aspects and particularly when the victims have been made aware of the breach of their rights (15). Obviously an act prescribed or authorised by criminal law (16) constitutes grounds for an exemption from criminal responsibility that is frequently applied, especially when the perpetrators of the infringement are investigative bodies acting in accordance with the rules contained in the

Criminal Procedure Code, which makes provision for the possibility of invading privacy in a variety of ways, such as telephone tapping (17).

This legal framework is now somewhat out of date.

B) An inevitably outdated legal framework

These offences have, since their creation, been amended several times. However, many invasions of privacy remain outside their respective scopes, owing in particular to developments in the methods involved in such invasions.

Criminal offences must be set down clearly and precisely; if not, they are likely to be struck down by the Constitutional Council (18) or even infringe the provisions of Article 7 of the European Convention on Human Rights (19). Consequently, criminal sanctions are necessarily limited and the criminal courts are confined to a strict interpretation of the same (20).

Communication technologies have, however, evolved considerably. As regards text messages sent by telephone (short message service or SMS), several decisions highlight the difficulties for positive law in protecting privacy. Thus, an employer who views text messages sent on the work phones used by employees has not invaded their privacy. Indeed, the text messages are deemed to be of a professional nature. Therefore, *"the employer is entitled to view them in the absence of the person concerned, unless said messages are established as being personal"* (21). Similarly, according to the Court of Cassation's Social Chamber *"folders and files created by an employee with software tools made available by his employer for the performance of his work tasks are presumed to be professional in nature so that the employer can access the same in his absence, unless the employee marks those folders and files as being private*" (22). Emails in an employee's work inbox were not marked as personal and could therefore be opened on a regular basis by the employer in the absence of the employee concerned (23). Similarly, letters sent or received by an employee on work premises are deemed to be of a professional nature, in such a way that the employer has the right to open that correspondence in the absence of the relevant party, unless said correspondence is marked as personal (24). The same solution governs checks conducted by an employer of websites visited by employees (25).

Moreover, the criminal offences concerned here do not apply to all acts that may invade privacy, particularly in cases of voyeurism, since the image of the victim is not recorded. Thus, the act of making a hole in the wall of a swimming-pool changing room in order to watch young women getting changed cannot be classified as one of the offences provided under Articles 226-1 and subsequent of the Penal Code. As violent offences cannot apply either (26), the only possible classification then lies in the damage to another's property (27). These gaps relating to acts of voyeurism were also highlighted by a Member of Parliament (28).

The same applies to acts of eavesdropping. Where voices are not picked up and/or recorded, this simple act is not criminally punishable.

In the absence of any legislative intervention, it therefore falls to the court to adapt its position depending on the case and the existing legal provisions.

II) A renewed system

Given this situation, the legislature could not remain indifferent and intervened to amend existing positive law with new provisions (section A), the effectiveness of which remains unclear (section B).

A) A social need relayed by law

Many invasions of privacy could therefore not be sanctioned by criminal law. Moreover, the development of new technologies and the online availability of personal information posted online by an increasingly young general public has increased the risk of invasion of another's privacy through the use of social media.

This is what led the legislature to intervene. Thus, Law n° 2011-267 of 14 March 2011 on guidance and programming for the performance of domestic security has created a so-called offence of identity theft (29) inserted into invasions of privacy (30).

Is now a criminal offence *"[t]he act of impersonating a third party or making use of one or more data of any kind allowing that person to be identified with a view to disturbing him or others or to damaging his honour or recognition, is punishable by one year's imprisonment and a €15,000 fine".* The second paragraph adds that *"[t]his offence is punishable by the same penalties when committed on an online public communication network"*.

Initially, it was planned to include this offence amongst violent offences. Indeed, through the use of a false identity, several malicious acts can be performed such as sending malicious messages to members of a person's entourage or even to set up a scam. It is thus not solely by the use of the internet that the offence is likely to be characterised. The law avoids employing the vague, imprecise concept of *"digital identity"* so often used in the media. The exact content of the concept remains unclear. Nevertheless, at the preparatory stage, names, nicknames and even pseudonyms used online were all mentioned as constituting identity. In this way, the law takes account of the current practice on electronic communication networks of a person calling himself or being known by a name other than his own.

However, was the creation of this offence really necessary? Indeed, it greatly resembles other classifications. Now, faced with a single act, only one charge may be brought (31). One might imagine a difficulty arising insofar as Article 433-19 of the Penal Code criminalises, in particular, *"1° using a name or part of a name other than that assigned by civil status [...] in an authentic or public document or in an administrative document drafted for public authority [...]*". A different scenario is also criminalised: that of not assuming one's own name, rather than that of assuming the name of another. As to Article 434-23 of the Penal Code, this criminalises the act of *"[a]ssuming the name of another person in circumstances that lead or could have led to the initiation of a criminal prosecution".* This charge was also brought in the case where the use of a third party's email address led to a risk of criminal prosecution (32). However, this is the criminal punishment of a form of obstruction of justice and not an attack on another's identity. So the two offences have different aims and protect different social values. Both charges can therefore be brought (33).

However, this criminalisation was merely a legislative step.

B) A relative effectiveness

These new provisions did not really halt the phenomenon (34), to the point where the legislature had to intervene again to criminalise conduct that, often using private details coming from the victim, led to bullying and harassment by some members of the social networks to which the victim belonged. Thus, Law No. 2014-873 of 4 August 2014 for real equality between women and men (35) created an offence of private harassment (36).

A Resolution of the European Parliament had previously drawn the legislature's attention to the phenomena associated with cyber-harassment and bullying, particularly involved children (37). Law No. 2014-873 prohibits acts falling within the scope of cyber-bullying. First, it extends the scope of Article 222-16 of the Penal Code, *"repeated sending of malicious messages sent through electronic communications".* The Law thus enshrines the case law that, at the cost of the least extensive interpretation of Article 222-16, had accepted that the offence which had previously only concerned phone calls and noise disturbance was also applicable to the sending of SMS messages *"when receiving an SMS is manifested by the emission of a sound signal by the mobile telephone of the recipient"* (38).

The new offence of harassment created by Law No. 2014-873 (mentioned above) was also accompanied by that of aggravating circumstances relating to the fact that the offence was committed "*through the use of a public online communication service*", which characterises the essential acts of cyber-bullying. Furthermore, the creation of the offence of submitting a person to repeated humiliation or intimidation or repeated invasions of privacy has the fight against cyber-harassment as its main objective. The wording adopted to define this new offence does not explicitly cover the commission of such acts through online communication, because, according to the *rapporteur* for the Senate's *Commission des lois* (Committee on Legislation), it would not have been possible "*to target new information technologies and communication only*"; however, the underlying intention is to allow the prosecution of acts of "*cyber-bullying*" (39).

In addition, Law No. 2004-575 of 21 June 2004 on confidence in the digital economy has also been amended slightly, particularly those provisions requiring ISPs and webhosts to *"contribute to the fight against the distribution and dissemination*" of illegal content, "*taking into account the public interest attached to the punishment of the denial of crimes against humanity; incitement to racial hatred; hatred of persons on grounds of gender, sexual orientation, gender identity or disability; child pornography; incitement to violence, including incitement to violence against women; and offences against human dignity*" (40).

Furthermore, the Law added incitement to hatred or violence against a person or group of persons on grounds of gender, sexual orientation, gender identity or disability to the list of offences that intermediate internet techniques must combat (41). The legislature therefore intended to punish cyber-harassment in its various forms. However, in doing so, it adopted a broad standard that can be applied to other scenarios. It should be noted that the Constitutional Council concluded that the Law complied with constitutional requirements (42).

In conclusion, the legislature would appear to have the greatest difficulty in containing the most serious invasions of privacy by resorting to criminal law, given the myriad ways in which this subjective law can be ignored. However, its reluctance to adopt overly extensive criminal provisions can only be welcomed in that it allows the necessary respect for private life to be

reconciled with other fundamental rights and freedoms. The fact remains that these frequent legislative interventions would appear to bear witness to a positive law in search of its own identity between prevention and punishment, and which fails to stamp out events with sometimes irreversible consequences (43).

Notes:

(1) *Essai sur les mœurs et l'esprit des Nations*, 1756.
(2) Article 8.
(3) Article 9.
(4) Article 10.
(5) *The Spirit of Laws*, 1748.
(6) ECHR, *Amann v. Switzerland*, Application No. 27798/95, 16 February 2000, ground 65.
(7) Proclaimed in Article 9 paragraph 1 of the Civil Code.
(8) CA Paris, 17 May 1966 D. 1966, p. 749; Cass. 1st Civ., 23 October 1990, Bull. Civ.1990 I, No. 222.
(9) ECHR 24 June 2004, *Von Hannover v. Germany*, Application No. 59320/00, § 69.
(10) The main criminality under Article 226-1 of the Penal Code which provides:
"A penalty of one year's imprisonment and a fine of €45,000 is incurred for any willful violation of the intimacy of the private life of other persons by resorting to any means of:
1° intercepting, recording or transmitting words uttered in confidential or private circumstances, without the consent of their speaker; 2°
taking, recording or transmitting the picture of a person who is within a private place, without the consent of the person concerned.
Where the offences referred to by the present article were performed in the sight and with the knowledge of the persons concerned without their objection, although they were in a position to do so, their consent is presumed".
Article 226-2 of the Code criminalises "*the keeping, bringing or causing to be brought to the knowledge of the public or of a third party, or the use in whatever manner, of any recording or document obtained through any of the actions set out under Article 226-1*". Article 226-3 of the Criminal Code creates a series of offences to prevent the acquisition of technical devices that could be used to invade. Article 226-4 punishes the act of entering or unlawfully occupying the residence of another.
(11) Thus, a prison is not a public place (CA Paris, 19 November 1986 D. 1987 somm. 141). The same applies to the deliberation room at an assize court (CA Amiens, 4 February 2009, JCP ed G No. 15, 8 April 2009, II, 10063).
(12) Article 226-6 of the Criminal Code.
(13) Cass. crim., 19 May 1981, Bull. crim., No. 161.
(14) Cass. crim., 4 March 1997, Bull. crim., No. 83.
(15) Cass. crim., 4 March 1997, Bull. crim., No. 83.
(16) Article 122-4 paragraph 1 of the Penal Code.
(17) Articles 100 to 100-7 and 706-95 of the Criminal Procedure Code.
(18) Cons. Constit., 4 May 2012, No. 2012-240 QPC.
(19) ECHR 15 November 1996, *Cantoni v. France*, Reports 1996-V.
(20) Article 111-4 of the Penal Code.
(21) Cass. com., 10 February 2015, No. 13-14779.
(22) Cass. soc., 18 October 2006, No. 04-48025.
(23) Cass. soc., 15 December 2010, No. 08-42486.

(24) Cass. soc., 11 July 2012, No. 11-22972.
(25) Cass. soc., 9 February 2010, No. 08-45253.
(26) Cass. crim., 5, 2010, No. 10-80050.
(27) Articles 322-1 and subsequent of the Penal Code.
(28) Written Question No. 425, OJ Senate, 27 December 2012.
(29) A. Lepage, « Le délit d'usurpation d'identité : questions d'interprétation », JCP ed G 35, 29 August 2011, doctr.913.
(30) Article 226-4-1 of the Penal Code.
(31) Article 4 of Protocol No. 7 to the European Convention on Human Rights establishing the rule of *non bis in idem*.
(32) Cass. crim., 20 January 2009, No. 08-83255.
(33) This is an exception to the *non bis in idem* rule (Cass. crim., 3 March 1960, Bull. crim., No. 138, RSC, 1961, 105, obs. Legal) accepted by the European Court of Human Rights (ECHR, 30 July 1998, *Oliveira v. Switzerland*, Reports 1998-V).
(34) http://www.lemonde.fr/societe/article/2013/08/01/.html
(35) Cons. Const., 31 July 2014, No. 2014-700 DC.
(36) Article 222-33-2-2 of the Penal Code.
(37) European Parliament non-legislative resolution No. 2012/2068 (INI), 20 November 2012.
(38) Cass. crim., 30 September 2009, No. 09-80373, JurisData No. 2009- 049991, Dr. pén. 2009, pers. 147, obs. Mr. Véron, Comm. com. electr. 2009, pers.115, Rev. pén. 2010, p. 899, obs. V. Malabat.
(39) JO, Senate Debates, session of 17 September 2013, p. 8269.
(40) Articles 6 and 7-I, paragraph 3 of Law No. 2004-575 of 21 June 2004.
(41) Article 24, paragraph 9 of the Law of 29 July 1881.
(42) Cons. Const., 31 July 2014, No. 2014-700 DC.
(43) www.lefigaro.fr/actualite-france/2014/10/23/01016-20141023ARTFIG00199.php (paywall)