Contents this issue

Editorial:
Olivier Dutheillet de Lamothe, Honorary President of the Social Section, Conseil d’Etat, Honorary member of the Constitutional Council 3

The right to respect for private life and the right to respect for privacy: the case for an aggiornamento
Associate Professor Hubert Alcaraz, Université de Pau et des pays de l’Adour 6

Criminal provisions for the protection of privacy: between the archaic and the ineffective
Associate Professor Mikaël Benillouche Faculty of Law & Political Science, University of Amiens 13

The right to respect for private life: an effective tool in the right to be forgotten?
Associate Professor Maryline Boizard Faculty of Law & Political Science, University of Rennes 1 20

The right to privacy: twenty years of constitutional recognition
Estelle Bomberger, Lecturer, Sciences Po and the Institut Catholique de Paris 27

Privacy and political assassinations in France during the Trois Glorieuses: the meanderings of Orleanism
Associate Professor Sophie Delbrel. University of Bordeaux 34

Privacy and the disclosure of administrative documents: a well-guarded secret?
Marie–Odile Diemer, Lecturer, University of Bordeaux 41

The war on terror and the protection of personal data
Philippe Ch.–A. Guillot, Professor of International Relations, French Air Force Academy 47

The personal life of the employee versus the interests of the company
Associate Professor Chantal Mathieu, University of Franche–Comté 55

Privacy and ethics
Associate Professor Olivier Pluen, Université des Antilles et de la Guyane 64

Invasions of privacy via the internet: aspects of private international law
Associate Professor Jean Sagot Duvauroux, University of Bordeaux 69

Transparency in public life and respect for private life
Associate Professor Messaoud Saoudi, Université Lumière Lyon II 77

The fatal metamorphoses of image rights
Professor Isabelle Tricot–Chamard, Kedge Business School, Bordeaux 84
Editorial

Privacy: a comparative perspective
Olivier Dutheillet de Lamothe, Honorary Section President, Conseil d’Etat; honorary member of the Constitutional Council

Under the terms of Article 8 of the European Convention on Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950 and ratified by France pursuant to Law n° 73-1227 of 31 December 1973: “Everyone has the right to respect for his private and family life, his home and his correspondence”.

The European Convention is at the root of the recognition of the right to respect for private life as a constitutional right in French law.

Indeed, this right features neither in the 1789 Declaration of the Rights of Man and of the Citizen, nor amongst those economic and social principles “being especially necessary to our times” in the Preamble to the 1946 Constitution. For a long time, the Constitutional Council saw therein a purely legislative right protected by Article 9 of the Civil Code, under the terms of which “everyone has the right to respect for his private life”.

The Constitutional Council initially recognised the right to respect for private life as an aspect of individual freedom protected by Article 66 of the Constitution. The decision of 13 August 1993 on the Law on Immigration Controls enshrines a very broad conception of individual freedom within the meaning of Article 66 of the Constitution, which includes the freedom to come and go (recital 3), freedom to marry (recitals 3 and 107) and, lastly, the protection of personal data (recitals 121 and 133).

That decision was confirmed even more clearly by a decision of 18 January 1995, according to which “ignorance of the law on respect for private life can be of such a nature as to restrict individual freedom” (Decision n° 94-352 DC, 18 January 1995).

The Constitutional Council then detached the right to respect for private life from individual freedom, placed under the supervision of the judicial authority, to make it an element of personal freedom or freedoms of the individual, which arise from Article 2 of the 1789 Declaration of the Rights of Man and of the Citizen.

This is how the decision of 23 July 1999 on the Law establishing Universal Health Coverage enshrines the right to respect for private life as an element of personal freedom (Decision n° 99-416 DC, 23 July 1999, recital 45).

Ten years after the 1993 decision, the decision of 13 March 2003 on the Law on Internal Security enshrines a broad conception of personal freedom and its link with individual freedom: “it is the task of the legislature to reconcile, on the one hand, the prevention of breaches of public order and the search for offenders, both necessary in order to safeguard constitutional rights and
principles; and, on the other hand, the exercise of constitutionally guaranteed freedoms, which include the right to come and go and the right to respect for private life, protected by Articles 2 and 4 of the 1789 Declaration of the Rights of Man and of the Citizen, as well as individual freedom, which is placed under the supervision of the judicial authority by Article 66 of the Constitution” (Decision n° 2003-467 DC, 13 March 2003, recital 8).

The Constitutional Council gives the principle of respect for private life a particularly extensive field of application: the decision of 2 March 2004 on the Law on Adapting Justice to the Changing Face of Crime extends the concept of personal freedom to the inviolability of the home and to the confidentiality of correspondence.

It also gave the principle very broad scope:

– by requiring, in respect of the most serious infringements of respect for private life, intervention on the part of the judicial authority in relation to search and seizure and also in relation to telephone tapping and sound and film recordings of certain locations and vehicles (Decision n° 2004-492 DC, 2 March 2004);

– by deleting certain metafiles likely to infringe the freedoms of citizens: the Council thus ruled that the processing of personal data to be used in identifying consumer credit agreements entered into by natural persons, the household credit repayment incidents linked to those credit agreements, together with the information relative to excessive debt and compulsory liquidation, in order to prevent situations of excessive debt earlier and more effectively by furnishing financial establishments and bodies with elements allowing them, when granting a loan, to assess the solvency of natural persons applying for credit or standing as guarantor, infringes the right to respect for private life in such a way that it cannot be considered proportionate to the objective pursued “having regard to the nature of the registered data, the scope of processing, the frequency of usage, the large number of people likely to have access to it and the inadequacy of guarantees relating to access to the register” (Decision n° 2014-690 DC, 13 March 2014).

The expansion of respect for private life in France is part of a general trend across Europe:

– All European countries have acceded to the European Convention on Human Rights, which expressly recognises the right to respect for private life;

– The Charter of Fundamental Rights of the European Union also recognises the right to respect for private life in particularly clear-cut terms as, under Article 7: “Everyone has the right to respect for his or her private and family life, home and communications”;

– Recent Constitutions such as Spain’s Constitution expressly recognise this same right;

– Lastly, as an extension of France’s Informatique et libertés Law n° 78-17 of 6 January 1978 on computer technology and freedoms, the European Union adopted the Data Protection Directive in 1995.

In this respect, the European situation is very different to that of the United States.
In the American Constitution, as in the French, there is no recognition of the right to respect for private life.

This right was recognised for the first time by the Supreme Court in its 1965 decision in *Griswold v Connecticut* (381 US 479), in which it held that “[w]e deal with a right of privacy older than the Bill of Rights – older than our political parties, older than our school system. Marriage is a coming together for better or for worse, hopefully enduring, and intimate to the degree of being sacred”.

The Supreme Court went a step further in the recognition of that right in its famous decision in *Roe v Wade* (419 US 113) on abortion, in which it stated that: “[t]his right of privacy, whether it be founded in the Fourteenth Amendment’s concept of personal liberty and restrictions upon state action, as we feel it is, or, as the District Court determined, in the Ninth Amendment’s reservation of rights to the people, is broad enough to encompass a woman’s decision whether or not to terminate her pregnancy” and found that “[w]e, therefore, conclude that the right of personal privacy includes the abortion decision, but that this right is not unqualified and must be considered against important state interests in regulation”.

In practice, the scope of the respect for private life is limited in the United States, owing to two factors:

– On the one hand, its very liberal case law on freedom of speech, which excludes any restriction on that freedom, particularly as regards defamation or incitement to racial hatred: for Americans, nothing must restrict expression and the clash of ideas that must regulate themselves through their free interplay, like the market for goods and services.

– Through the doctrine of judicial deference to the Executive and the President in matters of national security: this explains the development of programmes that are highly intrusive in terms of individual freedoms, both within the United States and without, such as the National Security Agency’s mass surveillance programme known as PRISM.
Right to respect for private life and the right to personal privacy: the case for an aggiornamento
Hubert Alcaraz, Associate Professor, Université de Pau et des pays de l'Adour


At the heart of a shifting reality, the person has seen his place and aspirations reformulated, while the line between public and private, constitutive of contemporary societies, has been blurred. And yet, at the same time, the legal system has continued to implement concepts, some of which probably merit a second reading. The concept of "right to respect for private life" (1) is one of these. Born and considered in the field of sociology, "private" no longer seems to lend itself as easily to its implementation in the legal sphere. Although French law remains committed to the "right to respect for private life", there is a great deal of confusion between "privacy", "private life" and "l'intimité" (literally, "intimacy") or personal privacy (2). Privacy generates as much self-determination on the part of the individual as it does reserve; and, while privacy is always involved, two different wishes are expressed: one facing inwards and the other outwards.

So why not provide litigants with a more operational tool by promoting a right to personal privacy which would cover only one of the rights that fall within the category of "right to respect for private life"? This would not cover the individual’s wish for self-determination, i.e. the guarantee of his existential choices, but an additional element, indicating his control over information concerning his own person: the right of every person that elements relating to his or her personal life remain undisclosed; elements which are, by their nature, unknown to third parties and over which each person must consequently have control. Similar but not to be confused with the "right to secrecy of private life", the reference to the right to personal privacy would appear to be more accurate and effective.

More exactly, it takes better account of case law: the French courts and tribunals do not protect private life as a whole, but only part of it, corresponding to the right to personal privacy as defined here. This is more effective, on the one hand, insofar as developments in terms of technology and behaviour invite the legal system to cast off the shackles of a distinction between public and private which, in space, loses its substance; secondly, because the "right to respect for private life", as it is currently implemented, often dissipates into mere procedural guarantees.

The right to personal privacy does not purport to address all issues but offers a different direction which serves to set aside recurring conceptual problems. Firstly, it demolishes the spatial criterion: the vain distinction between private and public life is repelled and when the individual leaves his home, "privacy follows". Next, this right sets aside the reserve of absolute jurisdiction held by the ordinary courts: the administrative courts may thus establish their jurisdiction without controversy and without, for all that, the intervention of the ordinary courts being excluded or proving problematic (3). Finally, whereas currently the constitutional court cannot handle a fundamental
right that has substance, it could go further than a simple response to referrals, having a complementary and reinvigorated conception of personal freedom.

Therefore, if the protection of privacy should be rethought, it is particularly in order to shed light on the added value that the reference to the right to personal privacy can produce. An examination of the current state of the law, without masking the French legal order’s restraint *vis-à-vis* the right to personal privacy, shows the benefit of identifying that right (section I), the better to protect a sphere of reserve around the person more effectively (section II).

I – The right to personal privacy: an identified law

In French law, the concept of *intimité* or personal privacy plays a marginal role. Before the Law of 17 July 1790 was passed (4), only Article 15, paragraph 2 of the Law of 29 July 1881 on press freedoms provided that proof of the truth of defamatory statements is prohibited in three cases, including "where the imputation concerns the person's privacy". In reality, the disregard for the right to personal privacy is the consequence, firstly, of a lack of differentiation with the right to respect for private life (section A); and, secondly, a failure to distinguish it from some "neighbouring" rights (section B).

A – The distinction between the right to respect for private life and the right to personal privacy

Efforts to define "privacy" have not been in vain. On the one hand, some authors have understand the concept broadly so as to include the right to a normal family life, the "right to sexual life" (5), "respect for the appearance of personality", anonymity, and freedom of conscience and opinion (6). Thus, this conception may be likened to privacy (7) or private life as conceived by the European Court of Human Rights (8). On the other hand, part of the doctrine takes a stricter line and prefers to speak of "the right to keep the privacy of one's existence secret" (9) or the "right to personal privacy" (10). However, the preparatory work of the Law of 17 July 1970 (11) seemed to be clear and, within Article 9 of the Civil Code, paragraph 1 covers "private life" while paragraph 2 punishes "invasion[s] of personal privacy", which scenario alone authorises seizure and sequestration (12). However "the delineation has become all the more difficult as privacy has sometimes ceased to be considered in relation to the necessary protection of a sphere of privacy for the person in relation to a certain right to be different" (13).

As regards constitutional law, in order to enshrine the right to respect for private life, the suggestion was made that a paragraph 2 be added to Article 66 of the Constitution, stipulating that "everyone has the right to respect for his private life and the dignity of his person" (14). After much prevarication, in 1999, affirming that the freedom proclaimed by Article 2 of the Declaration of 1789 "implies respect for privacy" (15), the Constitutional Council established the "respect for private life" as a "constitutionally guaranteed freedom" (16). However, it is unclear whether this right thereby gained any more autonomy because its juxtaposition to personal liberty breeds confusion. Nevertheless, although their respective normative sources are sometimes similar (17) how can these rights be confused? Admittedly some observers seem to suggest such an interpretation (18); however, nothing in the reading of constitutional case law confirms it. On the contrary, although it relates to an individual’s private life, personal freedom enshrines protection for manifestations of personal liberty externalized on the social scene, i.e. a sphere of autonomy. It therefore complements the protection afforded by the right to personal privacy, but does not encompass it. Continuing the identification of the right to personal privacy, the clarification of the differences with a number of related concepts serves to confirm it.
B – The distinction between the right to personal privacy and "neighbouring" rights

Caution with regard to the right privacy also emerges as a consequence of the choice made in national case law which, like its European counterpart (19), often intends to bring together the various legal instruments protecting private life under a single law. Civil law thus recognises that each person has the right to uphold his honour, i.e. the feeling that one has one’s own dignity and the sense that others feel or experience it. Without denying that much of the harm done to individual reputations is caused by the invasion of a person’s private sphere, it is possible to be more specific. On the one hand, the right to personal privacy aims to establish the individual’s control over the distribution of a number of aspects relating to his personal life, while the right to honour aims to protect the reputation of individuals against unlawful damage to reputation. Moreover, the scope of these rights is also quite distinct: the right to honour covers defamatory allegations relating to private life, but also those related to public activities.

As for image rights, traditionally ranked among personality rights, these were only recently "emancipated" from the right to respect for private life (20). The courts have increasingly found that it was not to be confused with the right to personal privacy and could be subject to infringements related to a person’s public life (21). It covers the reproduction and representation of the human form in a visible and recognisable way (22), so that there are interferences that solely infringe image rights: these are little more than but the capture, in places open to the public, of an image of a person subsequently published without his consent.

Lastly, in France, where the protection of personal data is involved, the guarantee established by the Law of 6 January 1978 (23) covers a wider sphere than that of the right to personal privacy. Indeed, in light of the protection of personal data, the nature of the information in question is irrelevant; it is sufficient that said information be directly or indirectly nominative, regardless of whether it is private or not. Furthermore, from the point of view of the legal system, the protection of personal data can be analysed first in terms of rights of information rights, access, correction and objection; then in terms of principles relating to data quality and the legal basis of the data collection concerned; and finally, in terms of the data controller’s safety obligation, under the supervision of an independent authority (24). It is not absurd to consider that the protection of personal data relates more to a desire for self-determination in the social scene, rather than in a sphere of reserve (25).

Rather than being connected to the protection of personal data or personal freedom, privacy ought to refer to it. The inclusion of privacy and the protection of personal data within a wider personal freedom is the result of a reversal of perspectives. At the price of its details, the advantage of using the right to personal privacy is highlighted; once identified, we manage to highlight the effectiveness of this right.

II – The right to personal privacy: an effective right

The effectiveness of the right to personal privacy requires, on the one hand, that it combine material content and formal guarantees (section A) and, on the other, that the relevant reasoning be freed from the distinction between public and private spaces (section B).

A – A right combining material content and formal guarantees

The right to personal privacy has content whilst benefiting from formal guarantees. Its content covers two aspects. On the one hand, it is possible to identify elements the private nature of which
is established, this being the minimum amount of content that is likely to constitute a common denominator for all individuals. Furthermore, above or below that minimum level, nothing is anybody's business: the individual is free to agree to temporary restrictions on that minimum level or, conversely, to make it known that he expects a higher level.

On the basis of material content, we must first of all mention information relating to health. Doctor–patient confidentiality is one that maintains the "closest ties with the protection of privacy" (26) and the Code de la santé publique (Public Health Code) structures confidentiality as to health status (Art. L. 1110–4), also protected by the Penal Code (Arts. 226–13 and 226–14). There must also be a place for the human body, but physical intimacy or privacy ought not to be confused with the physical reality of the human body, and it must be considered in light of each society’s respective customs. Moreover, the will of the individual also has its place: if a person does not wish to give information on or expose parts of his anatomy that are not usually seen, he is protected by the law. Lastly, information about his sexuality is also covered (27). This does not cover the freedom to establish and maintain sexual relations, the right to engage in defined sexual practices, or sexual orientation. The right cannot be reduced to mere procedural safeguards (28) and thus has real content whilst being supplemented by formal guarantees.

French law has developed a number of mechanisms, such as the right to confidentiality of communications and the right to the inviolability of the home, which appear as formal guarantees for the right to personal privacy. It is understood that with these rights, the legal system aims to implement a guarantee safeguarding a medium for privacy, i.e. a channel through which it is deemed to be deployed, rather than a space or an act that would, in essence, be private. The aim is to posit a presumption in order to protect the various forms that the private sphere can take or occupy. Thus the right to the inviolability of the home keeps third parties away from a space that is viewed geographically, as an area or a territory (29).

The guarantee of the inviolability of communications follows the same logic (30): the law establishes a presumption that all that is transmitted through the communication process (31) should remain undisclosed. Regardless of the material content of the communication (32), the mere fact of disclosing, intercepting or retaining the elements communicated is an infringement of that right. It is the interference of individuals who are not party to the communication (or in the home), quite aside from any consent from the interested parties, that constitutes the proper basis for analysis. Complementing its material content, these two elements form the measures specific to the right to personal privacy, which is not hampered by the distinction between public and private spaces (33).

B – A right granted to the distinction between public and private space

The distinction between public and private spheres, which is always difficult to establish, currently suffers from a profound relativisation. Moreover, subordinating the implementation of a fundamental right to the identification of a space called "private" acts as an impediment in a time of unspecific spheres. The right to personal privacy eliminates the spatial criterion by leaving room for subjectivity and individual will. Beyond the core elements discussed above, it is the meaning that the individual wishes to imprint on this or that act, and what such and such information reveals of his personality, which will prove decisive. The applicability of the law in circumstances where it is difficult to speak of "private life" is thus assured.
This observation is necessary, for example, in professional matters. In labour law, the "right to respect for private life" is difficult to invoke when it comes to examining the status of an employee’s e-mail of the employee, or the opportunity to review the contents of the hard drive of a computer belonging to the employer. Moreover, the Court of Cassation recognises that "the employee is entitled, even at the time and place of work, to personal privacy" (34). The situation is quite similar in matters involving insurance law (35).

In fact, the reference to privacy is also useful in those scenarios that are "reactivated" by technological progress. We may think, for instance, of conflicts between the right to personal privacy and freedom of information: a trend in case law can be picked out which, in settling such conflicts, makes use of the expression "right to respect for private life", a concept that corresponds to the right to personal privacy: the court’s discretion is guided by what the information disseminated will reveal about the person, quite aside from any consent, and where his actions were the manifestation of an implicit desire for reserve (36). Moreover, these solutions may be transposed to the reconciliation between safeguarding public order and the rights of individuals. Behind the subject of rights (the human being), it is the personality that emerges and room must be made for that which emanates from the individual’s personality behind certain details which are not, in principle, disclosed. For this, consideration must be given to what exactly those details reveal about the individual himself (37). Faced with these developments, there is no reason to challenge the scientific interest of the concept of privacy. However, while talk of "respect for private life" remains correct, this concept, in the legal field, covers different realities. Its uncertainty, so beneficial in the social sphere, increasingly rules it out from a legal standpoint. Without denying or disparaging it, action must be taken and, in order to a sphere of reserve around the individual, preference given to the right to personal privacy.

Notes:

(4) R. Lindon, « Les dispositions de la loi du 17 juillet 1970 relatives à la protection de la vie privée », JCP, I, 2357
(8) F. Sudre, « Les aléas de la notion de “vie privée” dans la jurisprudence de la Cour européenne des droits de l’homme », in Mélanges en hommage à Louis Edmond Pettiti, Bruxelles, Bruylant, 1999, p. 687
(11) Art. 9, Civil Code; Cf. speech delivered by J. PLEVEN, Minister of Justice, JORF, Débats, A.N., 28 May 1970, p. 2068
Cf. Also Art. 226-1, Penal Code, and Arts. 435 or 247, Civil Procedure Code, which cover the “intimacy of private life.”


Comité consultatif pour la révision de la Constitution, Rapport remis le 15 février 1993 au Président de la République (Consultative Committee for the Amendment of the Constitution: Report submitted to the President of the Republic, 15 February 1993)


The "respect for private life" was protected by the reference to personal liberty (December 76-75 No. DC 12 Jan. 1977) and to personal liberty, freeing it from the former only for it to spend a period in the orbit of the latter (Dec. No. 88-244 DC of 20 July 1988; see also No. 94-352 DC Dec 18 January 1995).

The Constitutional Council indifferently covers Articles 2 and 4 of the 1789 Declaration in its Decision No. 484 of 20 November 2003 DC.


F. Sidre (dir.), Le droit au respect de la vie privée au sens de la CEDH, Bruxelles, Bruylant, 2005.


Cass. 1er Civ, 12 December 2000; 2nd Civ., 24 April 2003. "The violation of the respect due to private life and the infringement of the right of each person to his or her image are separate sources of harm".


P. Kayser, op. cit., p. 385.


This is any process of transmitting messages between specific persons by any technical means.

Moreover, Art. 226–15 of the Penal Code makes no mention of the substantive nature of the
content of the correspondence. As to the domicile, cf. the sanction for keeping a person within the confines of their home.

(33) For details, H Alcaraz, op. cit., p. 273 and s.


(37) Cons. const., Decision No. 2004–492 DC of 2 March 2004, *Loi portant adaptation de la justice aux évolutions de la criminalité* ; cf. recital no. 65: as regards the sound system and fixing of images of certain places or vehicles, the court was asked to distinguish between images that are relevant to the prosecution of the offence and other images.
Criminal provisions for the protection of privacy: between the archaic and the ineffective

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


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 appeared essential as invasions of privacy have multiplied with the development of new technologies. However, a second glance 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 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 to the list of offences that intermediate internet techniques must combat: incitement to hatred or violence against a person or group of persons on grounds of gender, sexual orientation, gender identity or disability (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:
(2) Article 8.
(3) Article 9.
(4) Article 10.
(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.
(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).

(16) Article 122–4 paragraph 1 of the Penal Code.
(17) Articles 100 to 100–7 and 706–95 of the Criminal Procedure Code.
(20) Article 111–4 of the Penal Code.
(27) Articles 322–1 and subsequent of the Penal Code.
(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_.


(34) http://www.lemonde.fr/societe/article/2013/08/01/.html


(36) Article 222–33–2–2 of the Penal Code.


(39) JO, Senate Debates, session of 17 September 2013, p. 8269.


(41) Article 24, paragraph 9 of the Law of 29 July 1881.


(43) www.lefigaro.fr/actualite-france/2014/10/23/01016-20141023ARTFIG00199.php (paywall)
The right to respect for private life: an effective tool in the right to be forgotten?

Maryline Boizard, Associate Professor, IODE UMR CNRS, Faculty of Law and Political Science, University of Rennes 1


The right to be forgotten is not explicitly enshrined in positive law. Nevertheless, some legal provisions lead to it. Article 9 of the French Code Civil, Article 7 of the Charter of Fundamental Rights of the European Union, and Article 8 of the European Convention on Human Rights, which all enshrine the right to respect for private life; but also Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1) transposed into French law by an amendment to the Informatique & Libertés Act of 6 January 1978 – without making explicit provision for a right to be forgotten, all contain prerogatives that lead to such a right. French and European case law has been able to adapt and respond to critical cases. Since its inception, the Commission Nationale Informatique et Liberté (CNIL) has discussed the issue of the right to be forgotten in most of its annual reports.

Forgetfulness is the capacity to forget that an individual develops because it is necessary. In that perspective, the act of forgetting fulfils a constructive, even restorative, function. Forgetting modulates the memory in order to “close the doors and windows of consciousness from time to time” (2). Nevertheless, the advent of digital technology no longer allows forgetting to come into play under similar conditions and profoundly changes the situation under the combined influence of three factors (3). Firstly, the emergence of digital technologies which serve to store data with little or no risk of alteration. Next, the expansion of the internet, which offers potential access to a large proportion of stored data. Lastly, the use of search engines, which guarantees genuine access to a large proportion of stored data. As the act of forgetting no longer happens naturally, claims as to a right to be forgotten have emerged, which would be an individual’s prerogative to require that certain events or certain data concerning him no longer be accessible as they are no longer current (4).

In practice, the initial decisions that had to rule on the existence of a right to be forgotten related to objections raised by persons involved in legal cases to the reporting of the facts several years after these had taken place. The argument typically invoked was the right to respect for private life, of which the right to be forgotten is often seen as a counterpart. More recent applications have, however, encompassed a variety of situations that go beyond the framework of the right to respect for private life. They may relate to the publication of a person’s criminal conviction several years before; disseminating distasteful pictures or disadvantageous when viewed now; even the storage of medical data in data banks. It is therefore a matter of securing the obliteration of – now mostly digital – traces of a past that a person wishes to forget or have others forget.
In this context, the right to respect for private life would appear to be increasingly irrelevant in addressing the issue of the right to be forgotten. This why case law now turns more readily to the legal rules for the protection of personal data that offers more flexibility to the courts. The limits of the right to respect for private life as a basis of the right to be forgotten (section I) result in it being set aside in favour of measures for the protection of personal data (section II).

I – The limits of the right to respect for private life

In order to be protected by the right to respect for private life, acts or data ought to fall within the remit of private life. However, the most recent case law on the subject – both European and French – shows that the right to be forgotten is not confined to the private lives of individuals. Two major differences between the right to respect for private life and the right to be forgotten mark the limits of the former as the basis of the latter. The first difference lies the time criterion (A); the second in the very concept of private life (B).

A – The time criterion

The definition given to the concept of forgetting shows that time is a necessary component. By that single finding, it becomes a characteristic of the right to be forgotten. Time is not, however, a criterion for classifying private life. However, the time factor how a public act may be protected by the right to be forgotten when it cannot be by the right to respect for private life. Conversely, it also means that the same act can sometimes be protected by the right to be forgotten and sometimes not.

In the matter of Diana Z. v Google of 15 February 2012, the tribunal de grande instance (regional court) at Paris condemned the famous search engine for invading the privacy of a woman who, twenty years earlier, had taken part in a pornographic video under a false name and whose real name had been associated with pornographic websites. The court characterized the “manifestly unlawful disturbance” by including a direct reference to the right to be forgotten “if, when she made this film, Ms. Z. necessarily accepted necessarily a certain distribution even then she did not consent a priori to its digitization and dissemination on the internet; and, while this video does not itself reveal scenes of private life, the fact remains that this film reflects a particular time in the life of the young woman, who wishes to exercise her right to be forgotten”. The court differentiated between the time criterion and private life, the former becoming essential in the enshrinement of the victim’s right.

In the matter of Google Spain v AEPD of 13 May 2014 (5), a Spanish citizen had asked a newspaper in 2009 to remove a publication concerning a seizure of property resulting from the non-payment of debts incurred but eventually paid back to Social Security several years previously. Following a request for a preliminary ruling on the interpretation of measures for the protection personal data, the ECJ established the principle of a right to be forgotten for people whose surname links to information concerning them. This right is not absolute. Beyond identifying the specificity of search-engine activity, the decision establishes the time criterion as a determining criterion for being forgotten. Here again, no reference is made to an invasion of privacy.

The ECJ decision was echoed in the French courts: the regional court at Paris handed down a decision on 19 December 2014, ordering the search engine to remove a link from its search results (6). Google was condemned for ignoring a request made by the interested party to be forgotten on the basis of the right to be forgotten, which request concerned an article about his
conviction in 2006 for fraud. In order to recognize that right, the court relied heavily on the age of the case as almost eight years had elapsed between the publication of the article and the filing of the complaint.

B – The concept of privacy
For the ECHR, privacy is a broad, shifting concept (7). In 1992, the Court stated that: “it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings” (8). Nevertheless, restricting the right to be forgotten to an individual’s personal data atrophies the scope of that right because it makes identifying the public or private nature of the information disclosed a key element in the protection afforded to the person. The qualification is not always obvious. We must in particular consider whether the initial dissemination of information exhausts the right to privacy. Case law is divided (9).

Media coverage of an event at the material time may have an impact on the legal treatment of the exploitation of the facts which gave rise to the event. Whenever a news story has had a great deal of media coverage, freedom of expression allows the story to be discussed without any objections raised on grounds of the right to be forgotten. In this area, the Court of Cassation appears to make the following distinction: either the facts have been sufficiently disclosed to be considered public, in which case the replay not affect privacy and blocks the right to be forgotten (10); or the facts were revealed by the person himself and, having formerly held the opposite view, that fact should not come into play: the re-disclosure by a third party therefore crystallizes a new invasion of privacy (11). This distinction is however not always followed. Disclosure by the applicant may also be seen as a justification. In reality, the distinction ought not to be based on a qualification of the facts but on the public interest in knowing the information.

Technological progress has led the ECHR to shift the boundaries between the public and private domains (12). Privacy has thus been argued in order to challenge electronic data capture (13) the systematic storage of public data (14), the disclosure of visual data obtained by video surveillance of public places (15) or even the storage in a font file of personal data, the accuracy of which is questionable (16). However, it would seem that requirement as to the qualification of privacy elements does not afford sufficient protection to individuals and the lack of relevance of a connection between the right to be forgotten and the right to respect for private life is even more marked in the current context of the digital environment. Social media service providers, for instance, collect information that is initially private but which, when shared, is treated like any other information that one may decide to make public. Thus, even if the information is specific to the user, the user no longer has the monopoly on its use and may lose control over that information. Indeed, once private data is considered “public“, the administrators of the social network or the search engine, subsidiaries, partners, advertising customers or other third parties may use it. It may be noted that Facebook has expressly developed this concept of “public information” that was originally private. The social network provider states that this is “Something that’s public can be seen by anyone. That includes people who aren’t your friends, people off of Facebook and people who use different media such as print, broadcast (ex: television) and other sites on the Internet” (17). When a person shares information about another member on the network, he may choose to make that information public, though he himself may have chosen to
make it visible to a restricted audience on his own profile. Lastly, some information is always considered public, such as name, profile photos and cover, networks used, gender, the user name and ID. Similarly, some group content on LinkedIn, a professional social network, may be public and available on the Internet if the group owner has opened it to public discussion (18).

In this context, one can think that "privacy has become an irrelevant concept" (19) especially because it only addresses part of the problem raised by the right to be forgotten. "On the Internet, there are public activities, while others involve a number of interests relating to privacy. In order to establish an approach consistent with the imperative of balance between all human rights, consideration must be given to the continuum aspect of public and private situations. In cyberspace, nothing is wholly public or wholly private, as if there were only black and white. The public and private intensity of situations is in varying shades depending on the context and circumstances" (20). This is what explains the interest there is in re–exploring measures for protecting personal data.

II – The alternative basis for the right to respect for private life: the protection of personal data

The European authorities took hold of the right to be forgotten by adopting, on 25 January 2012, a draft Regulation making direct reference to it (21) – a choice that the European Parliament nevertheless revised (22) without, however, amending all the provisions inducing it. The measures for protecting personal data can be applied when information constituting personal data is subject to processing by a controller (section A). However, any information falling within the scope these measures is not eligible for the right to be forgotten. Its implementation must be subject to certain criteria (section B).

A – The processing of personal data

The measures protecting personal data are broad in scope. Flexible and adaptable, they are likely to cover a wide variety of data processing despite the developments of digital technology and the internet. Where case law relies on the measures protecting personal data, it does not question the public or private nature of the information disseminated. The result is that information made public by the data subject or against his will (particularly when the publication is of legal origin or by journalists) is eligible for the protection scheme provided by Directive 95/46/EC if it constitutes personal data processed by a data controller.

Personal data is not necessarily an element of privacy. The family name, for example, does not fall within the scope of privacy. Defined by Article 2 of the Informatique & Libertés Act of 6 January 1978 (23), personal data can be extremely diverse and one may consider that very little personal information falls outside the scope of the classification, which makes it of particular interest when faced with the issue of the right to be forgotten. Additionally, the legislature reserves even more protective measures for so–called sensitive data than those applicable to other data. This is the case for "personal data that reveals, directly or indirectly, the racial or ethnic origins, political, philosophical or religious opinions or trade union affiliations of persons, or which relate to the health or the sexual life of said persons" (24).

The processing of personal data is, in turn, to "any operation or set of transactions (of personal data), whatever the process used [...]" (25). The data processing concerned is extremely diverse and again covers a wide range of activities that may be carried out with the data.
Finally, the data controller is "the person, public authority, agency or body that determines its purposes and means" (26). The definition of the data controller is very broad and thus covers the vast majority of operators. It even includes, a priori, journalists, archivists and scientists. There are, however, derogations relating to the purpose of the processing that they perform. However, in the current context of the digital environment and networks, there is no doubt that the definition covers internet players. Under cover of a right to be forgotten, it is possible for victims to sue websites publishers, social network service providers (27) or search engine service providers to obtain either the deletion or dereferencing of online content. In Google Spain v AEPD, the Advocate General denounced the risks of an extensive vision of the concept of data controller which did not, according to him, include search engine providers (28). Rather, the ECJ considered that it is their specific processing activity, which differs from but is added that of website publishers who feature data on web pages, which serves in equating them to data controllers.

B – Implementing the criteria of the right to be forgotten

For the right to be forgotten to come into play, the processing performed must be classed as unlawful. A person’s objection to such data processing renders the latter unlawful on certain conditions. As regards requests made to search engines, there is no vested right to be dereferenced or forgotten. The request will be rejected if, for specific reasons, such as the role played by the person in public life, the interference with his fundamental rights is justified by the overriding public interest in having access to the information in question. However, the ECJ stipulated that the right to be forgotten prevailed, in principle, not only over the economic interests of the search-engine operator, but also over the public's interest in accessing information when making an online search using a person’s name.

The implementation of the right to be forgotten involves building a grid of indicators that could be taken into account to justify the deletion of dereferencing of data. The criteria are gradually emerging under the influence of case law (29), the European authorities (30) and operators themselves (31).

The time criterion is not absent from the data protection measures which, in our view, makes it even more relevant for the victims. The legislature pays particular attention to the time limits for storing data. It is true, however, that the provisions governing such periods are scattered and sometimes lack clarity. In the present state of positive law, it is impossible to identify a time sequence. The solutions are often very factual and the outcome will depend very much on the context. The implementation of the right to be forgotten via indexing or deletion can therefore come up against the issue of identifying the timeframe within which a request may be submitted. In Google Spain v AEPD, the ECJ made the passage of time a parameter for assessing the right to be forgotten. It allows the loss of relevance of information to be qualified. It is not, however, the only criterion. The capacity of the person concerned is also a criterion for recognising the right to be forgotten. More specifically, what about information which, at the time of the withdrawal request, concerns an illustrious unknown who later becomes a public figure, a politician perhaps? The benefit of accessing the information on the basis of the person’s name is likely to evolve and bypasses an objective approach to timeframes. There is no doubt that if data protection measures overcome the shortcomings of the right to respect for private life, they do not solve all of the problems arising from the implementation of the right to be forgotten.
Notes:
(2) F. Nietzsche, On the Genealogy of Morals (1887); published in translation in France as Généalogie de la morale by Flammarion, 1996
(4) M. Boizard (dir.), Le droit à l’oubli, Rapport pour la Mission de recherche Droit et justice, fév. 2015, p. 12.
(7) ECHR, Costello–Roberts v United Kingdom, Application no. 13134, judgment of 25 March 1993, para. 36.
(8) ECHR, Niemietz v Germany, Application no. 13710/88, 16 December 2012.
(13) ECHR, Wieser and Bicos Beteiligungen Gmbh v Austria, Application no. 74336/01, 16 October 2007.
(14) ECHR Rotaru v Romania, Application no. 28341/95, 5 May 2000.
(16) ECHR, Khelili v Switzerland, Application no. 16188/07, 18 October 2011.
(17) "Public information" section – Facebook Privacy Policy.
(18) Clause 2.10, "Groups" – LinkedIn Privacy Policy.
(20) P. Trudel, « Quelles limites à la googleisation des personnes ? » in La sécurité de l’individu
numérisé, Réflexions prospectives et internationales, S. Lacour (dir.), L’Harmattan 2010, p.52.

(21) Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM/2012/011 final – 2012/0011 (COD).

(22) European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation Of the European Parliament and of the Council on the protection of individuals with regard to The processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7–0025/2012 – 2012/0011(COD))

(23) The amended proposal for a Regulation on the protection of personal data aims to be more complete, see Art. 4 (2).


(25) Article 2 of the 1978 Act. Article 4 (3) of the proposed Regulation does not proceed with such a flagrant amendment.


(28) Case C–131/12, conclusions of Advocate General Niilo Jääskinen, para. 29.

(29) In particular, CJEU Case C–131/12, Google Spain v AEPD and TGI Paris, 19 December 2014, above.


(31) The Advisory Council to Google on the right to be forgotten, 6 February 2015.
“Ignorance of the law on respect for private life can be of such a nature as to restrict individual freedom” – thus ruled the Constitutional Council in its decision of 18 January 1995 (1). In this assertion, the Council recognized and explicitly linked privacy to the constitutional principle of individual freedom, thus hauling it up to the zenith of the pyramid of norms. This was an essential step as, up until then, France stood out by its conception of privacy, which was neither part of the Constitution (unlike Spain (2)) nor of the “bloc de constitutionnalité”, the body of constitutional rules and principles (unlike Germany (3)).

The above statement leads us to infer that there then existed no real long tradition in French constitutional law (4) in relation to the protection of privacy; on the contrary, it is a concept that has recently and gradually become a part of national law through international and European legislation on the one hand, and the development of information technology on the other.

However, and paradoxically, a quick glance at history confirms that the concept of privacy is one of the cornerstones of our society. Indeed, soon after the French Revolution, Benjamin Constant (5) suggested a distinction between la liberté des Anciens, exercised through active participation in collective power; and la liberté des Modernes, which consists in protecting individual rights and the private sphere against government interference. For Alexis de Tocqueville, privacy must be examined in light of the “growing equality of conditions” and the spread of democracy, which encourages the rise of individualism, that “considered and peaceful sentiment that disposes each citizen to isolate himself from the mass of his fellows and to withdraw to the side with his family and his friends” (6). It emerges, from such intellectual considerations, that the notion of privacy is intrinsically linked to the individual and the exercise of his freedoms, as society acknowledges his right to dispose of his own private sphere, independently of collective public life.

Previously, invasions of privacy were essentially government acts; nowadays, however, it would appear that private persons may also be perpetrators of such acts. The protection of privacy, initially a political issue, has over time become a financial concern. Technological progress has facilitated that transition by making database creation and data collection – the new challenges faced by said protection – accessible to businesses, sometimes even with the consent of the citizen–consumer. It would appear that privacy may no longer be separated from personal data.

So it is a concept marked by the intellectual and technological considerations of a given age. It fluctuates and changes, and this is why case law is called upon to play a central role, particularly in how best to reconcile that concept with other fundamental principles. The recent classification of private life as an area of constitutional concern thus leads us to question the content of said protection in light of the development of Constitutional Council case law. These considerations invite us first to consider the recent emergence of constitutional protection under the twofold
restriction of national and international pressures, before observing its current development in light of technological progress.

I – Recent constitutional protection

Article 9 of the Civil Code, created by the Law of 17 July 1970, formally enshrines the principle that “everyone has the right to respect for his private life”. For a long time, it fell to the ordinary courts to take the necessary steps in order to bring an end to any invasion “of personal privacy” (intimité de la vie privée) (7). Thus, like “personal privacy” under Article 18 of the Spanish Constitution or the German constitutional courts’ theory of the spheres (8), French law places the notion of intimité or personal privacy at the very heart of private life. On that basis, constitutional protection can be erected and, thereafter, strengthened and empowered.

A – A favourable context for the emergence of constitutional protection

This recognition was first of all the result of international law, which naturally influenced national law.

The favourable international context for the protection of privacy opened in 1948 with the adoption of the Universal Declaration of Human Rights (9). Shortly thereafter, the 1950 European Convention on Human Rights stated at Article 8 that “[e]veryone has the right to respect for his private and family life, his home and his correspondence”. This fundamental piece of legislation, at the root of an abundance of case law, has contributed to the emergence of a number of new rights in French national law. Indeed, we cannot help but note that the Constitutional Council “takes inspiration directly and in numerous cases in its case law” (10) from the ECHR in Strasbourg, the bedrock for the protection of rights and freedoms. However, the Council is under no obligation to align itself with ECHR case law even if, in order to maintain “the unity of the French legal order and legal certainty”, it is implicitly subject to it. From this unofficial perspective, arises “a conversation without words” (11) and ultimately “the Constitutional Council and the ECHR protect […] the same rights” (12). Privacy gradually emerged as a constitutional concept. The international context that was favourable to recognition at the highest level accelerated the development of a similar process on a national level which, in 1977 (13), allowed the Constitutional Council to bestow greater legal value on privacy by integrating it into the fundamental principles recognised by the laws of the French Republic (14).

Lastly, the constitutional enshrinement of the said protection was definitively established when, in 1993, the Vedel Report (15) suggested the addition to Article 66 of the Constitution of a paragraph stipulating that “everyone has the right to respect for his private life and the dignity of his person”. The proposal was not acted upon; nevertheless, it opened the way for more protective Constitutional Council case law. The legal and legislative foundations had been laid to allow full and complete acceptance into the body of constitutional rules and principles.

B – The concept becomes independent and explicit

In Spain, the protection of privacy expressly included in Article 18 of the Constitution serves in establishing guaranteed legal stability as to its basis and content. In France, as in Germany, there are multiple legal bases which force the courts to make choices.

This in particular is the reason why “the constitutional value of respect for private life was long cast into doubt” (16). Indeed, it took the “video-surveillance” decision of 1995 for the
Constitutional Council to refer expressly to privacy. In the absence of any constitutional provisions on that protection, the Council had to find the best legal response. This is why it based the protection on the foundation (17) of Article 66 of the Constitution, i.e. on a broad conception of individual freedom including security, freedom of movement, freedom to marry, and the right to respect for private life.

Nevertheless, difficulties arising from that approach have been brought to light. Indeed, the process bolstered the powers of the judicial courts, which dealt with cases of privacy almost exclusively to the detriment of the administrative courts. As part of a political strategy and in order to share jurisdiction more equitably, the Constitutional Council decided in 1999 (18) to amend the legal basis by expressly linking privacy to Article 2 of the Declaration of Human Rights (19), stating that "the freedom proclaimed by this Article implies respect for private life". It is therefore a new right nonetheless founded on an old provision dating back to 1789, the affirmation of which had been renewed a number of times by the case law of the ECHR in Strasbourg relying on the Convention. This new basis allowed the Council to “freely manage its case law on the division of trial jurisdiction between the ordinary and administrative courts” (20). Henceforth and quite apart from the protection of the home which rests on the foundation of Article 66C, the protection of privacy is based on the jurisdiction sometimes of the ordinary courts, sometimes of the administrative courts. The modulation that the Council allowed itself is echoed in German law, which considers that some rights enjoy specific protection (protection of the home or of correspondence), while others (such as personality rights) are subject to general subsidiary protection.

For the French as for the German courts, the objective is to avoid fencing off the content of that right and leave a margin of appreciation.

II – Constitutional protection tested by current demands

While private life was initially synonymous with the \textit{sphere de l’intimité} or the “sphere of privacy”, to use Jean Carbonnier’s phrase, it would appear that with new technology, the emphasis is now on information. Indeed, the consistency between information and personal data would make substantial changes to the content of privacy. The latter could be defined as “a collection of personal, i.e. identifying information” (21). The right to respect for private life would become “a right of control over personal information” (22).

A – Strengthening the constitutional affirmation of respect for private life

In accordance with Article 34 of the French Constitution, it falls to the legislature to set the rules and restrictions concerning fundamental freedoms granted to citizens. However, the Constitutional Council then has the task of establishing a framework reconciling the safeguarding of public order and respect for private life, both principles having constitutional value.

In 1978, France was among the first few countries to pass data protection legislation in the form of the \textit{Informatique et Libertés Act} (23). The \textit{Loi} allowed the Constitutional Council to deliver the law on the protection of personal data as, under Article 4, it defined personal details as those that “\textit{in whatever form, serve in the identification of the physical persons to whom they apply, be it directly or otherwise}”. On that basis, the Council regularly reminds the legislature that it must respect those “\textit{provisions safeguarding individual freedom provided by legislation on information, databases and freedoms}” (24).
Next, in 1995, the European Union adopted a Data Protection Directive, transposed in France by the Law of 6 August 2004. This proposed a series of flexible principles intended to provide a sustainable framework for that protection: purpose; proportionality; data security; right of access and rectification; right to information; right to object; and the right to prior consent. It was ultimately on that basis that the decisions of the ECHR and the Constitutional Council would interact consistently.

Fairly typically; the right to respect for private life is defined as the "right not to be disturbed by others either in one’s own home (inviolability of the home) or one’s own interests (inviolability of the private sphere)" (25). Constitutional Council case law connects private life with classic concepts such as the inviolability of the home, the interception of correspondence and doctor–patient confidentiality, but also more modern concepts linked to video surveillance and data processing.

An examination of the various decisions shows that, for the ECHR as for the French court, the frontier between the lawfulness or otherwise of invasions of privacy depends on whether national law complies with procedural requirements and the various forms of protection provided against any potential infringement.

Thus in its decision of 2 March 2004 (26), the Council ruled that certain provisions that seemingly invaded privacy nevertheless complied with the Constitution, in light of “public order requirements and the prosecution of the perpetrators of criminal offences". This compliance was also based on the fact that the relevant judicial authority must give consent in order to approve such practices (searches, seizure of evidence outside the hours provided by the Criminal Procedure Code, etc.) which, in the eyes of the court, constitutes a sufficient constitutional guarantee.

This is why some writers stress the fact that that "strengthening the constitutional affirmation of respect for private life did not bring with it a genuine reinforcement of its effectiveness or its protection" (27).

B – The lack of genuine reinforcement for the protection of privacy

For a number of years, the growing demand with regard to increased security through powerful surveillance and monitoring systems has been expressed in a number of rulings against the right to private life. New technology is indeed viewed as the possibility of combatting insecurity and we can see fairly broad social acceptance of these, nevertheless intrusive, tools.

Consequently, requirements as to the respect of that right are increasingly flexible and, like her European neighbours, “the boundaries of private life are shrinking while the authorities’ surveillance powers continue to expand” (28). The European Commission has described this trend in terms of a “period of decline” as the majority of national legislation is passes in order to combat terrorist threats and serious crime.

France is no exception to this trend. Involved as she is in the international war on terror and in response to the Charlie Hebdo attacks of January 2015, she has sought to increase the powers of the intelligence services in the Bill (29), approved at first reading by the National Assembly on 5 May 2015 and which is currently the subject of a broad consensus in public opinion and amongst Members of Parliament; it would appear that it will be referred to the Constitutional Council, whose decision will be hotly anticipated, particularly with regard to private life, the respect of
which, according to the Council, supposes both (30) public interest grounds and the proportional nature of the means implemented in order to achieve the established aim (31).

Equally, the use of geolocalisation is permitted within a very strict procedural framework. It is a judicial police procedure consisting in the surveillance of a given person using considerable technical means that allow the geographical location of a vehicle or telephone to be followed in real time. The invasion of privacy is characterised by this continuous, instant localisation. That is why, in its Geolocalisation decision of 25 March 2014 (32), the Council examined the compliance of this practice in light of the right to respect for private life and the inviolability of the home. While the technique is permitted by the legislature for serious offences, it is nevertheless placed under the guidance and control of the judicial police. These procedural and restrictive legislative measures are intended to guarantee that "the restrictions imposed on constitutionally guaranteed rights are necessary for ascertaining the truth and are therefore not disproportionate to the seriousness and complexity of the offences committed". It therefore concluded that the measures were constitutional.

Conclusion

The legal restrictions linked to the respect for private life are gradually being relaxed by successive Council decisions but also by the technological context. The emergence of "new digital memory devices" (33) or, more generally, the digitisation of society "threatens our traditional conception of privacy" (34). The recent but rapid development of the smart cities phenomenon in France, equipped with digital sensors which serve to locate any individual and monitor their consumption habits at any given moment, it a relevant example, the existence and evolution of which have evaded the Constitutional Council’s scrutiny.

This raises the question of the future of the concept of privacy.

We could well imagine the emergence of a distinction between the scope of privacy – linked to the intimate sphere, according to the classic conception, which would enjoy greater protection – and that of the more technological personal life, which would be linked to digital personal data and on that basis subject to more relative protection.

Whether it be under the influence of political will, legal restrictions or even economic needs, it is clear that the current situation is destined to undergo significant change in the near future.

Notes:


(3) In the same vein, see the study conducted by Laurence Burgouge–Larsen, "L’appréhension constitutionnelle de la vie privée en Europe. Analyse croisée des systèmes constitutionnels allemand, espagnol et français", in Frédéric Sudre, Le droit au respect de la vie privée au sens de la CEDH, Bruylant, coll. Droit et Justice, 2005, p 98 onwards, for whom, regarding Germany, "the right to private life does not feature per se in the Basic of 23 May 1949 but is
apprehended through other rights that are closely linked to it”.

(4) It is important to emphasise that only Constitutional Council decision will be examined here; the constitutional case law of the ordinary courts will not be taken into consideration

(5) Benjamin Constant, Discours prononcé à l’Athénée Royale de Paris, 1819.

(6) Alexis de Tocqueville, Democracy in America, Volume 3, Part II, Chapter II

(7) Article 9 para.1, Civil Code

(8) See Christoph Gusy, « La théorie des sphères », AIJC, 2002, pp. 467–484. The German courts make the distinction between the intimate, the private and the public spheres, and ultimately reconcile the intimate and private spheres.

(9) Article 12 UDHR "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation”.


(11) Idem.


(13) See Decision 76–75DC of 12 January 1977, known as the "fouille de véhicules » ("vehicle search") decision, on the law "permitting the search of vehicles for the purpose of investigating and preventing criminal offences".

(14) In the first recital, the Council states that "individual freedom is one of the fundamental principles guaranteed by the laws of the Republic”.

(15) Comité consultatif pour une révision de la Constitution (Consultative Committee for a revision of the Constitution", chaired by Dean Jean Vedel, « Propositions pour une révision de la Constitution », 15 February 1993, p.23


(19) Article 2, Declaration of the Rights of Man and of the Citizen: "The aim of every political association is the preservation of the natural and imprescriptible rights of Man. These rights are Liberty, Property, Safety and Resistance to Oppression".

(20) Dominique Rousseau, « Chronique de jurisprudence constitutionnelle », RDpub, 2001–1, p.76


(22) Daniel Gutmann, Le sentiment d’identité, n° 247, p.221, LGDJ, coll. Bib privée de droit privé, 2000, n°247

(23) Law 78–17 of 6 January 1978


(25) Vocabulaire juridique, Association Henri Capitant


(27) Bertrand Mathieu, Michel Verpeaux, Contentieux constitutionnel des droits fondamentaux, p.452


(29) The Bill adds an Article L. 811–1 to the Internal Security Code, which guarantees "respect for
private life, and particularly for its components which are the confidentiality of correspondence and the inviolability of the home, by provising that these may only be infringed in the event of overriding public interests provided by law, while complying with the proportionality principle”.

(30) Decision 2003–467 DC 13 March 2003, on internal security
(31) Decision 2004–504 DC of 12 August 2004 on the law on sickness insurance
(32) Decision du 2014–693 DC 25 March 2014 on geolocalisation
Privacy and political assassinations in France during the Trois Glorieuses: the meanderings of Orleanism
Sophie Delbrel, Associate Professor, University of Bordeaux


The Trois Glorieuses, being the three days of the July Revolution (27, 28 and 29 July 1830) that resulted in the fall of Charles X, are inextricably linked in the collective memory with Eugène Delacroix’s painting of the same year, Liberty Leading the People. The allegorical figure of liberty as a woman of the people illustrates the ambivalence of the reign that was just beginning: the uprising ended with the acclamation of the Duke of Orléans at the Hôtel de Ville in Paris (1): “Lafayette’s republican kiss made a king. Strange consequence of the whole life of the Hero of Two Worlds!” (2). The very name of Louis-Philippe I is a transaction (3), in the absence of transition: symbolically, it had already become essential to set aside memories stirred by the Bourbons and signal the dawn of a new era. This departure was also intended to be constitutional in nature, with the acceptance – and no longer the authorisation – of the Charter, as voted upon by the Chamber of Deputies on 7 August (4).

Louis-Philippe had long cultivated his difference from the more senior branch of the French monarchy, and this with a degree of skill. The Duke of Orléans had been demanded of Charles X all prerogatives befitting his position as a prince of the blood (5); he was therefore able to receive the wishes of the Court of Cassation in a ceremony similar to that usually intended for the King (6). This attachment to his rank did not, however, prevent the Duke of Orléans from making his residence, the Palais-Royal, a place known for the warmth of its welcome and festive, even “populist”, atmosphere (7), likely to disconcert the Court (8). In fact, the Duke of Orléans was out of place in the aristocratic world of the 1820s, as he sought the support of the bourgeois classes. Hence an idea was entertained as to a bourgeois monarchy, as opposed to the aristocratic monarchy of Charles X. The political skill of Louis-Philippe’s supporters would be seen in their hijacking, when the time came, of what was essentially a republican popular uprising (9).

Orleanism made itself increasingly felt from January 1830, particularly with the founding of a newspaper, Le National, which bolstered the opposition press (10). Admittedly, from the very beginning of the Restoration, censorship had revived the dissemination of political and literary writings criticising the monarchy. Symptomatically, editions of the complete works of Voltaire were constantly part of the longest print runs. The phenomenon was undoubtedly an expression of political aspirations (11). A publisher boasted, for instance, of having published two million copies of the Charte constitutionnelle à cinq centimes (The Five-Cent Constitutional Charter) (12). Even before it unfolded on the streets, the fight for a regime change was a battle of the written word, made possible by the modernisation of printing equipment and a fall in the price of paper (13).

The role of popular literature in preparing for and strengthening Louis-Philippe’s accession cannot, therefore, be underestimated, if only in considering its proliferation. Highly heterogeneous
in form and content (14), this literature reflects a change in the national state of mind. Violence prevails and reveals itself in proportion to the censorship that has oppressed it. Under the cover of information to be delivered to the reader, a full-scale attack was made on the very persons of Charles X and his intimates. As was noted by the Prince of Polignac, “private acts, just like public acts, were revealed, scrutinised, wracked with impropriety” (15). Although such a view is the result of a judgment formed a posteriori, it provides a sufficient indication of the singularity of political assassinations following the Trois Glorieuses, with the displaying of the private lives (real or assumed) of public figures.

Ambivalence on the part of Louis-Philippe, the ‘Citizen King’ and, consequently, his accession to the throne, are a reflection of the trials and tribulations of an age at the mercy of contradictory influences, in which private life occupied an increasingly important place. Incidentally, this development drew on the English example, which served as a source of inspiration (16) from the very beginning of the Restoration. Supporters of Louis-Philippe did not fail to present him as a French-style William III. In the image of the Glorious Revolution of 1688, the 1830 Revolution was intended to established parliamentary freedoms: to this end, the page had to be turned on the Ancien Régime at all costs, hence the discrediting of Charles X and his ministers. As a corollary, a dynastic change had to be made, which necessarily entailed the irrevocable disqualification of the Duke of Bordeaux, grandson of Charles X, from the line of succession.

I. Charles X and his ministers discredited

The 1830 Revolution had its origins in Charles X’s stubbornness in pursuing an ultra-royalist policy against a newly-elected, predominantly liberal Chamber of Deputies. By doing so, in the words of Charles de Rémusat (17), legitimacy lost the legitimate monarchy. The coup materialised with the enactment of four orders said to be fatal to freedom, published on 26 July. Come the end of the Trois Glorieuses, several hundred insurgents (18) had lost their lives and Charles X was about to lose his crown. During the night of 29 June, Thiers, Mignet and Laffitte orchestrated a large-scale poster campaign, with a view to making the Duke of Orléans the man for the job, emphasising that Charles X ne peut plus rentrer sans Paris; il a fait couler le sang du peuple: “Charles X can no longer set foot in Paris; he has spilt the blood of the people” (19). An indelible stain on Charles X’s reign, the repression of the Revolution became the common denominator for the publications examined, although it is not possible to establish the exact moment when the people became aware of this. Some blossomed in August 1830, when Louis-Philippe had only just come to power. More generally, they appeared before the trial of Charles X’s ministers, which was held in December before the Chamber of Peers.

A minima, in the spirit of the posters put up in the streets of Paris, it was a question of obstructing the path and persons of Charles X and Louis-Philippe; thus, while the people were being “machine-gunned”, the former “was off hunting” (20). Charles’ weakness of character had disastrously pushed him to enact the contemptible orders. Other factors in the challenge to the King were his great age, and the pernicious influence of his son, the Duke of Angoulême, who was nevertheless presented as “idiocy personified. That dull, fixed stare, that vague look, that gangling gait; everything about the Prince suggested bigotry and stupidity” (21). Guiding the son’s hand were a number of Jesuits accused of having planted “fanaticism” (22) in his mind and, in fact, contaminating the King. In reality, Charles X was essentially accused of incompetence in conducting public affairs, as was shown in the harmful nature of his entourage.
As a consequence, the blows struck against those ministers who signed the orders proved to be even harsher. Moral and social reprobation was a precursor to their political and criminal condemnation, which task fell to the Chamber of Peers, re-named the Court of Peers in the circumstances. The ministers in question were the Prince de Polignac, president of the Council of Ministers, loyal friend of Charles X and embodiment of the priests’ faction that had dominated the Court (23); the Comte de Peyronnet, Minister of the Interior, author of the renowned *loi de justice et d’amour* (law of justice and love) (24); Jean de Chantelauze, Minister of Justice; and, lastly, Count Martial de Guernon–Ranville, Minister for Religious Affairs and Public Education. In truth, the latter two, both senior judges before their appointment as ministers (25), were not very well known to the general public and were secondary targets (26). Conversely, Polignac, as the son of Marie-Antoinette’s favourite, symbolised the *Ancien Régime* and emigration, which points were endlessly hammered home by the pamphleteers (27). For his part, Peyronnet, vilified for his arrogance, crystallised the hatred of the ultras: “admitted as a lawyer at a time when everyone was admitted”, this former Minister of Justice who passed as being “one of the most distinguished ‘fashionables’” (28) of Bordeaux”, the city of his birth, had allegedly led a life of debauchery and corruption (29).

The publications of the time, despite the risky, even vulgar nature of their assertions, in many respects announced the judgment of the Court of Peers that sat on 21 December 1830, “[…] considering that while the personal will of King Charles X may have brought about the determination of the defendants, that circumstance cannot absolve them of legal responsibility” (30). Coldness, indifference and obstinacy had resulted in a great deal of bloodshed, even though not all the defendants had played a similar role to that of the monarch. In any event, the sentence had to be severe: life imprisonment on in mainland France, the sentence being doubled for civilian deaths in Polignac’s case (31).

The political and judicial judgment was based on a spirit of revenge in correlation with the Romantic age (32). The cult of the victims of the *Trois Glorieuses* explains the outburst aimed at the former King and his family. The popular press is an indicator of the Revolution of July 1830, the person of the Duke of Bordeaux crystallising quite spectacularly the divisions between legitimists and orléanistes.

II. The Duke of Bordeaux disqualified from the line of succession
The young Duke of Bordeaux found himself at the centre of the controversy owing to the abdication in his favour of Charles X and the Dauphin, the Duke of Angoulême, on 2 August 1830. Notwithstanding the circumstances, the gesture was surprising as it breached the rule on the *indisponibilité de la couronne* [find translation] posited under the *Ancien Régime*. The abdication indicated in any case to Louis–Philippe and his supporters every danger that could be represented, in the future, by he who the legitimists were calling Henri V (33). The weakness of the royal child was also his strength at a time when political and moral responsibilities had to be taken into consideration. Following the failure to reasonably push the Duke of Bordeaux into tripping up in the blood already spilt, another stain emerged: that of his birth.

Far from being an heir to the throne who could be taken seriously, the Duke of Bordeaux was allegedly little more than a bastard born to the Duchesse de Berry, according to a hoax (34) that has since been carefully stripped apart. We must emphasise here the willingness shown to inform readers, which went hand in hand with historical preoccupations in some respects (35). Indeed, the
political momentum was rooted in a reflection which appears to be back on facts past and present (36). Through this tale, or the tales related in the popular press, the connection was made with the 1789 Revolution. Such a need was felt all the more keenly as, for the regime emerging from the Restoration, “history beggars belief” (37).

According to one pamphleteer, the silence on the part of the Bourbons as to the 1789 Revolution and its repercussions was matched by their oblivion before they seized power again by surprise (38). From such a perspective, the bad luck that had allowed Louis XVIII then Charles X to take the throne would be extended with the birth of the Duchesse de Berry’s child. Every act and gesture of Charles X’s daughter-in-law was dissected, from the disappearance of the Duc de Berry to the birth. Not a single aspect went unnoticed: even the umbilical cord was discussed, to take but one example. This concern for detail is justified by the application of private standards to the royal family, as though that went without saying: “Such fraud is regarded as a crime amongst the ordinary classes, where the consequences thereof nonetheless affect only one family and only concern individual interests” (39).

Above all, several publications reproduced a text presented as a ‘protestation’ by the Duke of Orléans with a view to denouncing the birth of the Duke of Bordeaux in all its aspects. The document did little more than relate the content of an authentic instrument at the wish of Louis-Philippe; it had been disseminated immediately after the birth, in 1820, in England (40). In fact, distribution in England at that time guaranteed an unofficial dissemination in Paris, bearing in mind the significant cultural exchange between the two countries (41). For reasons relating to censorship and the Duke of Orléans’ tenuous position, it was only in 1830 that the majority of French citizens learned of the document. The text was originally published in Le Courrier français (42), which assertion was reiterated by Louis Blanc several years later (43). In any event, Louis-Philippe did not deny the ‘protestation’.

Lastly, the reference to the Glorious Revolution proved straightforward to the point of caricature (44), demonstrating (were it necessary) the strength of the ideas conveyed by the liberals. Furthermore, the English influence went beyond revolutionary references considering that, from 1820 onwards, public opinion across the Channel had taken a keen interest in the marital setbacks of Queen Caroline and George IV (45). The private lives of dignitaries seized upon by public opinion also marked a move towards a form of modernity, bearing in mind the scale of the means of distribution.

Ultimately, popular literature after the Trois Glorieuses materialises the influence of the liberal, through the development of connections with the English Revolution of 1688, as well as the promotion of links with the French Revolution of 1789–1791. Relying on the sinister appeal of the private lives of government members to the general public, these publications are nevertheless a reminder of the most virulent writings of those revolutionary years, including 1792–1794. Admittedly this does not contribute to liberal thinking, but rather reinforces the paradoxical nature of Louis-Philippe’s accession: the monarchy, as Chateaubriand announced “is a strange graft that will not take on a republican stem” (46).

Notes:
tradition of insurrection, the mob once again using the technique of barricades, as had been seen in the previous popular uprisings of Spring 1795.


(3) François Furet, op. cit., p. 124.


(5) Ibid., p. 137.


(7) Which made it quite unlike the Tuileries, the royal residence: cf. ibid., p. 60.

(8) Ibid., p. 62.


(10) Benoît Yvert, La Restauration..., op. cit., p. 107; the newspaper was founded by Talleyrand and the banker Laffitte; Thiers, Carrel and Mignet were its editors.


(12) Ibid.; this was Jean–Baptiste Touquet, who fully committed himself to defending liberal thinking.

(13) The authors of these books, brochures and pamphlets often remained anonymous. As regards the publications cited in this article, they have been digitised and may be viewed on the Bibliothèque Nationale de France website: http://gallica.bnf.fr/


(16) Georges Matoré, Le vocabulaire et la société sous Louis–Philippe, Slatkine Reprints, 1967, p. 79–84; seen both in everyday and literary language.

(17) Quoted/cited by Benoît Yvert, op. cit., p. 144.

(18) Jean–Claude Caron, La France de 1815 à 1848, Armand Colin, 2011, p. 94, estimates that the battles led to 800 insurgents dead and 4,000 injured.

(19) Emmanuel de Waresquiel, Benoît Yvert, op. cit., p. 461. Conversely, Louis–Philippe’s position was, according to Madame de Rémusat, "beyond compare": "He is of Bourbon blood and he is covered in it"; cf. Benoît Yvert, op. cit., p. 137.


(21) Vie scandaleuse, anecdotique et dévote de Charles X, depuis sa naissance jusqu’à son embarquement à Cherbourg, Paris, 1830, p. 104.

(22) Ibid., p. 108; these terms show the anticlericalism that continued to grow during the reign of
(23) Emmanuel de Waresquiel and Benoît Yvert, op. cit., p. 435.

(24) Ironic name for a restrictive law on press freedoms, which in reality remained in draft form in 1827.

(25) Ibid., p. 442 et 449, Guernon–Ranville had been Chief Prosecutor in Lyon, while Chantelauze had been First Presiding Judge of the Court of Appeal at Grenoble.

(26) Their stigmatisation was an extension of that of Charles X’s ministers as a whole. For example, the Grande et sublime complainte de la famille royale, rédigée à Rambouillet d’après quelques notes authentiques, par un élève de l’ex-ministre Guernon de Ranville, 1830, 15 p., barely mentions Guernon–Ranville, even indirectly.


(33) Chateaubriand, op. cit., p. 495, emphasises that the very name of Henri V has been removed from the Duke of Orléans’ statement on the abdication, “by a wretched ruse and cowardly reticence”.

(34) This would also affect the Duchesse de Berry’s pregnancy and the substitution of a male newborn for a female newborn.


(39) Ibid., p. 8.


(42) T.P. Gavaud, Le duc de Bordeaux, le duc de Reichsstadt et la France nouvelle, Lyon, Roubier, September 1830, p. 23.


(44) Le Duc de Bordeaux bâtard…, op. cit., presents as an appendix a table on the almost perfect “rapprochemens historiqués” (sic – literally, "historic similarities") between the two revolutions.

Privacy and the disclosure of administrative documents: a well-guarded secret?
Dr Marie-Odile Diemer, University of Bordeaux


The dematerialization of procedures serves to improve the efficiency of the administration and access to administrative data. The flipside of this dematerialization is the vast database that is the preserve of the administration. Potentially open to all, this database can encroach on the private lives of citizens.

An administrative document is a document produced or received by the administration (the State, local authorities, public establishments or even private bodies with a public service mission). Administrative documents can be in writing either as hard copy or in electronic format. This therefore applies to all documents produced under the auspices of the executive branch, and excludes any document related to the exercise of legislative or judicial power.

Firstly, administrative documents include reports issued by ministers or committees, or even ministerial circulars. Impersonal and produced for informational or policy purposes, these seem far removed from issues of privacy. Nevertheless, administrative documents are varied. They often contain elements relating to a citizen’s private life, and that content can raise doubts as to their complete disconnection with private life. However, a citizen’s life is not a citizen’s private life: land use planning or notice of a civil service appointment provides information on a person’s life without touching on personal details.

Other documents encroach significantly on the privacy of citizens. Where a person can be identified (when their name appears) or where personal details appear in an administrative document, such as an address or telephone number, the family situation or marital status, the person’s assets and financial situation or even membership of a political party, the document is deemed to relate to the citizen’s private life.

Private life is protected by leading national and international legislation, but it has not received any real definition in law or in case law. Article 9 of the French Civil Code provides that “everyone has the right to respect for his private life”. Private life corresponds overall to everything linked to a person’s privacy, personal data, family life, doctor–patient confidentiality or even image rights. In short, it is everything relating to his own person, not his public life.

The relationship between the administrative authorities (and, more generally, government itself) and the protection of private life is therefore a delicate subject.

The exceptional database available to the administration must be strictly protected while the modalities for its disclosure must be carefully framed. Thus, while private life and administrative
law would appear to be antithetical at first glance, private life regularly crosses paths with administrative law though the documents available to the administration.

In France, the Law of 17 July 1978 sets down the principle that each person has a right of access to administrative documents. The Commission d’accès aux documents administratifs (CADA – Commission for Access to Administrative Documents), an independent administrative body, was established that same year to ensure compliance with the principle (1).

Article 6, II of the 1978 Law reiterates this requirement as to the protection of privacy in the context of the disclosure of administrative documents, providing that only the interested parties have a right of access to documents “the disclosure of which would infringe the protection of private life” (2).

The administration’s interference in private life can also sit alongside the thorny question of whether private life can be monitored.

In France, the forthcoming adoption of the new law on intelligence, which has caused such controversy in a context of terrorist threats, raises crucial questions as to the protection of personal data and the confidentiality of correspondence (3). This new State prerogative will allow information concerning the private life of individuals to be monitored and collected as part of the war on terror. The pre-eminence of the protection of State interests justifies such an incursion by the government.

The same problem affects the issue of the communicability of administrative documents. However, confidentiality is established as a genuine rule in administrative procedure. It serves to protect citizens, who remain assured that their own administrative documents will not be easily accessed by third parties. Confidentiality is, however, sometimes linked to aspects of the “private life” of the administration itself, like military secrecy in particular. Such administrative secrets stand a real obstacle to the law of evidence and can sometimes prevent a citizen from obtaining elements that would help him prove that he has, for example, suffered harm as the result of an act of the administration.

This protection for the confidentiality of public and private persons should not, however, overshadow the substantial expansion in the transparency of all administrative documents. A balance must be struck between transparency and the protection of private life.

The extent of the disclosure of administrative documents thus concerns not only the “private life” of physical persons (section I) but also includes the “public life” of the administration (section II).

I - Confidentiality within the administration: protecting the private life of physical persons

One principle dominates the disclosure of administrative documents across Europe: the free movement of documents. This free movement is fundamental in any democratic society as it serves to ensure the transparency of administrative activities.

Sweden was alone in recognising this guarantee for citizens very early on, doing so at the end of the 18th century (4). The remaining European States – such as Germany, Italy or the United
Kingdom, but especially France – all belatedly introduced legislation which is currently considered as recent (5).

Since 1978 in France, the combination of the creation of an independent administrative authority and a law establishing the modalities for communicability, guarantees the disclosure of documents (section A). The guarantees are provided under the aegis of an especially benevolent administrative court, in charge of hearing litigation that can occasionally be plentiful (section B).

A - The conditional opening for the disclosure of administrative documents impacting on private life
While the theory is to open the disclosure of administrative documents are wide as possible, this must necessarily respect private life.

Certain documents would appear to be quite unrelated to a person’s private life, such as driving licence applications, tax files, or the deliberations of administrative authorities. However, there is a thin line between such documents and private life, and the former may indeed contain personal data.

Private life is recognised as such in the 1978 Law, but it is also scattered through many other provisions protecting the disclosure of documents.

The 1978 Law protects the modalities for communicating documents, “containing an appreciation or value judgement of a physical person, named or readily identified or presenting a person’s behaviour, where the disclosure of that behaviour could be prejudicial to that person” (6). Where this is the case, such documents may only be communicated to the interested parties. This category of documents includes those concerning private life, client confidentiality or doctor-patient confidentiality.

Doctor-patient confidentiality implies that the results of medical tests or examinations be communicated exclusively to the person concerned. Third parties may only access these with the consent of the person concerned.

The “appreciation or value judgement” will, for example, concern candidates’ grades in competitive examinations, or a complaint made to the administrative authority as to negligent behaviour on the part of a citizen or an official. Such documents may only be disclosed to the interested parties. The administration thus protects a wide range of documents by allowing these to be communicated only to the interested parties. The importance of confidentiality is emphasised here.

Nevertheless, some civil-status documents such as birth, marriage or death certificates are now readily accessible on the internet. The dematerialization of administrative procedures may render all of the rules set down null and void. It is now possible to obtain such certificates via municipal websites; indeed, with only a few details, it is easy to obtain such documents, which nevertheless contain personal data.

The protection of privacy is ensured by an administrative authority and the administrative courts.
B - Administrative and judicial protection of privacy

When a citizen wishes to obtain an administrative document, he submits a request in writing, with acknowledgement of receipt, to the relevant administrative department. He must clearly state which document he wishes to have disclosed to him. The administration then has a month from the date of receipt to produce that document.

Silence on the part of the administration is deemed to be an implicit refusal of the request. The reform of non–contentious administrative procedure which stated that "silence is deemed to signal consent" was not transposed to the rules governing the disclosure of administrative documents (7).

Where a citizen is faced with a refusal to disclose the document, he must apply to the Commission d’accès aux documents administratifs (CADA – Commission for access to administrative documents) before applying to the courts, and this within two months of the refusal. The CADA then gives a favourable or unfavourable opinion which is then notified to the administrative authority and the applicant. The administrative authority then has a month as of the date on which the CADA opinion is received in order to make known the action that it intends to take further to the request. The citizen will then have to apply to the administrative judge (first the administrative court, then the Conseil d’État) in order to assert his rights.

The link between the courts and the disclosure of administrative documents is significant.

Firstly, litigation concerning the disclosure of administrative documents falls within the remit of the administrative court. However, quite aside from the litigation itself, the court can ask that the administration provide it with a document that is essential to resolving the dispute. The administrative court has considerable investigative powers. In the context of an inquisitorial procedure, the court directs the investigation and can then turn to a recalcitrant administration and order it to communicate documents. The extent of the administrative court’s powers could already be gauged in the well-known decision in Barrel (8), where the court enshrined its investigation methods by asking the administration for all documents in light of which a decision had been made.

Transposed directly to the disclosure of an administrative document to a citizen, case law acknowledges that the court may “require that competent administrations produce all necessary documents” to decide the case. The court’s investigative powers are so great that it may even require “those documents for which the refusal to communicate is the very subject of the dispute” (9). In such cases, the document will not necessarily be communicated to the applicant (10) but will serve to inform the court as to the document’s contents.

Privacy is therefore afforded particular protection by French administrative law, especially in relation to the modalities for communicating documents. However, the obstacles to the disclosure of administrative documents (concerning, in particular, timescales for obtaining them, being protected by the court) come up against confidential matters held by the administration.

II – The administration’s secrets: protecting the privacy of public entities

The secrets held by public entities prove to be veritable fortresses preventing citizens from proving the harm they have suffered (section A). However, there are exceptions allowing citizens
to obtain disclosure of such documents. More generally, the data relating to the administration tend to be increasingly accessible and published (section B).

A – The administration’s secrets: an obstruction to the law of evidence in legal proceedings

Where a document relates to a government secret and affects State interests more generally, the administration must refuse to disclose the same. The result is a failure to produce evidence in support of the allegations made by the applicants.

Documents relating to military secrets, foreign policy, State security or even public or individual security cannot be disclosed. Thus any documents that may reveal negotiations with other States, intelligence or data gathered by a State on the behaviour of another State and thus challenging the latter, or even documents that may have repercussions for current State relations may not be disclosed.

The 1978 Law also makes general reference to secrets that are protected by law, thus precluding the need for an exhaustive, closed list of documents not to be disclosed.

In the context of administrative proceedings and in order to obtain evidence, the only possibility of obtaining a classified document is for it to be declassified.

Documents relating to public security or that may affect the safety of physical persons may occasionally be disclosed in whole or in part where disclosure of the same does not run the risk of having repercussions that worsen the situation for said persons. This is the case, for instance, for gendarme or police reports where legal action has not been taken.

In tandem with the protection of official secrets, there is now greater transparency in the publication of data held by the administration.

B – The expansion in the disclosure of administrative data

Data held by the administration includes data concerning public persons representing the administration, such as members of the Government (who may be called upon to publish their tax returns), as well as the administration’s own public data.

The latter category is overseen by the Direction de l’information légale et administrative (DILA – the Directorate of Legal and Administrative Information), which is a central administrative directorate within the Prime Minister’s Office. The DILA is also responsible for publishing and distributing the Journal officiel, the legislature’s Official Journal containing French legislation and regulations.

This distribution makes all French legal rules available to all, and guarantees economic and financial transparency through the national publication of all legal, economic and financial information pertaining to businesses and the voluntary sector. The DILA interfaces with each Ministry website, together with the Légifrance site, which provides access to all legislation, case law and Codes. Citizens thus have guaranteed access to documents produced by the Administration that can generally concern them.
The growth of open data fits into the above approach. Open data allows government data to be accessed in digital format. In the context of respect for the general interest, public information is part of a common good. Data may therefore be accessed by all, allowing restrictions on rights of access to and the re-use of data to be circumvented.

The publication of open data is possible thanks to open knowledge. The latter is defined as knowledge of any work, whatever its format, be it musical, cinematographic, etc. It also concerns data such as a scientific paper, or geographical, governmental or administrative information. This open access to data allows original works to be used, re-used and distributed freely.

Open data fits into a broader initiative for transparency and citizen participation that can be found in all open access policies and is sometimes known by the ODOSOS2 acronym (“open data, open source and open standards”).

This dematerialization of and large-scale access to public data must not, however, affect personal data. As regards dematerialization, be it of public or personal data, the protection of privacy and of personal data can currently be seen as a principle defended in vain. The ease and freedom of access afforded by the internet must not obscure the potential invasions of privacy that it can engender.

The new challenge for the Administration is therefore not to improve the timeframes applicable to disclosure or appeals, but above all to ensure that secrets are sufficiently well guarded. The balance between transparency and privacy has yet to be struck in a satisfactory manner, as that same balance is upset by new technologies that have yet to be fully understood.

Notes:
(1) (http://www.cada.fr)
(2) Full title: Loi n° 78–753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.
(3) Projet de loi sur le renseignement, 2015.
(4) Sweden has recognised the right of access since 1776.
(5) The Spanish Constitution has protected the right to information since 1978, Italy since a law of 7 August 1990, and Germany since 2006.
(6) Article 6 of the 1978 Law.
(9) CE, 23 December 1988, Banque de France c/ Huberschwilfer, n° 395310.
(10) CE, 14 March 2003, Kerangueven, n° 231661.
The terrorist attacks that took place in Paris in January 2015 have reopened the debate on passenger name records (PNRs), files created by airlines for each flight booked by a passenger—highly intrusive in terms of privacy as they concern data of a personal nature (hereinafter referred to as “personal data”)—containing names, methods of payment and, potentially, dietary requirements or health issues, even contact details for the passenger. According to the former chairman of the Commissione nationale informatique et libertés (CNIL) generalised registration threatens to put “privacy in jeopardy” (1).

Indeed, the war on terror raises the issue of striking a balance between the protection of privacy and the preventive measures implemented without the oversight of a court or an independent authority. The United States rides roughshod over privacy—the Privacy Act 1974 is very narrow in scope (2)—while the European Union and its Member States consider the protection of personal data as a fundamental right—Article 8 of the Charter of Fundamental Rights of the European Union (CFREU) and Article 16 of the Treaty on the Functioning of the European Union (TFEU). Enshrined by Convention n°108 of the Council of Europe of 28 January 2001 and by the interpretation of Article 8 of the European Convention on Human Rights by the eponymous Court (3)—echoed by decisions handed down in France by the Constitutional Council (4) and the Conseil d’État (5)—the protection of personal data is governed in particular by Directive 95/46/EC of 24 October 1995, supplemented by Council Framework Decision 2008/977/JHA of 27 November 2008. The scheme, inspired by France’s Informatique & Libertés (data protection and civil liberties) Law (6), forbids the inclusion of sensitive data—concerning race or ethnic origin, political persuasions, religious or philosophical beliefs, union membership or those relative to drug and alcohol abuse, health or sex life—in data processing and makes such data subject to monitoring by an independent administrative authority—the CNIL in France, the European Data Collection Supervisor (EDPS) for the European Union. Article 29 of the Directive establishes a European group of national authorities—the “G29”—to contribute to the consistent implementation of national provisions. Any person whose personal data has been entered into a database has the right to informed, a right of direct access, a right to have data rectified, a right to object and, more recently, a “right to be forgotten” (7). These are not genuine rights over personal data, but rather personal rights over the processing carried out through a third party (8), even though the Conseil d’État recommends “conceptualising the right to data protection as a right to “informational self-determination”, which is to say the individual’s right to decide on the disclosure and use of his or her personal data” (9).

Counter-terrorism co-operation between Europe and the United States must reconcile conflicting approaches, as illustrated by the events surrounding PNRs and the Society for Worldwide Interbank Financial Transactions—Terrorist Finance Tracking Program (SWIFT–TFTP) agreements, which have caused conflict at the very heart of European Union institutions owing, on the one hand, to differences of perspective on the concessions to be made by the Commission and the Council;
and, on the other hand, those to be made by the Court of Justice and the European Parliament (section I). This inter-institutional opposition has prevented the adoption of a European PNR, but France has decided to follow the British example by developing a national PNR. On a European and French level, other measures to prevent terrorism threaten privacy through the widespread surveillance and collection of personal data (section II).

I – Co-operation between the European Union and the United States in the prevention of terrorism versus the fundamental right to protection of personal data
Commission Directive 95/46 defines an adequate level of protection to be attained in each Member State and prohibits the transfer of data to any country not providing a similar level of protection. The United States does not offer adequate guarantees – unlike Australia or Canada, with which nations PNR agreements have been adopted (10) – which explains why such long negotiations were necessary to conclude the PNR (section A) and SWIFT-TFTP (section B) agreements.

A) PNR Agreements
The differences of perspective within European institutions on the legality of the initial agreements concluded with the United States (section (a)) led to the adoption of an agreement in 2011 which better respects data protection (section (b)).

a – The 2004 and 2007 Agreements
The Aviation and Transportation Security Act 2001 requires airlines operating flights to, from or through the United States to allow the US authorities to access PNR data, on pain of heavy fines, even not being able to enter American airspace, but European carriers could not then comply with those requirements, being incompatible with EU law and their national legislation.

An initial agreement was therefore concluded on 28 May 2004, but Commission Decision 2004/535/EC and Council Decision 2004/496/EC implementing that agreement into European law were annulled on 30 May 2006 by the European Court of Justice (11), which nevertheless maintained the effects of the agreement until 30 September 2006. Following an interim agreement of 19 October 2006, which expired on 31 July 2007, a new agreement was concluded on 23 and 27 July 2007. This provided that air carriers would allow the Department of Homeland Security (DHS) to access data concerning passengers travelling to or from the United States; however, in May 2010, the European Parliament (EP) deferred its vote on the agreement and called on the Commission to negotiate a new agreement.

b – The 2011 Agreement
The new PNR Agreement (12) provides that carriers are to provide the DHS with their data in order to prevent or detect terrorist offences or criminal offences related thereto, together with transnational offences punishable by at least three years’ imprisonment, or in the face of a serious threat or even if a court orders it. The DHS must filter and delete within 30 days – except in cases of threats to a person’s life or a specific criminal procedure – sensitive data, and protect all other data from any alteration, destruction or unauthorised disclosure. The DHS must inform the European authorities of serious incidents of invasion of privacy of European citizens. PNR files are stored in an active database for five years then transferred to a dormant database for ten years or longer in the event of investigations or prosecutions; however, six months after they have been received, the files are "anonymized" (removal of information allowing identification).
The Agreement provides that the DHS may only share the PNRs with Europol, Eurojust or national public authorities investigating the abovementioned offences; thus the use of PNR data runs the risk of extending to uses other than the war on terror. There is cause for concern that a global profiling system infringing individual rights may be set up, the effectiveness of which has not been established: a total of two terrorists have arrested further to the transfer of PNR data and the diversions of aircraft en route to the United States have only concerned instances of similar names (13) and journalists who have been overly critical of US policy (14).

B – The SWIFT–TFTP Agreement
Here too, the EP opposed legislation that infringed the fundamental right to the protection of personal data (section (a)), thus forcing the EU to renegotiate an acceptable agreement (section (b)).

a – History
This Agreement takes its name from the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a Belgian company that processes nearly 80% of international bank transfers. Initially, the US authorities could serve administrative subpoenas on SWIFT in order to obtain data as its servers were located on US soil; however, influenced by data protection agencies (15), SWIFT now operates its processing and transfer of financial messaging data from the Netherlands and Switzerland.

In order to reconcile the war on terror and European law on data protection, an Interim Agreement was negotiated and accepted by Council Decision 2010/16/CFSP/JHA of 30 November 2009. In spite of pressure from the US (16), this initial SWIFT–TFTP agreement was rejected by the EP on 11 February 2010, owing to the lack of proportionality between the rules relative to data transfers, their storage and the security allegedly provided and because European citizens would not have been able to appeal against US authorities in the event of a wrongful use of their personal data as the Privacy Act reserves such actions for American citizens (17).

b – The Agreement
The new SWIFT–TFTP Agreement (18) provides that financial messaging service providers must, at the request of the United States Treasury Department, transfer data to the latter for the purposes of preventing and detecting terrorism or the financing thereof. Treasury subpoenas must clearly identify the data necessary for anti-terrorist intelligence, investigations or prosecutions. A copy of such subpoenas is sent to Europol, which must verify that the request is admissible; in the affirmative, the request becomes legally binding, obliging the provider to export the data requested to the Treasury Department. Nevertheless, Europol's supervision has been heavily criticised for being ineffective by both the Joint Supervisory Body (19) and the EP (20).

The data thus transferred is deleted after five years, while the information extracted from the data provided is kept for the period necessary for specific investigations or prosecutions.

The Treasury Department can share the data with any State or international organisation, as well as with Europol or Eurojust, but any sharing of information relative to an EU citizen with the authorities of a third party is subject to the prior agreement of the authorities in the relevant Member State, except where the sharing of data is essential in preventing a serious and immediate threat. The Treasury Department can also share relevant information obtained in the context of
the TFTP at the request of Europol, Eurojust or a competent authority in a Member State of the European Union.

The Agreement structures transparency; access, rectification, deletion or blocking rights; the preservation of the accuracy of information; and appeals. Its innovation lays in the monitoring of guarantees by independent supervisory bodies, including a person appointed by the European Commission with the agreement of the United States.

The EP accepted this new, more balanced agreement – and also because the European Banking Federation had stressed the need to return to legal certainty, which the vote of 11 February 2011 had undermined (21).

The PNR and SWIFT–TFTP Agreements continue to be criticised owing to the absence of an independent administrative authority responsible for the protection of personal data in the United States, and they also elicit fears as to excesses that Edward Snowden’s revelations have only served to intensify. The fundamental right to protection of personal data has been sacrificed on the altar of the prevention of terrorism, as the Commission has not been able to obtain from the United States that which it secured from Australia or Canada (22).

II – The right to protection of personal data and French and European preventive measures
The establishment of a PNR system, together with other methods for mass, indiscriminate surveillance, are hot topics in the EU (section A) and in France (section B).

A) European Union measures
The development of a European PNR is back on the agenda (section a); however, the annulment of the Data Retention Directive offers food for thought as to the compatibility of systematic preventive measures with the CFREU (section b).

a – The issue of the European PNR
In November 2007, the Commission presented a proposal for a directive establishing a European PNR for the purposes of preventing terrorism, which was rejected the following year by the European Parliament. The Commission then submitted a new proposal in 2011 (23), but the EP again opposed it on 24 April 2013 – which did not prevent the Commission from funding national PNR projects in 14 Member States (24).

On 11 January 2015, the French Minister of the Interior exhorted the EP to adopt the European PNR, which request was relayed two days later by the President of the European Council who feared that in the absence of such a Directive, 28 national systems would be set up, forming a “patchwork full of holes”. The change of position on the part of ADLE and S1D MEPs will be crucial to the adoption of the PNR Directive, but many will make their vote subject to the Court’s forthcoming decision on the PNR Agreement concluded with Canada (25).

In addition, Directive 95/46 having to be replaced by a Regulation (26) and the Framework Decision by a Directive (27), it would be appear more logical to wait for that legislation to be adopted before envisaging a vote on a PNR Directive which will have to be compatible with it.
b - Other preventive measures
Following the terrorist attacks in Madrid and London, Directive 2006/24/EC of 15 March 2006 on the retention of data was adopted in order to harmonise national measures requiring telecommunications and IT service providers to retain client metadata – and not the content of communications or websites visited – in order to supply the same on request to police or intelligence services.

Two referrals were made to the Court of Justice for a preliminary ruling on the compatibility of the Directive with the CFRE; the Court found that it was incompatible, given that “[t]hose data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained…” (ground 27), which constituted an “interference […] [which was] wide-ranging […] likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance” (ground 37), all the more so as the Directive covered “in a generalised manner, all persons and all means of electronic communication” (ground 57), provided no “objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use” (ground 60) and that the retention period had been set without taking account of the usefulness of the retention as compared to the objectives pursued (grounds 63 & 64) (28).

This indiscriminate and disproportionate surveillance differs from Europol’s operational measures or the co-operation and exchange of information between law enforcement authorities (29) which target persons who have already been convicted or are strongly suspected in the context of procedures overseen by judges. The strict rules on the protection of personal data – which should be strengthened with the adoption of the proposed Regulation and Directive (30) – that apply to Europol offer satisfactory guarantees, reconciling the war on terror and privacy (31).

B) French measures
France has set up her own PNR system, which is not operational as yet (section a), together with surveillance measures, the most recent of which have only been adopted by the National Assembly – the Senate and the Constitutional Council (to which the President ought to refer the issue) not having decided yet (section b).

a - The French PNR
Article 7 of Law n° 2006–64 of 23 January 2006 on the war on terror authorises the collection of PNR data and Advance Passenger Information (API – passenger data collected by airlines at the check-in stage for any given flight) for international travel to or from third-party States to the EU. This also applies to data directly collected from the machine readable zone on travel documents, identity cards or visas held by passengers travelling with air, sea or railway carriers.

An Order of 19 December 2006 instituted, on an experimental basis, an air passenger record that only concerns passengers aboard direct flights to or from Afghanistan, Pakistan, Iran, Syria and Yemen. However, the experiment mostly revealed “a lack of rigour in the transmission of data by some airlines and […] multiple errors due to similar names or inaccurate transcriptions of names” (32).

Furthermore, Article 65 of the Code des douanes (Customs Code) allows the Administration to demand PNR data expressly and on an ad hoc basis for certain flights.
Article L.232–7 of the Code de la sécurité intérieure (CSI – Internal Security Code), resulting from the 2013 Law on military planning, establishes the French API–PNR system (from which sensitive data is expressly excluded) for flights travelling to or from France, as implemented by Decree n° 2014–1095 of 26 September 2014. In an opinion of the same date, the CNIL considered that the guarantees reduced the risk of data protection infringements (33).

b – Extending surveillance
The Law on military planning also allows the intelligence services to create an automated data processing system (Article L. 232–7–1 CSI), under the supervision of the Commission nationale de contrôle des interceptions de sécurité (CNCIS).

Articles L. 246–1 to L.246–5 CSI require communications operators to retain, for a one–year period, all metadata in order to fulfil requests from anti–terrorist or intelligence services. As this processing of such “traffic data” by those services constitutes purely administrative police operations, so the ordinary courts do not have jurisdiction (34).

The draft bill on intelligence lists seven public–interest grounds (35) that allow, under future Article L 853–1 CSI, the “use of technical devices allowing [...] the collection, transmission and recording of computer data transiting through an automated data system or contained within such a system”. These measures will be supervised by the Commission nationale de contrôle des techniques de renseignement (CNCTR) – an independent administrative authority replacing the CNCIS – which will submit an opinion to the Prime Minister on the authorization of data collections, except in the event of absolute urgency.

The draft bill also introduces significant innovations into the CSI, including the guarantee of privacy and – thanks to a parliamentary amendment – the protection of personal data and reference to the proportionality principle (36) (Article L.811–1), the destruction of data extracts or exploitations that are no longer essential (Article L.822–3) and, above all, the possibility of bringing an appeal before the Conseil d’État, which option is open to any person with a direct and personal interest, the CNCTR or any court making a referral for a preliminary ruling. The Conseil’s requests cannot be refused on “military secrets” grounds, even though it will not disclose any information classified as such (Article L.841–1).

It is still too early to know what the law on intelligence will ultimately be; nevertheless, France is attempting to perform a balancing act between the prevention of terrorism and the protection of personal data. Future case–law interpretations of the Digital Rights decision, be it in France or the EU, may tip the scales in favour of the latter, at the expense of Articles L.246–1 to L.246–5 CSI. Even if the current trend is towards greater security measures, all is not lost for privacy.

Notes:
(1) A. Türk, La vie privée en péril. Des citoyens sous contrôle, Odile Jacob, 2011.
(3) ECHR, Leander v Sweden, Application n° 9248/81, 26 March 1987; ECHR, Amman v Switzerland, Application n° 27798/95, 25 March 1998; ECHR, Rotaru v Romania, Application n° 28341/95, 4 May 2000; ECHR, Turek v Slovakia, Application n° 57986/00, 14 February 2006; ECHR, S. &
53

Marper v United Kingdom, Applications nos. 30562/04 and 30566/04, 4 December 2008; ECHR, Dimitrov–Kazakov v Bulgaria, Application n° 11379/03, 10 February 2011; ECHR, Association “21 December 1989” and others v Romania, Application n° 33810/07, 24 May 2011; ECHR, Brunet v France, Application n° 21010/10, 18 September 2014. The Court nevertheless recognises that the war on terror may justify restrictions on the confidentiality of correspondence and telecommunications (ECHR, Klass and others v Germany, Application n° 5029/71, 6 September 1979) or the conservation of certain types of data by the security services (06.06.06, Segerstedt–Wiberg and others v Sweden, Application n° 62332/00, 6 June 2006). Cf. A. Petropoulou, Liberté & sécurité : Les mesures anti–terroristes et la Cour européenne des droits de l’Homme, Pédone, 2014, p. 443–461.

(4) Decision 2012–652 DC of 22 March 2012, Loi relative à la protection de l’identité, para. 8; the Constitutional Council found that judicial police files were constitutional (Decision 2003–467 DC of 13 March 2003, Loi sur la sécurité intérieure, para. 17–46), as was the fichier national automatisé des empreintes génétiques (FNAEG – automated DNA database) regarding, in particular, the identification of perpetrators of terrorist acts (Decision 2010–25 QPC of 16 September 2010).

(5) CE, Ass., 26.08.11, Association pour la promotion de l’image, Rec., p. 505.


(10) Agreement between the European Union and Australia, 13 September 2011, inter–institutional dossier 2011/0126 (NLE); Agreement between the European Union and Canada, 30 November 2011, inter–institutional 2013/0250 (NLE) – the latter has yet to be approved by the EP, which has referred the issue of the Agreement’s compatibility with the CFREU to the ECJ. In the interim, a previous agreement between the EU and Canada, concluded in 2006, remains in force. Furthermore, an agreement between the EU and Mexico is under consideration, while Russia and South Korea have made similar requests.


(12) Inter–institutional dossier 2011/0382 (NLE), 8th December 2011.


(14) Cf. Le Monde, 03.10.12.


(16) Cf. J. Santos Vara, The Role of the European Parliament in the conclusion of the Transatlantic
Agreements on the Transfer of Personal Data after Lisbon, CLEER Working Papers, 2013/2, p.16.


(18) OJEU, L.195/5, 27.07.10.


(20) www.europol.europa.eu/en/pressroom/content/20110314IPR15463/html/SWIFT


(33) www.cnil.fr/les-themes/deplacements-transports/du-systeme-api-pnr-france/


(35) National security, essential foreign policy interests and the execution of France’s European and international commitments; France’s essential economic and scientific interests; prevention of terrorism; prevention of the re-formation or continuation of disbanded groups; prevention of organised crime; prevention of collective violence likely to constitute serious offences affecting the maintenance of law and order.

The personal life of the employee versus the interests of the company
Chantal Mathieu, Associate Professor, University of Franche-Comté


The interface between the employee’s right to respect for private life and the company’s interests is based essentially on a case-law construct. Any student of French labour law knows the Ronsard case (1), named after the secretary at a car dealership who was dismissed for purchasing a vehicle produced by a rival manufacturer. For the employer, as for the trial judge, the purchase undermined the brand and therefore justified the dismissal. Relying on Article 9 of the Civil Code, the Social Chamber of the Court of Cassation took a different approach and set down a strong distinction between private life and its effect on the company’s operations. Yet the solution was heavily criticised by authors on the grounds that the purchase of a vehicle could not be classed as private life (2). This criticism was echoed by certain authors (3) who proposed that “personal life” designate acts outside the scope of an employer’s power. The Social Chamber of the Court of Cassation (4) then the legislature (5) were quick to adopt the term which is why, since Ronsard, court decisions and the Labour Code rarely use the term “privacy”, preferring “personal life”. The latter term refers not only to private life in the strict sense, but more broadly to the employee’s individual freedom, together with his social and family life.

Since the 1990s, there has been a proliferation of rules protecting the personal life of the employee against employer interference. The employee is primarily a person; he has an inalienable freedom, despite his subordination. The Court of Cassation also considers that the employee is entitled, even on work premises and during working hours, to respect for private life and an employer cannot freely read the employee’s private correspondence (6). Beyond the prohibition on interference by the employer in the employee’s personal life, the French legal system also tends to grant the employee the means to pursue his personal life without sacrificing his professional life. This is why various rules compel the employer to take into account extra-professional details before making a decision about his employee (7).

Still, as revealed in Ronsard, the choices made by the employee in his personal life sometimes collide head-on with the company’s interests. A conflict must then be resolved between the employee’s interests and those of the company: which should be upheld? Occasionally, priority is automatically given by law to the employee’s personal life, especially in cases involving a serious family situation (8). More often, legislation requires that a balance be struck between the company’s interests and those of the employee and, in the event of a dispute, entrusts the courts with the task of separating the two (9). There remain scenarios in which precedence is given to the company’s interests. The way in which those interests are grasped can then either guarantee and curtail the employee’s personal life. One point seems clear: the employer is not the one to decide the matter. In other words, it cannot content itself with arguing the company’s interests in imposing its decision and thereby sacrifice the employee’s personal life. It must explain its decision, stating how the interests of the company are at stake. Two levels of argument registers are admissible: the smooth running of the business, and company safety. At first glance, the
I - Personal life protected by the objectivisation of the smooth running of the business

As part of its management powers, the employer must make decisions to ensure the smooth running of the business. When it considers that a malfunction is attributable to the employee’s personal life, it will make a decision affecting the latter’s interests. To avoid the arbitrariness of power, the Labour Code establishes procedures requiring that the employer explain its vision of the proper running of the business, thereby opening up room for discussion (section A). In addition, the courts tend to outline the concept of the smooth running of the business by establishing a set of indicators to assist in its definition. The employer’s response to the employee’s behaviour is then no longer assessed in light of what the employer identifies as the company’s interests, but rather in terms of an objective point of reference: disruption (section B).

A - Room for discussion

The Labour Code contains many prerogatives allowing the employee to suspend his employment contract or reduce his working time in order to devote himself to personal projects. He may wish to take a training or an educational course (10), devote himself to a charity project (11) or even take a sabbatical (12). The employee’s absence may hamper business operations. Additionally, the law sometimes allows employers to oppose the employee’s departure. The exact conditions vary depending on the legislation, but we do a common reference: the smooth running of the business. In order to halt the employee’s plans, the employer must objectivise the reasons for its decision. It must then issue written information for the employee, giving reasons for the decision. It must also account for its position with staff representatives who, where appropriate, are simply informed or to be consulted on the final decision or give their consent (13). In the event of a dispute, the employer’s refusal can be challenged in court through an accelerated procedure. The employer must then provide proof of the organisational difficulties caused by the employee’s plans. Specifically, it should demonstrate how the person’s absence would have “adverse consequences for production and the smooth running of the company” (14). It must therefore not plead mere inconvenience but the risk of real harm to the company. Sometimes, the legislature goes further and completely removes any room for discussion by setting down an arithmetic criterion. Refusal is then possible if the number of employees concerned by the application reaches a certain threshold relative to the company’s workforce (15). A malfunction is treated as a percentage of employees concurrently (16) or successively absent over a reference period (17). No risk assessment is therefore left to the employer alone.

B - Characterising objective disruption

Since the early 1990s, the Court of Cassation has tended to reject any grounds for dismissal based on subjective criteria specific to the employer. This is why the loss of confidence (18) or the risk of a conflict of interest between the employee and his employer (19) cannot constitute acceptable grounds for dismissal. Thus, an employee cannot be dismissed simply because his spouse works for a competitor (20). In addition, the Court of Cassation made a careful distinction between an employee’s behaviour in his personal life and his impact on the running of the business. The employee’s attitude of the employee in his personal life can never be grounds for dismissal. However, if the employer proves that this attitude caused disruption, it may issue a non-
disciplinary dismissal (21). Disruption is a legal standard that gives rise to a variety of arguments. Yet the Court of Cassation has established a narrow framework. Not only must the disruption be physically verifiable, but it must also have a degree of intensity. Again, moderate disruption will not suffice. Above all, the Court of Cassation has outlined indicators for establishing it.

Disruption is considered as a malfunction in the running of the business due to the employee’s personal life, likely to cause harm to the company. Firstly, this may be a strong reaction from third parties (colleagues, clients, sub-contractors) with respect to the employee’s personal circumstances. The employer must demonstrate a proven risk of disruption due to such condemnation. Publicity surrounding a private act is not sufficient. The publicity must also provoke indignation or act the company’s reputation. Such will be the case for example when an employee’s conviction for raping a minor causes a considerable emotional reaction on the part of colleagues who have to associate with the mother of the victim who also works in the business (22). Similarly, the indictment of an employee for indecent assault while running an establishment for people with disabilities is likely to bring the organisation into disrepute (23). The malfunction may also consist in a lack of activity on the part of the employee owing to personal events, without that inactivity being described as wrongful. Such is the case when the employee is ill. His prolonged absence may hamper the smooth running of the business. However, the disruption will be accepted if it was such as to compel the employer to seek a permanent replacement (24). The Court of Cassation also accepts that the withdrawal of a driving licence for offences committed outside the scope of an employee’s functions is an objective situation and cannot characterise a disciplinary offence (25) but justifies the termination of the employment contract where the licence is necessary for the effective exercise of the professional activity (26).

The smooth running of the business might be a subjective reference, allowing the employer to give precedence systematically to the company’s interests, as viewed by the employer, at the expense of the employee’s private life. The objective reading given by the Court of Cassation prevents such a drift. However, the case law may easily be circumvented if the employer relies on a different argument: company safety.

II – Personal life stifled by company safety
The company’s interests may take on safety aspects. The people present in the company, whether customers or employees, must be protected. Property allocated to the business activity cannot be damaged or used to cause injury to others. In order to avoid incurring civil or criminal liability, the employer is duly authorised to supervise and punish. That authority may quickly impact on the employee’s personal life. However, the test applied by the courts to the employer’s arguments is quite weak. Safety becomes an argument that easily justifies the extension of such supervision of employees in the workplace (section A) or of discipline outside working hours (section B).

A – Extending supervision in the workplace
In the name of the right to respect for private life, there is a framework governing an employer’s access to personal information. As regards email (27), folders (28), sound recordings (29) or SMS (30), the Court of Cassation makes a distinction between professional and private documents. While the employer is free to read the former, it must follow a specific procedure for the latter. In particular, it must first inform the employee so as to allow him to the present. However, the Court has stated such documents may be opened in the employee’s absence “in case of a particular risk or event” (31). The same rules apply to the opening of a locker or a desk drawer (32). As regards
searching an employee’s personal belongings, such as a handbag, this is framed more extensively. The employer must obtain the employee’s consent and inform him or her right to refuse and to require the presence of a witness. Yet again, the Court of Cassation raises the possibility of “exceptional circumstances” overriding the need for the consent of an employee who refuses to open his bag (33). Such phrasing provides the employer with the means to respond quickly where company safety is compromised. One thinks, for example, of the risk of a terrorist attack, computer viruses or unfair competition. Nevertheless, the Court has not established objective criteria that would identify these extraordinary powers. It sets down no procedural requirements such as the presence of staff representatives. An examination of the various judgments shows that security appears as an end in itself legitimising emergency rules. However, if the employer could invoke security as soon as it has the slightest suspicion, the right to respect for private life on company premises would be an empty shell. Moreover, only a situation of extreme urgency must be able to justify such an invasion of an employee’s privacy. In all other cases of “particular risk or event,” the Court has encouraged employers to use the ex parte procedure provided under Article 145 of the Civil Procedure Code. This procedure allows the applicant to request that the presiding judge of the tribunal de grande instance (regional court) order the investigative measures required to protect the rights of others (34). It therefore implies the consideration of the legitimate grounds invoked by the employer before it conducts investigations.

B – Extending discipline outside working hours
In disciplinary matters, the Court of Cassation makes the distinction between personal and professional life. Acts falling within the scope of personal life enjoy immunity in the sense that the employer cannot under any circumstances use these to justify a sanction (35). This distinction does not, however, mean that an employee is completely free outside working hours. The safety approach allows the employer to sanction various forms of behaviour when the employee is no longer finds himself in a work context. Firstly, the Court of Cassation (36), like the Conseil d’Etat (37), considers that so long as he is on company premises, the employee is under a duty not to undermine the safety of other staff, even when he is not working (38). Next, the employment contract gives rise to a continuous duty of loyalty. This obligation has two facets: contractual loyalty and the loyalty of the contractor. The first allows the court to identify the duties and obligations inherent to a same category of contracts where the parties have not expressed their intentions. The Court of Cassation recognizes that the employee owes a non-competition obligation (39) and a duty of discretion (40) for the term of the employment contract. The second allows the employee’s behaviour to be scrutinised and any maliciousness, dishonesty, or insulting, defamatory or excessive statements to be sanctioned (41). This is why derogatory comments about the company that are expressed on social media such as Facebook can be qualified as misconduct (42). The company’s safety is protected by the reference made to loyalty. The Court of Cassation tends to take an increasingly broad approach, going so far as to sanction an employee’s silence on information relating to his professional activities, which, had they been known to the employer, would have allowed him to anticipate a risk (43).

Lastly, the Court of Cassation links acts to the “life of the company” in order to justify the imposition of a disciplinary sanction. These are acts committed while the employee is no longer under the subordination of the employer but which are dangerous in nature and likely to incur the employer’s liability. Thus a disciplinary sanction was imposed on a waitress who smoked on the premises in spite of the legal ban and made racist comments about another waiter (44). Similarly, a care assistant was sanctioned for using her mobile telephone on clinic premises outside working
hours when she was bound to respect the rule prohibiting the use of mobile telephones within the building on grounds of patient protection (45). An employee, who had won a holiday following a competition organized by his employer, could be dismissed for misconduct for assaulting one of his colleagues during his stay (46).

The duty to ensure safe results which is incumbent on the employer certainly comes to bear in case law. At the same time, however, the Court dismisses all the guarantees usually offered to the employee on the grounds that it is not a matter of monitoring the employee in the performance of his duties. Thus, as regarded an employee who had just left his post still wearing his work clothes and had dishonestly taken a telephone that a customer had forgotten at the store’s ticketing desk, the Court held that this behaviour impacted on the employer’s obligation to ensure the safety of customers and their property, and was linked to the life of the company. The evidence was taken from a CCTV system and the employee challenged the employer’s compliance with the provisions of the Labour Code relating to the implementation thereof (47). The Court dismissed the argument on the grounds that the system had been installed to ensure the safety of the store and had not been used to monitor the employee in the performance of his duties (48). Safety comes into play here, linking the employee’s behaviour to disciplinary power and excluding guarantees related to surveillance and monitoring. The safety-based approach restricts the scope of personal life, without any objective limit being identified, and without any parameters being set for safe surveillance. There is therefore a significant risk that the employer will judge any behaviour on the part of the employee by artificially linking them to a risk for the company. A romantic relationship between two colleagues which then turns sour could quickly pass for sexual or psychological harassment (49). The illegal downloading of music files with a laptop made available to the employee could quickly be seen as conduct that would incur the employer’s responsibility (50). Gradually, buying a brand of vehicle other than that marketed by the employer would end up being qualified as an act of mistrust in the quality of the company’s merchandise, thus putting its financial security at risk. Security is certainly a legitimate purpose but it is likely to bring down the whole edifice built since the Ronsard decision. Moreover, like the reference to the smooth running of the business, it is up to the courts to require not only the demonstration of materially verifiable elements but, more importantly, to outline the attendant issues.

Notes:
(2) J. Savatier, La protection de la vie privée des salariés, Dr. Soc. 1992, p. 329
(3) Ph. Waquet, Vie personnelle et vie professionnelle du salarié, CSBP, 1994, p. 289
(4) Soc. 14 May 1997, Bull. civ. V. n° 175 ; J. Richard de la Tour, La vie personnelle du salarié, rapport annuel de la Cour de cassation, 1999
(7) During a change of work schedule (L. 3123-24, Labour Code) or during the implementation of a mobility clause (Soc. 28 January 2015, No. 13-28111).
(8) E.g. compassionate leave for bereavement (L. 3142–1 Labour Code), family care leave (L.3142–16, Labour Code), parental leave (L.1225–48 Labour Code); the employer cannot object to the employee’s decision.
(9) L. 1121–1 Labour Code
(11) E.g. international solidarity leave (L. 3142–32 Labour Code.) or leave of absence following a

(12) L. 3142–91 Labour Code
(14) Soc. 6 May 1998, No. 96–41066
(20) Soc. May 27, 1998, No. 96–41276
(22) Soc. 26 September 2012, No. 11–11247
(23) Soc. 21 May 2002, No. 00–41128
(24) Soc. 3 May 2011, No. 09–67464
(25) Soc. 15 January 2014, No. 12–22117
(26) Soc. 5 February 2014, No. 12–28897
(27) Soc. 17 June 2009, No. 08–40274
(28) Soc. 10 May 2012, No. 11–13884
(29) Soc. 23 May 2012, No. 10–23521 (personal voice recorder)
(30) Com. 10 February 2015, RTD 2015, p. 191, notes Adam P.
(31) Soc. 17 May 2005, No. 03–40017. The discovery of erotic photos in a desk drawer is not considered as such.
(33) Soc. 11 February 2009, No. 07–42068; Soc. 3 April 2001, No. 98–45818
(34) Soc. 10 June 2008, No. 06–19229
(35) Soc. 23 June 2009, No. 07–45256
(36) Soc. 4 October 2011, No. 10–18862 (an employee had left his dog inside his parked vehicle in the company parking lot and was not able to stop him attacking an employee).
(37) CE 27 March 2015, No. 368855 (staff representative who strikes a colleague during a break in a works council meeting)
(39) CE 27 March 2015 No. 371174; Soc. 9 July 2014, No. 13–12423
(40) Soc. 5 February 2014, No. 12–28255
(41) Soc. 28 April 2011, No. 10–30107.
(42) Cons. prud'h. (industrial tribunal) Boulogne–Billancourt, 19 November 2010, No. 10/00853
(43) Soc. 29 September 2014, RTD, 2014 N. obs Moizard, p. 762, Lexbase Weekly, No. 587 obs S. Tournaux (employee who conceals his indictment on charges connected with his his functions).
(44) Soc. 16 October 2013, No. 12–19670
(45) Soc. 5 February 2014, No. 12–27251. There could be a risk of interference between medical devices and the waves emitted by mobile phones
(46) Soc. 8 October 2014, No. 13–16793
(48) Soc. 26 June 2013, No. 12–16564
(49) Sexual harassment can be accepted even if the actions are taking place outside of time and place of work: Soc. 11 January 2012, No. 10–12930
(50) L. Casaux-Labrunée, « Vie privée des salariés et vie de l'entreprise », Dr. Soc. 2012, p.331
For a number of years, France has witnessed a veritable craze for deontological ethics. It is the fruit of a long gestation rooted in history but the renewal of which is influenced by the common-law and Scandinavian countries and related to a national context marked by "scandals" and a quest for "transparency in public life".

Long associated in mainland France with the regulated professions, since its introduction under that title in 1845 (1), deontological ethics now extends to an ever growing number of representatives of public-interest activities or those necessary to democracy, from journalists to members of administrative courts, including elected representatives and political leaders. No sooner do scandals come to tarnish new spheres than the word "ethics" is put forward as the appropriate remedy. It is then deemed necessary that members of the failing "profession" be subject to "a morally- and ethically-inspired collection of principles and rules of conduct, of empirical extraction, which suggest responsible behaviour by which the professional community is identified to ensure a climate of integrity and an activity that is both respectful of the general interest and conducive to retaining public confidence". The product of the combination of two Greek words: deon (that which is proper) and logos (knowledge), deontological ethics does indeed correspond to "knowledge", on the part of members of a given group, “of what is right or proper" (2). More exactly, it is a method of regulation, inspired by morality and law, which is nonetheless distinct from the latter two due to the concern for going beyond the traditional binary contrasts of "good vs evil" and "allowed vs forbidden", in order to foster a preventive approach to "doing better", thus setting aside the notion of punishment (3). According to the Supreme Court of Canada, “[e]thical rules are meant to aim for perfection" (4).

The fact that this “passion for deontology and ethics” (5) has got the better of the political sphere is symptomatic of a trend that some would characterise as “invasive”. Indeed, up until recently, popular legitimacy – as compared with the divineunction of monarchs under the Ancien Régime – appeared to make such a breakthrough unlikely. It has nevertheless gone very far as, in early 2014, when the gossip magazine Closer revealed his affair. The French press has been an arena for political point-scoring and jostling for position, sometimes to defend the private lives of heads of state, sometimes to demand full transparency of the same (6), and this under the gaze of a British and American media shocked by this French hereditary “mystère du pouvoir royal” (mystery of royal power) exception. Thus, The Guardian published an article titled “A very British scandal about a very French affair”, sub-titled "Now, France's tradition of privacy and discretion is under pressure from the global celebrity media" (7).

Quite aside the facts, this news illustrates the conflict between two principles. The first is the right to private life, a relatively recent fundamental right, the constitutional value of which was recognised by France’s Constitutional Council on the basis of Article 2 of the 1789 Declaration (8) and the respect of which is ensured by the European Court of Human Rights (ECHR) in light of
Article 8 of the 1950 Convention. The second is deontological ethics (defined above) which, while having a formal constitutional basis vis-à-vis judicial magistrates only pursuant to Article 65 of the 1958 Constitution, appears to be part of the very essence of a Constitution. In Bentham's posthumous publication, *Deontology or the Science of Morality* (1834), which gave birth to the concept, deontology was perceived as a new theory of duties in society, with the quest for individual and collective happiness as its ultimate purpose. What seems to foreshadow a genuine “deontology of the citizen” here concerned precisely that of the President of the Republic in the abovementioned affair, for which Article 68 of the Constitution makes reference to “a breach of his duties patently incompatible with his continuing in office” and that of the journalists responsible for revealing it, for whom the 1971 Declaration of the Duties and Rights of Journalists (known as the Munich Charter) features among the duties that it sets down, “feeling obliged to respect the private life of people”. A professional who is subject to a code of ethics shall thus be bound either by a duty of exemplarity in their private life, or by a duty to respect that of others.

Starting from the basic consideration that deontological or ethical rules and principles are, as has already been stated, inspired by morality and ethics, and that they become legal rules and principles owing to their incorporation into law, it is possible to wonder the extent to which such a regulatory method interacts with private life, when it is supposed to offer an alternative to the previous two but proves in reality to be a corollary of the same, and particularly of the law governing sanctions thereof. Do the concerns, on public interest grounds, of a professional who is ethically irreproachable in his private life, and respectful of that of the persons forming the subject of his activity, run the risk of ultimately becoming a potential channel for invasions of privacy, in the name of that same public interest? Indeed, an examination of the relationship between ethics and private life leads us to view the former as an extrinsic vector for restricting the private life of the professional falling within its remit (section I), together with a relative guarantee against professionals interfering in the private lives of others (section II).

I – Ethics, extrinsic vector for restricting the private lives of professionals

The proper exercise of a professional activity justifies the consideration given to ethical requirements within the “official” private lives of the individuals concerned, in a broader approach based on self-discipline (section A). However, the profession’s desire to avoid “scandal” is reflected in the invasions of privacy by a disciplinary scheme occasionally tainted by morality (section B).

A – The submission of professionals to a code of ethics in their private lives

Persons entrusted with public interest missions – at the forefront of which number we find elected representatives, political leaders and public officials – are inextricably bound to the activities that they perform. As explained by Christian Vigouroux, President of the Home Affairs Section of the Conseil d’Etat: “An official is no longer viewed as someone simply doing a job but, in some sense, as the bearer of a position which involves the Administration’s “reputation”, which is to say the confidence it can inspire in a service user” (10). He is an integral part of the Administration, thus blurring the distinction between the function and its holder. Such an approach necessarily has an impact on the behaviour that the official must adopt in his private life. This was especially well highlighted by the Commission de réflexion sur l’éthique dans la magistrature in its 2003 Report, with regards to members of the judiciary, in respect of whom citizens have the highest expectations. Having recalled that a judge is first of all a citizen who benefits, in that capacity, from rights and freedoms recognised in national and international law, the Commission noted that
“his behaviour is necessarily restricted by the duty of impartiality which must not only be observed subjectively internally, but also appear objectively as such in the eyes of litigants. Part of a judge’s life belongs only to him; it is inexorably private. But what cannot be ignored is the fact that part of his existence is subject to scrutiny (which the European Court of Human Rights expresses in the adage inherited from French law: “not only must justice be done; it must also be seen to be done” (11). This concern for transparency therefore implies the regulation of private life.

A misunderstanding must however be avoided as to the perimeter of such regulation. The European Court of Human Rights, cited by the “Cabannes” Commission, had incidentally given an indication on the subject, in its decision in Özpinar v Turkey of 19 January 2011 concerning ethics, stressing that: “professional life often overlaps with private life in the strict sense of the word, in such a way that it is not always easy to identify the capacity in which the individual acts at a given time” (12). Thus ethical regulation concerns that area corresponding to the “official” private life of the state official, in such a way that it supposes: “a proper delimitation between that which falls exclusively within the scope of private life and that which, whilst being private, may bring about professional consequences” (13). Without multiplying the examples here, there is one put forward by the 2010 Recueil des obligations déontologiques des magistrats (France’s collection of judicial ethics) is worthy of mention, insofar as it gives consideration to the relationship between private life and the personal approach towards various behavioural requirements. Point A.20 on independence states that: “[t]he judge has, like any other citizen, the right to respect for private life. However, he shall abstain from displaying relationships or adopting public behaviour of such a nature as to give rise to doubt as to his independence in his functions” (14). Equally, Point C.22 on integrity provides that: “In his private life, the judge remains subject to a strict duty of probity, which includes delicacy. He is bound to show discernment and prudence in his social life, his choice of relationships, the conduct of his personal activities and his participation in public events” (15). In order for the extra-professional behaviour of an official to be reproved by his profession’s code of ethics, that behaviour must be of a public nature and attain a certain degree of gravity. The European Court of Human Rights emphasised the same in the abovementioned decision, asserting that: “a judge’s ethical duties may impinge on his private life when, through his behaviour, though it be private, the judge damages the judiciary’s image or reputation” (16).

8. Ethics, vector for a discipline’s interference in private life

Submitting professionals to ethical principles and rules even in their private life thus appears as a tool for avoiding “scandal”, which may damage the image of the institution to which those professionals belong. However, once that has been noted, an examination of the means usually implemented to put an end to such failures leads us to identify within those codes of ethics a danger for private life, the former appearing to be a discipline’s “Trojan horse” infiltrating the latter. While the Conseil supérieur de la magistrature (CSM – France’s High Council for the Judiciary) considers that: "demonstrations in a judge’s private life do not ipso facto fall within the remit of disciplinary action" (17), First Presiding Judge Charvet observed that "the entry point for ethics in our country remains the discipline itself and the search for judicial responsibility" (18).

This situation – which is not specific to France – is linked, first of all, to the need to separate those bodies responsible for dealing with ethical and disciplinary failures. In its Opinion n° 3 of 2002, regarding the private lives of judges, the Consultative Council of European Judges (CCJE) “encourages the establishment within the judiciary of one or more bodies or persons having a consultative and advisory role and available to judges whenever they have some uncertainty as to
whether a given activity in the private sphere is compatible with their status of judge” (19). In France, the *Conseil d’État* in particular has subscribed to this approach, entrusting a *Collièges de déontologie* with the task of shedding light for any and all interested parties on the restrictions contained in the 2011 *Charte de déontologie* (or Ethical Charter) for members of administrative courts. Conversely, consulted by the Minister of Justice in the *Mur des cons* case, the CSM sitting in plenary session, duly empowered by Article 65 of the Constitution to give opinions on issues relative to the judicial code of ethics, was compelled to decline jurisdiction in the matter. Evoking a possible conflict in light of Article 6 (1) of the ECHR on the right to a fair trial, the CSM considered that its composition, shared in part with its disciplinary formations, would incidentally lead it to step out of “the field of ethics and into the sphere of discipline” (20).

From the moment when such a separation is lacking, the risk that submitting professionals to a code of ethics extending as far as their private lives will have disciplinary implications is all the greater as the degree of precision of the requirements in the field is either too great or too little. The CCJE thus recommends that “the standards applying to judges’ behaviour in their private lives cannot be laid down too precisely” (21). The danger would effectively be that of indulging in the same excesses seen in the judicial systems of the federated States in the US, where the judiciary is “subject to extremely detailed codes of ethics and sanctions that go so far as to include costs and fines, which had led some commentators to assert that it ‘is accepted in the United States that the state judiciary is not a judiciary that enjoys guaranteed independence’” (22). Conversely, it is possible to wonder whether it would be appropriate to see, in a disciplinary sanction based on legislation governing an overly imprecise code of ethics, an invasion of privacy not provided by law, and thus contrary to Article 8 ECHR (23). This was the position defended by Judge Sajó in a separate opinion in *Özpinar v Turkey*. The ECHR, no doubt in order to remain consistent with the opinion of the CCJE, preferred to approve the initial stage in its review, and held that the sanction was not proportionate to the legitimate aim pursued, on the grounds that “in cases relating to a functionary’s private life, the latter must be able to foresee, to some extent, the consequences of his private actions and, where applicable, benefit from sufficient guarantees” (24).

II—Ethics, relative guarantee against professional life interfering with private life

The proper exercise of a professional activity also rests on voluntary restraint on the part of professionals, who must safeguard the private lives of persons concerned by that activity (section A). Nonetheless, this ethical ban is likely to give way when the same right allows or orders such an infringement on the basis of an overriding reason in the public interest, or even where ethics has become that overriding reason and itself orders the same so as to protect the image of a given profession (section B).

A. Ethics as a guarantee of “voluntary restraint” on the part of professionals in private life

With a view to safeguarding integrity and public confidence vis-à-vis a given profession, the normative instruments that govern its members’ code of ethics are likely to contain one or several principles concerning respect for the private life of those persons concerned by the activity in question. In some fairly rare and belated texts, a general principle of “voluntary restraint” is set down; this belatedness relates to the date on which the respect for private life became a subjective right, i.e. with the Law of 17 July 1970. The same can be said regarding service provision and security. The most explicit affirmation is linked to employees of La Poste. The Decree of 10 November 1993 provides that the employee’s professional oath is subject to an undertaking signed with a second paragraph drafted as follows: “I hereby undertake to respect scrupulously...
the due confidentiality of correspondence, information concerning private life of which I may become aware in the performance of my duties” (25). Much more recently, the Code de déontologie de la police nationale et de la gendarmerie nationale (National Police and National Gendarmerie Code of Ethics), which was included in the regulatory section of the Code de la sécurité interne (French Internal Security Code) and came into force in 2014, provides at Article R. 444-21, paragraph 1, that: “the police officer or gendarme shall protect the privacy of persons, particularly during administrative or judicial investigations”. The Code de déontologie de la police nationale previously in force and, as its title indicates, applicable only to police officers, focused solely on respect for professional confidentiality (26).

For other professionals, the texts regulating their code of ethics mainly focus on the latter confidentiality requirement. This rule of law appears to be rooted in Article 378 of the old Penal Code, which provided: “Doctors, surgeons and other health officials, together with pharmacists, midwives and any other persons who, through their state, profession or temporary or permanent functions, are custodians of the confidential matters entrusted to them... who have disclosed said confidential matters, shall be punished”. This provision was subsequently adopted by Article 226-13 of the new Penal Code, without specific reference to this or that profession. This is why the Decree of 12 July 2005 on the rules of conduct for the legal profession warns members of the Bar against any breach of client confidentiality (27).

B – Submitting codes of ethics to general interest requirements
The ethical principles and rules of conduct that call on members of a given profession to respect the private life of persons concerned by their activity are not, however, absolute and must give way in the face of overriding requirements demanded by the general interest. In this respect, the right to respect for private life and ethical requirements come up against the principle identified by the Constitutional Council in its 1985 “Etat d’urgence en Nouvelle Calédonie” decision, according to which it falls to the legislature, pursuant to Article 34 for the Constitution, “to take the necessary steps to reconcile respect for freedoms and the safeguarding of public order without which the exercise of such freedoms cannot be guaranteed” (28); Without going over Council case law on privacy restrictions, it is possible to see that the abovementioned legislation governing professional ethics usually carries with it a number of conditions. Article R. 444–21, paragraph 1 of the Internal Security Code subjects respect for private life to the proviso “without prejudice to requirements linked to the performance of their mission”. Equally, Article 226–14 of the new Penal Code adds a qualification to the application of client confidentiality, and particularly when “the law requires or authorises disclosure”.

However, while the ethical principles and rules of conduct that protect privacy can falter when confronted with general interest requirements, the ethical requirement may itself feature amongst them. Far from being a purely hypothetical case, it is in fact precisely what has been seen in recent years in France, in the context of the fight against conflicts of interest in the public sphere. Firstly, ethics is becoming tougher. As the National Assembly’s ethics officer, Noëlle Lenoir, wrote in early 2014: “The Organic Law and Law of 11 October 2013 on transparency in public life, in founding the fight against conflicts of interest on a mechanism that was no longer solely preventive but also punitive, reinforce the ethical principles and practices instituted by the National Assembly... the parliamentary code of ethics has changed paradigms. A collection of “hard law” rules has broadly come to replace a “soft law” mechanism” (29). Next, the code of ethics permeates the various layers of private life. In its 2011 Report, the Sauvé Commission warned the legislature against an
“absolutist quest for transparency, with little concern for the private lives/privacy of public figures”. The Report consequently recommended that the institution of a mechanism for declaring interests ought to cover “only those jobs entailing responsibilities of particular importance” (30). However, two years later, the Bill of 17 July 2013 on ethics and the rights and obligations of civil servants provided for an extension of the *rationae personae* field for such declarations, although with the caveat “of not having an excessive adverse impact on the rights of officials subject to this new obligation to respect for their private life” (31). There was doubtless something prophetic about the latter stipulation as, in the two decisions handed down three months later on transparency in public life, the Constitutional Council emphasised several times that the submission of such declarations “containing personal data concerning private life, together with the publicity that may surround such declarations, infringe/violate the right to respect for private life; that, in order to be constitutional, such infringements must be justified on grounds of general interest and implemented in an adequate way that is proportionate to that objective”. While the Council ruled that the objective intended to “reinforce the guarantees for probity and integrity [of the interested parties], for preventing conflicts of interest and combatting the same” does indeed constitute grounds of general interest, the fact remains that the measure selected for implementing such an ethical requirement by law does not constitute an disproportionate infringement of the right to respect for private life (32).

Notes:
(2) *Supreme Court of Canada, Ruffo v Conseil supérieur de la magistrature* [1995] 4 R.C.S. 267, § 110.


(15) Özpınar v Turkey, *op. cit.*, para. 71.


(18) Opinion no. 3 of the Consultative Council of European Judges (CCJE) to the attention of the Committee of Ministers of the Council of Europe on the principles and rules governing judges’ professional conduct, in particular ethics, incompatible behaviour and impartiality, www.wcd.coe.int, para. 29.


(20) Opinion no. 3 of the Consultative Council of European Judges (CCJE), *op. cit.*, para. 29.


(22) Özpınar v Turkey, *op. cit.*, para. 25–26.

(23) Özpınar v Turkey, *op. cit.*, para. 76 and 79.


(30) Bill n° 1278 du 17 July 2013, National Assembly, p. 7.

Invasions of privacy via the internet: aspects of private international law
Jean Sagot Duvauroux, Associate Professor, CRDEI, University of Bordeaux


Evidently, all national legal systems are concerned about protecting individual privacy. However, in spite of this common objective, we cannot help but note that the technical arrangements for and the scope of that protection vary palpably from one country to the next (1). In particular, the relationship between the right to respect for private life and competing fundamental rights and freedoms (such as freedom of expression and freedom of the press) is the subject of very different conceptions depending on the legal culture, legislative policy or even the very meaning of what constitutes a person’s privacy.

The great disparity between national regulations explains for the most part the lack of standard legislation in this field. The protective rationales being so far removed from one another at this juncture, any attempt to reach a compromise seems doomed to fail.

In the absence of international agreements fully unifying legislation in this area, in the event of a legal relationship affected by an “international” element, it falls to private international law to perform the difficult task of ensuring the co-ordination of national legal systems.

This co-ordination is undertaken through the traditional mechanisms found in private international law, which allow the court hearing a given case to rule on its own international jurisdiction and to determine which of the various national protection systems concerned is applicable. Admittedly, this rationale is not exclusive to the protection of privacy. It is a line of reasoning that the court follows each time a situation between private individuals exceeds the framework established in one State and where there is no international unification of substantive law for the case in point.

Nevertheless, as regarding invasions of privacy, the expansion of the internet has considerably altered the situation.

Firstly, this technological and social development has conferred a hitherto unknown importance to private international law. Indeed, a consequence of the internet has been to multiply the possibilities of invading a person’s privacy, which possibilities are increasingly taking on an international character.

Next, from a more methodological point of view, we are currently witnessing a reconsideration of the relevance of the classic co-ordination procedures that are traditionally enshrined in French private international law. The latter, inspired by Savigny’s doctrine, usually founded such co-ordination on the location of the legal relationship based on a central aspect of the legal situation. It goes without saying that where electronic media are involved, that location is more difficult to
establish, “cybercrime being characterised by a sort of passive, generalised internationalisation” (2).

Faced with these new challenges, private international law – which is still under construction on both a French and a European level – has strived to develop solutions adapted to this new social and technological situation. From a methodological point of view, these solutions do not appear to be revolutionary in any sense. They are simply the result of a modernisation of traditional rules of private international law – a modernisation most often brought about by case law acting in accordance with the function naturally attributed to it. Moreover, this proves, in some sense, the timelessness and continuity (so often disputed) of the abstract logic of co-ordinating national legal systems as conceived by Savigny.

As regards invasions of privacy via the internet, this modernisation concerns the rules establishing the international jurisdiction of French courts (section I) and those serving to identify the applicable law (section II).

I – The jurisdiction of the French courts to hear cases involving invasions of privacy via the internet

In the event of an international invasion of privacy, the first question to be asked from the French point of view is naturally that of the jurisdiction of French courts to hear the case. Indeed, the international nature of the legal situation leaves room for doubt as to the relevance of the French court’s involvement.

Are the links between the French legal system and the legal relationship in question sufficient to justify the jurisdiction of the French courts? Do the twin objectives of the proper administration of justice and access to a judge militate in favour of the French legal system taking charge of and deciding the case?

These are issues which, in the French legal system, could not be left to a judge’s discretion. This is why international jurisdiction is governed by relatively precise rules which strive to delineate the field of intervention open to national courts. These essentially national rules could only, for reasons linked to State sovereignty, determine the jurisdiction of French courts within the international legal order.

This co-ordination was previously far from perfect. Indeed, as each State unilaterally established the jurisdiction wielded by its courts, there were frequent positive and negative conflicts. We cannot help but acknowledge the progress made by the European Union which, as soon as it was competent to do so, strove to streamline the various alternatives available by unifying the rules of direct jurisdiction between Member States.

Nowadays, the European rules are close to supplanting national solutions. The fact remains, however, that in cases of invasion of privacy, the application of European solutions is subject to the condition that the defendant’s domiciled be located on the territory of the European Union. Thus, where the defendant is domiciled outside the Union, the French court must no longer accept or decline jurisdiction on the basis of the European rules (section A) but rather on that of the French rules of direct jurisdiction (section B).
A – The court’s jurisdiction based on European rules of direct jurisdiction

Firstly, Article 4.1 of the Brussels I (recast) Regulation (3) states that a person may be sued by a claimant before the courts of the Member State in which said claimant is domiciled. This provision is general in scope and applies to all cases, with the exception of those for which exclusive jurisdiction is provided by the Regulation. The result is that, in cases of invasion of privacy via the internet, French courts will accept jurisdiction when the defendant is domiciled in France.

Next, with the aim of facilitating access to justice, Article 7 of the Regulation allows the claimant to sue before a court in a Member State other than that in which the defendant is domiciled. This choice of court varies depending on the subject of the dispute.

In order to identify the relevant provision of Article 7, invasions of privacy committed via the internet must therefore be qualified. As this involves European legislation, the qualification must be made independently, i.e. in light of European law and without reference to concepts under national.

The European Court of Justice considers that infringements of personality rights belong without the slightest doubt to the law of tort, delict and quasi-delict. Indeed, the Court has a very broad conception of that area, which it defines negatively as “all actions which seek to establish the liability of a defendant and which are not related to a ‘contract’” (4). Consequently, in order to see whether the French courts can accept jurisdiction even when the defendant is domiciled outside France, we must refer to Article 7.2. Pursuant to that provision, the claimant can bring an action before “in the courts for the place where the harmful event occurred or may occur”. As a result, French courts may also accept jurisdiction on the basis of the Regulation where the invasion of privacy has taken place on French territory and even where the defendant is domiciled in another Member State of the European Union.

The application of the above provision has raised three types of difficulty owing to the ambiguity of the expression “harmful event”.

Firstly, there are many scenarios in which the event that caused the harm and the damage did not take place in the same legal order. There is, in many cases, a dislocation between the different elements of the tort. Does the expression “harmful event” refer to the event that caused the damage or the actual damage suffered by the victim? The Court of Justice was quick to take up the difficulty of so-called “complex torts”, stating in a landmark decision that the expression “place where the harmful event occurred or may occur” must be understood as being intended to cover both the place where the damage occurred and the place of the event giving rise to it” (5). In other words, as regards complex torts the victim may, on the basis of Article 7.2, choose to bring an action before the courts of the Member State in which the harmful event took place or those of the Member State in which the damage occurred.

Thus, in application of that section of the Regulation, the French courts will also be able to accept jurisdiction where the event giving rise to the infringement occurs in France or where the damage has been suffered by a victim on French territory.

Secondly, the same event – and all the more so where it concerns an invasion of privacy via the internet – is likely to cause damage in various States.
In such a scenario, on the basis of Article 7.1 as interpreted by the Court of Justice, can the victim bring an action before any court of a Member State on the territory of which a part of the dispute has taken place or, on the contrary, must the victim focus on bringing their action before the courts of the Member State where the main part of the damage has been suffered?

The Court of Justice answered the question by stating that the victim could sue the person responsible for the invasion of privacy before all Member States on the territory of which part of the damage has been suffered (6). It did, however, stipulate in the same judgment that while the courts of the place where the harmful event occurred or those of the defendant’s domicile had jurisdiction to hear the full application for compensation, those of each Member State in which damage had been suffered could only, for their part, order compensation in respect of damage caused in the territory of their respective State. Thus, where the victim decides (most often for reasons of expediency) not to bring an action before the courts of the State where the defendant is domiciled (Article 4.1) or those of the place where the harmful event occurred (first branch of the option granted by the *Mines de Potasse* decision on the basis of Article 7.2), they will be forced to split their claim between each of the courts in the various places where the damage occurred.

Lastly, regarding invasions of privacy via the internet more specifically, a difficulty emerges as to the location of the various elements of the tort. Where did the harmful event take place? Where is the damage located?

The answer to those questions assumes above all else that what is understood by “event giving rise to the damage” and “damage” has already been determined in scenarios involving invasions of privacy via the internet. If, as is shown by the various European positive laws, several conceptions can be considered, the Court of Justice at least gave a clear decision in this issue. It stated that the place of the causal event had to be understood as being that of the publication or disclosure of the information at issue whereas the damage was located in the place where said information was disseminated (7).

As a result, in a scenario involving the dislocation of the elements of the tort, delict or quasi-delict, the French court will have jurisdiction on the basis of Article 7.2 of the Regulation if the information was disclosed (event giving rise to the damage) or broadcast (damage) in France.

This case law, which was developed for infringements of personality rights in general, then had to be adapted to the more specific scenario of invasions of privacy via the internet. In such a setting, the place of the event giving rise to the damage can easily be equated with the place where the website is hosted as the place where the information at issue was communicated.

Conversely, identifying the location of the damage poses greater difficulties. Indeed, in the case of electronic media, the broadcasting or disclosure criterion loses its relevance. It simply means that any European court can have jurisdiction to hear the case, the offensive information being disseminated on the internet being, by its very nature, accessible all over the world. However, despite that line of argument, the Court of Justice has taken the view that the accessibility of the site at issue in a given State suffices to give its courts jurisdiction (8). The Court was not receptive to the theory of “focalization” identified by the American courts (9). However, the ECJ did add that the victim could also bring an action before the courts of the Member State in which the victim
habitually resided, those courts having jurisdiction to order compensation for all the damage suffered (10).

In summary, where European law is applicable owing to the defendant being domiciled within the territory of the European Union, a French court can accept jurisdiction in accordance with various criteria. On the one hand, it would have jurisdiction to hear the case in its entirety if the defendant is domiciled in France, if the information at issue has been communicated from France or where the victim is habitually resident in France. On the other hand, the court will also have jurisdiction to order compensation solely for damage suffered in French territory where the website at issue can be accessed in France, which will almost systematically be the case.

Where the defendant is not domiciled within European territory, the French courts must assess their jurisdiction in light of French rules of direct jurisdiction.

B - The jurisdiction of French courts based on French rules of direct jurisdiction
Since the well-known decisions in Pelassa (11) and Sheffel (12), it is established that the international jurisdiction of French courts is determined by the extension of the rules of territorial jurisdiction contained in the Code de procédure civile (Civil Procedure Code).

Given the qualification of invasions of privacy via the internet as torts, delicts or quasi-delicts (13), two provisions are likely to form the basis of the jurisdiction exercised by French courts: Article 42 and Article 46 paragraph 2 of the Civil Procedure Code.

There is no need to go over those articles, which reiterate the criteria relating to domicile (Article 42) and the place where the harmful event occurred (Article 46 para. 2) previously discussed in the context of European law. It must also be noted that as regards the application of the legislation, French case law has adopted the same interpretations overall as the European Court of Justice, particularly as regards the scenario of complex torts that is so frequently encountered.

The particularity of French law on direct jurisdiction is even more apparent in Articles 14 and 15 of the Civil Code. By virtue of these exemptions from jurisdiction, French courts have the subsidiary possibility of accepting jurisdiction where the claimant (Article 14) or the defendant (Article 15) is a French national.

The criteria for the jurisdiction of French courts having been detailed, there now remains the task of establishing which law will apply to invasions of privacy via the internet.

II - The law applicable to invasions of privacy via the internet
In the absence of any applicable European legislation (14) or specific rule on conflicts of laws, the law applicable must be identified by means of the traditional mechanisms found in private international law. In other words, invasions of privacy via the internet should first be classified in order to include these questions in a connecting category provided by private international law (section A). Secondly, in order to identify the law applicable, it will simply be a matter of applying the connecting factor allocated to the “go-to” of invasions of privacy via the internet (section B).
A – Classifying invasions of privacy via the internet

In private international law, the classification of invasions of privacy has been the subject of significant doctrinal discussion. Indeed, the debate in national law relative to the existence of personality rights as independent subjective rights quickly extended to the international legal order.

Once it is accepted that the right to respect for private life exists independently of any violations thereof, the tortious classification loses its relevance and other connecting categories can be considered.

Firstly, invasions of privacy could, from a conceptual point of view, come under the personal status category defined as “rules, taken as a whole, that govern the civil status of individuals and the non-proprietary relations that they form” (15). It is true that personality rights are, generally speaking, dissociable from persons and contribute to defining their status by establishing their legal status with respect to the law (16).

Next, in view of the expansion of the patrimonialization of personality attributes, some authors have put forward a classification of personality rights based on actual status. We cannot fail to note that personality rights secure non-proprietary and proprietary prerogatives for the holder of such rights; prerogatives which consist in a monopoly over the exploitation of some aspects of an individual’s personality.

Despite these proposals, which can lay claim to strong conceptual arguments, French case law has stuck to the tortious classification traditionally applied in this area (17).

The reason for this attachment to the tortious classification – and this in spite of the emergence of independent subjective rights – is quite certainly due to the eminently functional, contingent nature of the classification process in private international law (18). It is not a matter of simply classifying the legal relationship in the appropriate category depending on its legal character. The ultimate purpose of the operation is to infer an appropriate, relevant connection in light of the interests at play.

As regards invasions of privacy, neither the application of national law (19) nor that of the location of property (20) appears satisfactory. This is undoubtedly why the tortious classification has been retained in spite of the ambiguous legal character of instances of invasions of privacy via the internet.

B – Implementing the corresponding connection

The tortious classification of invasions of privacy entails the application of the law relating to “the place where the tort, delict or quasi delict occurred” (21). Being easy to use when all the elements of the tort are located within a single national legal system, this connecting factor can prove more difficult to implement in cases of dislocation between the harmful event and the damage. As regards invasions of privacy via the internet, such a dislocation will be relatively common, the harmful event being the disclosure of the information at issue and the damage its dissemination.

Generally, for scenarios involving complex torts, the Court of Cassation has enshrined the equal purpose of the law on the harmful event and that on damage (22). Furthermore, after setting down
that principle, the Court stated that between those two laws, a choice had to be made as to which was most closely related to the case in question (23).

In cases involving invasions of privacy via the internet, this arbitration aspect of the proximity principle ought to have led a court to choose, on a case by case basis, between the law on the disclosure of the information at issue and that on the location of its disclosure.

Nevertheless, the Court of Cassation slightly amended the terms of the option by qualifying the dissemination of the harmful event giving rise to the damage (24). By examining the act of disclosing the information in this way, it tends to deny the potentially complex nature of invasions of privacy via the internet. Indeed, the two components of the tort – damage and harmful event – are consequently located in the same place.

This single connection to the place where the information at issue is disclosed thus contradicts the definition of the place where the harmful event occurred as set down by the Court of Justice in matters of direct jurisdiction (25). Moreover, it carries with it the downside of resulting in the application of several laws when the information is disclosed in several States, which is almost systematically the case when dealing with invasions of privacy via the internet. In such scenarios, it must therefore be considered that there are as many separate torts as there are disseminations, the legal consequences of each being subject to the laws of the country in which it arose.

Notes:
(4) CJEC, Case 189/87 *Athanasios Kalfelis v Bankhaus Schröder, Münchmeyer, Hengst and Co. and others* [1988] ECR 05565; and CJEC, Case C–51/97 *Réunion européenne SA and Others v Spliethoff’s Bevrachtingskantoor BV and the Master of the vessel Alblasgracht V002* [1998] ECR I–06511
(5) CJEC, Case 21–76 *Handelskwekerij G. J. Bier BV v Mines de potasse d’Alsace SA* [1976] ECR 01735
(7) Ibid.
(8) CJEU, Joined Cases C–509/09 and C–161/10 *eDate v X and Case Olivier & Robert Martinez v MGN Limited*, [2011] ECR I–10269. Jurisdiction is then based on the place where part of the damage occurred.
(9) By virtue of this theory, the mere accessibility of a site does not constitute sufficient grounds to justify the application of a law or the bringing of an action before a court. Other objective elements must serve in considering that the site content was consciously directed at this or that State which, on that basis, can claim jurisdiction or the application of its national law.
(10) Judgment cited above.

(13) See infra.

(14) For the time being, the rules on conflicts of laws have not been subject to unification on a European Union level. Indeed, in spite of a willingness in that sense, no consensus could be reached between Member States, in such a way that situations involving personality rights were ultimately excluded from Regulation n° 864/2007 of 11 July 2007, known as “Rome II”, on the law applicable to non-contractual obligations. The European Parliament adopted a Resolution on 10 May 2012 containing recommendations to the Commission on the amendment of the “Rome II” Regulation. The EP asked the Commission to submit two proposals aiming to add provisions to Rome II, concerning:

– a proposal designed to add to the Rome II Regulation a provision to govern the law applicable to a non-contractual obligation arising out of violations of privacy and rights relating to personality, including defamation;

– a proposal for the creation of a centre for the voluntary settlement of cross-border disputes arising out of violations of privacy and rights relating to personality, including defamation, by way of alternative dispute resolution”.

(15) M.-L. Niboyet et G. de Geouffre de la Pradelle, Droit international privé, LGDJ, 4ème éd. 2013, n° 5.


(19) In a number of scenarios, applying national law would result in an extra-territorial application of law which would not fail to surprise third parties. Indeed, the protection of personality generally operates by striking a balance between the interests at stake and, on that basis, is part of a given social context. Third parties quite legitimately expect the application of laws that usually govern the social setting in which they exercise their activities and find it difficult to understand that the protection of personality, which delineates the limits of some of their freedoms, can fluctuate depending on the nationality of the persons concerned.

(20) See P. Bourel, « Du rattachement de quelques délits spéciaux en droit international privé », cited above, n° 58: "while the concept of property points towards a well-defined category, namely the actual status, it does however leave untouched the issue of connection. The non-material nature of the subject-matter of the right (name, image, etc.) does not allow the effective location of the property in space to be used (...)".


(25) See supra.
Reconciling transparency in public life and respect for private life appears to be the objective pursued by the French laws of 11 October 2013 on transparency in public life, at the very least in their provisions relating to the duty to declare interests and assets imposed on individuals in public office or in charge of a public service mission.

The distinction between public and private life is the result of a liberal conception of political society: the Declaration of the Rights of Man and of the Citizen of 26 August 1789 (DRMC) establishes the separation of person (private life) and function (public life). In that sense, the French Revolution, which was intended to be democratic and liberal, was set against a monarchical Ancien Régime in which “private” and “public” matters were, in a “court society”, intimately linked and both symbolised in the person of the King, who was both a public and a private figure. Political liberalism in the French information society reaffirms the distinction by strengthening it. Furthermore, the Proclamation of the Republic in 1792 was based on an initiative to bring transparency to the management of public affairs, which contrasted with the often opaque nature of the financial management of the “King’s Household” under the Ancien Régime. It is, moreover, financial issues that appear to be at the root of European democratic revolutions. In that sense, in the words of one author, “democracy is a lie if it does not tackle the issue of money head-on” (2).

We can therefore understand the heightened tension that may be found within democratic societies between transparency in public life (public money calls for transparency) and respect for private life (public officials’ private funds may not be kept completely secret).

The issue of transparency in public life recently re-emerged following the “political shockwaves” of the Cahuzac affair, named after the deputy minister in charge of the Budget charged by an examining magistrate on 2 April 2013 with laundering the proceeds of tax evasion. The organic and ordinary Laws of 11 October 2013 on transparency in political life, known as the lois Cahuzac (Cahuzac laws) (3) appear to result, in addition to the report submitted by the Parliamentary committee that investigated the matter (4), from earlier work done by both the commission de réflexion pour la prévention des conflits d’intérêts dans la vie publique (Commission for the Prevention of Conflicts of Interest in Public Life), chaired in 2010 by the Vice-President of the Conseil d’Etat, Jean Marc Sauvé; and by the commission de renouvellement et de déontologie de la vie publique (Commission for Renewal and Ethics in Public Life), chaired in 2012 by the former Prime Minister, Lionel Jospin. Faced with the “crisis of confidence” currently experienced by French democracy, the former commission seeks to prevent or regulate conflicts of interest, in particular between public and private interests (5); while the latter seeks to start working on “a renewal of public life”, in particular by publishing the asset declarations made by elected representatives (6).
Both commissions thus affirm the need for a set of ethics governing the responsibility of political staff through the duty to declare interests and assets, particularly for Members of Parliament and ministers. A comparative approach shows that these democratic requirements for the prevention of conflicts of interest and the declaration of assets are framed by laws that vary in terms of their scope in order to protect the right to respect for private life: thus, common law, which so often serves as a model in instituting such measures, enshrines a scheme established on the basis of laws (Canada’s Conflict of Interest Act 2006) or simple codes of ethics (in the United Kingdom, the Ministerial Code issued in 2012 by the Prime Minister and the Civil Service management code issued on the basis of a 1995 ministerial decision) (7).

The aim of the “lois Cahuzac” is above all to re-establish ties between political power and citizens and thus strengthen the legitimacy of governors in the eyes of the governed; the Cahuzac laws have been heavily criticised particularly by the current Speaker of the French National Assembly, who decried the creation by those laws of a “paparazzi democracy” (8); they appear, in any event, to mark a new era in French democracy. Taxpaying citizens do indeed demand transparency in public life and greater responsibility on the part of political figures and their associates. These laws thus appear to incorporate the common-law concept of accountability, in the sense here of transparency in activities and the responsibility of public players. The organic and ordinary Laws of 11 October 2013 thus render more than eight thousand elected and unelected officials subject to a duty to declare assets and interests. While the content of the provisions under those Laws is quite ambitious, their scope however seems quite limited.

I. Ambitious provisions
The provisions under the Cahuzac laws relative to declarations of assets and interests attract attention as they are likely to infringe the right to respect for private life.

1. The declaration of assets
The organic law defines the duties incumbent on Members of Parliament in this area, and is supported by an ordinary law which stipulates the duties falling to members of the Government, local elected officials and any other person entrusted with a public service mission.

The following are thus subject to a duty to declare assets: members of ministerial offices; associates of the President of the Republic; the Speakers of the National Assembly and the Senate; Members of Parliament, Senators and French Members of the European Parliament; presidents of the conseils départementaux et régionaux (departmental and regional Councils); local mayors and presidents of Etablissements Publics de Coopération Intercommunale (EPCIs) with their own taxation of more than 20,000 inhabitants; the president of the Metropolis of Lyon; members of independent administrative and public authorities (known as AAls and APIs); the chief executive officers of companies, the share capital of which is held by a majority of public persons. The declaration concerns only the assets and property (9) of the office holder and not those of their spouse, civil partner or cohabitee (the professional or business activity of these persons must, however, also be declared); community property is also included. This declaration, which must be exhaustive, honest and certified on the office holder’s honour, is made within two months following their entry into service or from the date of their appointment, and filed with the Haute autorité de transparence de la vie publique (HATVP – High Authority for transparency in public life). The latter organisation publishes the asset declarations made by members of the Government. The declarations submitted by Members of Parliament may only be consulted at
prefectures and only by registered voters. The disclosure of information contained in such asset
declarations, which may only be consulted (Members of Parliament) and those not made public by
the HATPV (members of the Government), constitutes a criminal offence punishable by a year’s
imprisonment and a fine of up to €45,000 unless the declarant has himself made the details of his
declaration public. In order to protect privacy of an elected representative or a member of the
Government, certain details are not made public (e.g. personal address, names of
spouse/partner/cohabitee and other members of the family, the exact location of properties, etc.)
(10). Such criminal provisions are used to sanction any invasion of privacy, within the meaning of
Article 226–1 of the Code pénal (Penal Code).

2. The declaration of interests
When they were tabled before Parliament, the draft organic and ordinary Laws on transparency in
public life, having identified the limits of the current law on declarations of interests, envisioned a
complete overhaul of the scheme “with the aim of placing our country amongst the most advanced
democracies in matters of preventing conflicts of interest, and using the principle of transparency
in the service of that objective” (11). Under the terms of Article 1 of the ordinary Law, “shall
constitute a conflict of interest any situation of interference between a public interest and public
or private interests which is of such a nature as to influence or appear to influence the
independent, impartial and objective exercise of a function”. This objective definition of conflicts
of interest has the merit of going beyond the concept in criminal law of “prise illégale d’intérêt”
(illegal acquisitions of interest) under Article 432–12 of the Penal Code. Thus a conflict of interest
may be established on the basis of an apparently legitimate situation in the sense of the due
process of law; the person concerned is then subject to a duty to abstain (“system of deposit”),
which duty must consequently be supplemented in accordance with the rules of the body in
question (12). The person (be they elected or unelected) facing a conflict of interest then abstains
from being a member of the body and/or using their delegation of signing authority. This
concerns national and European parliamentarians, members of the Government and local elected
representatives, as well as members of ministerial offices, associates of the State’s highest
authorities (President of the Republic, Speakers of the National Assembly and the Senate), and
members of AAIs and APIs. The HATVP only makes public those declarations of interests submitted
by persons in elected and ministerial office. The declarations may only be consulted at prefectures
and only by registered voters.

In matters of the prevention of conflicts of interest, Members of Parliament and Senators are
forbidden from exercising an advisory role or roles within companies that maintain close ties with
the administration (Article 2 of the organic law). The law also provides for a reduction in the
duration of indemnity payments to made to ministers in the event that they do not resume any
paid activity (which indemnity is not paid in the event of a failure on the part of the interested part
to fulfil their duty to submit declarations of interests to the HATVP, as provided under Article 3). In
order to prevent certain conflicts of interest, the laws have toughened the incompatibility rules
applicable to Members of Parliament and of the Conseil constitutionnel (Constitutional Council). In
two decisions, the latter stated, even slightly amended, the effective scope of the provisions of the
two laws discussed above.
II. Provisions limited in scope
The decisions of the Constitutional Council stipulate the scope of the Cahuzac laws and thus establish the field of competence of the body responsible for monitoring the observance thereof: the HATVP.

1. Normative scope
In two decisions (13), the Council approved the two laws, with the exception of several provisions which were declared unconstitutional and certain interpretative reservations.

On the basis of the right to respect for private life guaranteed by Article 2 of the DRMC (14) of 1789 and enshrined in its earlier case law (15), the Council recalled that “the freedom proclaimed under that Article implies the right to respect for private life; that the submission of declarations of interest and asset declarations containing data of a personal nature pertaining to private life, together with the publicity to which such declarations may be subject infringe the right to privacy; that, in order to be constitutional, such infringements must be justified on ground of public interest and adequately implemented in proportion to that objective” (16). Thus, by an interpretative reservation, the Council restricted the scope of the duties to declare the professional or business activities of “parents and children” or of “other members of the family” of a parliamentarian (17) and the holders of certain functions or public posts (18). Furthermore, it struck down a large section of Article 12 II of the ordinary law which provided the possibility for voters to consult, at prefectures, those asset declarations submitted by their local elected representatives, taking the view that there lay a disproportionate infringement of the right to respect for private life in light of the transparency objective pursued by the legislature (19). Moreover, the declarations of interests submitted by officials who do not hold political office but rather an administrative role cannot be made public (20).

These reservations as to the interpretation or striking down of legislation ultimately have the effect of providing a stronger framework for the status and powers of the institution established to monitor the observance of the Cahuzac laws, the HATVP. The latter body had been granted a power of injunction by the legislature, the scope of which was restricted by the Council with regard to parliamentarians (21) and associates of the Speakers of the National Assembly and the Senate (22), and this on the basis of the principle of the separation of powers. The Council’s decisions thus have a not inconsiderable institutional scope.

2. Institutional scope
The Law of 11 October 2013 abolished the Commission pour la transparence financière de la vie politique (Commission for financial transparency in political life), formerly established by the Law of 11 March 1988 on financial transparency in political life, replacing it with the High Authority for Transparency in Public Life (HATVP), which has greater powers relating to supervision and sanctions). As an autorité administrative indépendante or AAI (independent administrative authority), on which basis its members are subject to the duty to declare assets and interests (23), the HATVP is composed of nine members, the chairman being appointed by the Head of State while the remaining eight are nominated by the courts (Conseil d’Etat, Cour de cassation (Court of Cassation) and the Cour des comptes (Court of Auditors)) and parliamentarians (Speakers of the Senate of National Assembly) (24). Its budget, however, remains part of the “Direction de l’action du gouvernement” (Government Action Directorate), which qualifies its financial independence and, consequently, its true independence with regard to the executive branch.
The HATVP is responsible for receiving declarations of assets and interests, particularly in electronic format (25), at the beginning and end of the term of office of a number of public figures, particularly members of the Government, national and European parliamentarians, local elected representatives, members of ministerial offices and associates of the President of the Republic (26). Any change in assets during the term of office or while exercising a function must be declared within two months for Members of Parliament or one month for other relevant persons. An incomplete or dishonest declaration is punishable by a prison sentence of three months and up to €45,000 in fines (27) (five years’ imprisonment and a €75,000 fine for members of the Government). Failure to fulfil the obligation to provide such information carries with it the sale criminal sanctions and also disqualification. The HATVP may rule on matters referred to it by the Prime Minister, the Speakers of the National Assembly and the Senate, and by accredited anti-corruption groups (“Regards citoyens”, “Anticor”, “Transparency International France”); it may also investigate on its own initiative where it finds failures and inform the relevant authorities of the same. “It publishes an annual report, which is submitted to the President, the Prime Minister and Parliament, and may formulate recommendations for the application of legislations, particularly in matters of relations with interest representatives (28).

The HATVP’s activity can be seen in a number of recent cases handed over to the parquet national financier (PNF – Financial State Prosecutor), established in 2013 and specialising in combating major financial crime (for cases of failure or omission to declare assets in relation to parliamentarians and members of the Government), cases that are often expedited with the help and support of the tax authorities, with which the HATVP has very close ties.

In 2013, taking inspiration from the common-law concept of accountability, the legislature appeared to assume that; in the absence of effective liability, it was more a question of promoting a simple code of ethics for those in power (29), thus reflecting the law’s limitations where it is a matter of providing a framework for and sanctioning the status and role of government representatives and their associates (30). It is also to be noted that it is in the name of the right to respect for private life that the decisions handed down by the Constitutional Council restrict the scope of the 2013 laws – and, consequently, the effectiveness of the HATVP’s activities. The right to respect for private life is precisely defined by legislation and case law, unlike the concept of transparency in public life. Only practice and the implementation of oversight and sanction procedures will reflect the effectiveness – and, therefore, the substantive value – of having established the HATVP.

Notes:
(2) A. Etchegoyen, La démocratie malade du mensonge, éd. François Bourin, 1993, p. 161
(4) Rapport n°1408 des députés M. Ch. de Courson (Président) et M. A. Claes (Rapporteur) fait au nom de la commission d’enquête relative aux éventuels dysfonctionnements dans l’action du Gouvernement et des services de l’État, notamment ceux des ministères de l’économie et des
finances, de l’intérieur et de la justice, entre le 4 décembre 2012 et le 2 avril 2013, dans la gestion d’une affaire qui a conduit à la démission d’un membre du Gouvernement, Assemblée nationale, 8 octobre 2013, p.96.


(7) Ministerial code, Cabinet Office, 21 May 2010, 30 p; Civil service management code, 88 p.

(8) Note from the Speaker of the National Assembly to the Prime Minister and published by Le Monde on 11 April 2013.

(9) Particularly, property (built or not built), securities, bank accounts, life insurance, land vehicles, boats, aeroplanes, etc; Décret du 23 décembre 2013 relatif aux déclarations de situation patrimoniale et déclarations d’intérêts adressées à la Haute Autorité pour la transparence de la vie publique (Decree of 23 December 2013 on asset declarations and declarations of interest submitted to the High Authority for Transparency in Public Life), JORF of 27 December 2013.


(14) Which provides "The aim of all political association is the preservation of the natural and imprescriptible rights of man. These rights are liberty, property, security, and resistance to oppression".


(16) Recital 13 of Decision n° 2013–676 DC

(17) Recital 29 of Decision n° 2013–675 DC

(18) Recital 16 of Decision n° 2013–676 DC

(19) Recital 20 of Decision n° 2013–676 DC

(20) Recital 22 of Decision n° 2013–676 DC

(21) Recital 39 of Decision n° 2013–675 DC

(22) Recital 45 of Decision n° 2013–676 DC

(23) Article 3 of the High Authority’s general regulations, declarations addressed to the President of the HATVP.


(26) Décret n° 2013-1212 du 23 décembre 2013 relatif aux déclarations de situation patrimoniale et déclarations d'intérêts adressées à la Haute Autorité pour la transparence de la vie publique (Decree n° 2013-1212 of 23 December 2013 on asset declarations and declarations of interest submitted to the High Authority for Transparency in Public Life), JORF n°0300 of 27 December 2013 page 21445

(27) Article LO 135-1 of the Electoral Code (parliamentarians), Article 26 I of the ordinary law of 11 October 2013 (members of the government and local elected representatives).

(28) HATVP website

(29) Hence the Charte de l'élu local (Charter for local elected representatives), enacted by Law n° 2015-366 of 31 March 2015 visant à faciliter l'exercice, par les élus locaux, de leur mandat (on facilitating the fulfilment of mandates by local elected representatives), JORF n°0077 of 1 April 2015 page 5921; and Charte de déontologie des collaborateurs du Président de la République (Ethical Charter for Associates of the President of the Republic), 19 December 2014.

(30) In this sense, see J. L Nadal (President of the HATVP), Renouer la confiance publique, Rapport au Président de la République sur l'exemplarité des responsables publics, LDF, Paris, January 2015, 192p.
Like the right to respect for private life, image rights originate in the individualist values brought about by the liberal revolutions of the 19th century. Judges immediately introduced them into positive law as a bulwark to protect the person, contributing to guaranteeing a sphere safeguarded against external intrusions in order to foster individual fulfilment. While image rights have rapidly prospered in French case law, so have new techniques. Since the end of the 19th century, the development of photography, combined with the liberalisation of publishing – and particularly the press – has fuelled an abundance of litigation. Moreover, it is significant that the decision marking the emergence of image rights in France concerns a photograph (of the actress Rachel on her deathbed) that was reproduced and retouched despite the formal refusal of the surviving family, a copy of which was acquired in particular by L’illustration.

The boom in the means of audio–visual communication in the 20th century allowed the “massification” of information and, as a corollary, awarded a central role to images. These developments emphasised the variety of issues raised since the 19th century by the rights held by individuals over their representation, without making any tangible changes to the substance thereof. Nevertheless, this product of case law was only very gradually been shaped by judges. Case by case, they drew a number of outlines, rejecting its absolute nature. However, in the absence of any legal enshrinement and in the face of a divided doctrine, French case law remained heterogeneous. It was only in 1998 that the Court of Cassation genuinely affirmed Article 9 of the Civil Code as the basis of image rights. Having thus become an attribute of personality, images officially gained independence two years later, as the subject of a fully-fledged subjective right. Lastly, owing to its unavailability, the relevant time limit was only definitively set with the demise of the de cujus principle in 2005.

While image rights entered the new millennium under the best auspices, they find themselves in critical condition a good ten years on. Their deterioration in related to their atrophy (section I) but also to their own development, expressing shifts as to their very essence (section II).

I – Atrophy
The dwindling scope of image rights is the result of an expansion of other rights that either circumvent (section A) or compete (section B) with it.

A – The delegitimization of the monopoly over one’s image
A person’s right to control their representation is now heavily circumscribed by transparency and truth requirements that structure freedom of expression on the one hand, and the law of evidence on the other.
While the former has long covered the public’s right to be informed, its interpretation in that sense has been palpably extended over the last decade to the detriment of image rights, nonetheless recognised as an aspect of Article 8 of the European Convention on Human Rights (ECHR) (8).

Firstly, on the basis of that right, current events and public interest debates have, as with privacy, become justifications for infringements of image rights. Through a comprehensive interpretation thereof, the Court of Cassation took a benevolent view of the use of images as illustrations (9). Its informational value was no longer assessed as such but rather in light of the connection with the illustrated statements (10), which also serves to justify images captured without the knowledge of the interested party, unless however that the representation of said party violates human dignity or is offensive. Lastly; the same rules apply to the dissemination of the image, authorised for specific purposes or subject to particular conditions; these restrictions do not infringe the right to information (11).

Next, the egalitarian conception of image rights – long set down in principle by the Court of Cassation (12) despite some hesitation due to hostility on the part of trial judges – is no longer relevant as regards the right to information. The decisive influence on this change of direction in linked to ECHR developments, once classing a princess as a “private’ individual” despite her fame (13), and now as a “public figure”, “who [is] undeniably very well known” (14). Celebrities can no longer “claim protection in the same way […] as private individuals unknown to the public” (15), the balance between their rights and freedom of expression being based on specific criteria (16). In that vein, the Court of Cassation accepted, for instance, a person’s fame “owing to their respective family relations” and dismissed the unlawful invasion of their privacy as a violation of their image rights (17). Ten years earlier, the Court considered that such infringements were characterised by the “sole purpose of relating”, with supporting photos, a celebrity’s attendance at a highly-publicised demonstration as it was “in a private capacity” and “unrelated to her professional activity”, the media company not having, moreover, proved that the star “had lent her support to the cause” (18). Henceforth, it is for the interested party to establish “relevant indications” or “particular circumstances” in order to prove that their image had been captured, not without their knowledge, but secretly or in unfavourable conditions (19).

Interpreted in light of the right to a fair trial (Article 6, ECHR), “the right to evidence […] for the purposes of supporting one’s claims” (20) also contributes to “delegitimising” a person’s monopoly over their own image. Usually, it only prevails over the guarantees offered by Article 8 ECHR on the twofold condition that the item produced is necessary (21) to the defence’s needs and constitutes an infringement that is proportionate to the interests at stake. The first criterion has, however, very recently been overshadowed.

In French case law, two recent decisions involving cases of surveillance by an private detective mark this new direction. One accepts the lawfulness of such evidence against a policyholder, followed and filmed “on the public highway or in places open to the public” for the purposes of challenging an expert report. Without regard for those grounds denouncing disloyalty and the needlessness of such evidence, the Court of Cassation rejected the disproportionate nature of infringements “relative solely to the mobility and independence of” the insured person “in light of the necessary and legitimate protection of the rights of the insurers and the interests of policyholders as a whole” (22). The second decision draws a similar conclusion concerning a dispute as to eye damage, observations made “from the public highway” covering only “the
absence of spectacles when driving a vehicle or when cleaning and tidying a balcony” (23). The infringement of image rights was also rejected on the basis of the sovereign statement made by the trial judges that the poor quality of the photographs made it impossible to identify the person. Does such a failure not constitute grounds for ruling that such evidence is inadmissible?

These solutions are all the more surprising when we consider that the fact of “voluntarily invading another person’s privacy […] by viewing, recording or transmitting, without (their) consent” “the image of a person in a private place” is a criminal offence (24). However, the position detailed above is not an isolated incident. In similar cases, the Swiss and Spanish courts in particular have taken an identical approach, approved by the ECHR. The latter accepts, for example, that insofar as a claim for compensation made by a policyholder is based on his disability, “the public interest of guaranteeing a fair trial for all litigants” requires “that any evidence to the contrary be put before the court” (25).

Gone is the requirement that, in order to be admissible, evidential methods that violate personality are the only relevant ones. As to proportionality (now the sole evaluation criterion), this implies a genuine right to private surveillance which includes images, with the right to a fair trial justifying the production of the results thereof where these are intended to support a litigant’s claims. Image evidence being admissible even where there are no allegations of fraud on the part of the person featuring in said image(s), the main question remains as to the possibility of capturing their image in a private place. France has already shown herself in favour where such an operation is carried out from a public place or a location that is open to the public.

B – Marginalising the control over one’s image
The boom in digital technology, and especially Web 2.0, has multiplied the ways in which a person may be exhibited, even carrying with it an unspoken injunction to display oneself on the Web. Social media, and search engines in particular, also encourage the mass dissemination of information, images particularly. The protection thereof, where the individual represented can be recognised, finds itself increasingly within the scope of those rules relating to personal data (26). While the latter appear to be more favourable to an improved control over information making a person recognisable, the scheme that those rules institute contribute in reality to weakened protection for images.

Subject as it is to a fundamental right to protection (27), personal data enjoy significant guarantees in Europe. Under Directive 95/46, data collection supposes “specified, explicit and legitimate purposes” in light of which the requirement as to the relevance and non-excessive nature of the data concerned is to be assessed (Article 6). The Directive also sets down strict conditions for data processing, an especially vast concept which extends to “any operation or set of operations which is performed on personal data, whether or not by automatic means” including their collection (Article 2). Among the six bases justifying such operations, the consent of the person concerned features as a principle, the others relating to situations in which data processing is “necessary”, under the terms of the Directive (Article 7). It must then correspond to imperatives (28), overriding interests (29) or even be required “for the purposes of the legitimate interests pursued by the controller or by the third party or third parties to whom the data are disclosed". This slightly enigmatic basis is nevertheless subject to the exception where “such interests are overridden by the interests for fundamental rights and freedoms of the data subject”. Nonetheless,
it seems destined to a flexible interpretation, as the ECJ has considered, in a cautious yet cryptic statement, that a search engine’s activities were “likely to fall within its scope” (30).

The well-known Google Spain decision which set down this solution offers an eloquent illustration of the way in which the law on personal data has marginalised the protection afforded to image rights. Firstly, by accepting that data collection on websites may be necessary to the legitimate interests of the search engine operator, the ECJ recognised a correlation between that basis for data processing and a company’s purpose. As a result, it undermined the principle condition, which is the consent of the interested party, potentially eliminating control over their image on the internet. Next, it considered that the possibility of obtaining the deletion of personal data displayed by a search engine did not imply the same option with regard to the publisher of a webpage. In this case, the storage of data in a newspaper’s internet archive, although over ten years old, appears to fall within the scope of the “solely for journalistic purposes” exception provided under Article 9 of the Directive. If this analysis were to be confirmed, the fate of images in the face of the right to information would again be altered online. Lastly, while the Court drew a right to be forgotten out of rights previously enshrined for individuals, it attached conditions that strengthened the essentially private framework in which those rights are to be exercised. The person concerned must assert his or her rights directly against the data controller. It therefore falls to the latter to decide on the merits of any such claims, in light of criteria that do not favour image protection.

The Court quite logically required that the compliance of data processing and its purpose(s) with the Directive be checked, but also that this be done in light of the time that has passed. While these checks leave room for a degree of subjectivity – especially with regard to photographs or videos – that is not the main problem.

The data controller must also examine whether their operations can “palpably affect the fundamental rights to respect for private life and the protection of personal data” without, for all that, any violation being necessary. It is nevertheless the “potential seriousness” of the interference that the data controller must establish, in order to weigh that up against the public interest in accessing the personal information at issue and their own economic interests. The margin of appreciation is all the greater as, while the Google Spain decision accepts the prevalence of the rights of the person concerned, on the one hand this is subject to “specific reasons, such as the part played by said person in public life” and, on the other hand, for a request on a search engine using a person’s name in this case. It is based in particular on the scope that such a tool confers to personal data, multiplying their visibility and accessibility in an aggregated, structured form, and furthermore concerning sensitive information here.

These reasons suffice to give an indirect insight into the difficulties encountered in controlling the reproduction and circulation of one’s image when faced with the power of data controllers. The seriousness of the intrusion into the fundamental rights of individuals, bearing in mind the growing banality of images on the internet, is only marginally accepted. Appeals to supervisory authorities, such as the CNIL in France, only stand to succeed in the circumstances established under European Union law.
II – Degeneration
Under the influence of the market for images and the development of communication technology, the purposes of image rights are undergoing change [section A]. Nonetheless, the usefulness of their primary purpose does not appear to be entirely destined for annihilation [section B].

A – Changes to the purposes of image rights
The fact that images are viewed as economic assets changes the nature of the law to which images are subject, even bringing about possible distinctions as to the ownership of the same. This then raises the issue of purpose.

While images have long been the subject of contracts covering their exploitation, the *summa divisio* between things and persons has been grounds for hesitation on the part of French judges on the marketing thereof up until quite recently. Josserand, who had already decried the “patrimonialisation” of persons in 1932, concluded that “we could be tempted to write that they are becoming Americanised” (31) The importation of a form of right of publicity, distinct from the right of privacy across the Atlantic owing to its commercial dimension, does not belie this nowadays. The Court of Cassation thus enshrined the commercialisation of image rights, bizarrely basing its decision on the “provisions of Article 9 of the Civil Code, solely applicable in matters of transfer (of that right)” and which, even more bizarrely, “fall within the scope of contractual freedom” (32). Pursuing that line of reasoning, the Court ruled on the sole basis of Article 1134 of the Civil Code that “the consent given by a person as to the dissemination of their image cannot be construed as consent to the disclosure of their name and rank” (33). The rigorous interpretation of intent here must not occlude the “contractualist” approach to image rights, without reference however to any transfer of rights whatsoever by the police officers who were the subject of the news report at issue in this particular case. The recognition of a right over an image, for which French doctrine had long hoped, is granted at the expense of a right to an image.

This shift towards contractualisation places agreements regarding images within a wider context of freedom of choice. Exploitation thus rests on what must be classed as consent. The Court of Cassation also went so far as to infer the possibility of granting “an exclusive right to use one’s image” (34) post mortem! If the person concerned must accept the commercial use of their image (35), they are then bound by their consent – at least according to the First Civil Chamber of the Court of Cassation. The Court rejected any inspiration that could be drawn from the rules framing the transfer of copyright in such cases, returning to the terms of the contract only. Thus, where a model has consented to the use of his or her image for specifically identified shots, the fact that consent does not circumscribe the duration, location or methods of use matters little (36). The same concept prevails as regards remuneration; there being no rules requiring that it be proportionate to revenue from its use, the lump sum set down in the contract is binding (37). The Second Civil Chamber of the Court of Cassation, however, has shown itself to be in favour of proportionate remuneration for models in addition to the lump-sum payment legally provided for their physical service. However, this interpretation of Article L.7123–6 of the Labour Code merely emphasises the availability of images and their implicit recognition by the French legislature (38).

Given the circumstances, are image rights intended to retain a moral dimension? If, aside from any connections the debates as to the public interest, it is only defensible through a contractual interpretation, it then loses any extra-pecuniary character and also becomes unequal. In that case, unknown individuals would have difficulty in claiming damage, unlike those persons who
habitually market their own image, with the exception of the public’s right to information. In spite of the growing commoditisation, images are not destined to lose all but their commercial protection, but rather face a change in their nature. Will this be by their re-entering the orbit of the right to respect for private life, under the cover of human dignity, or even as a tool for controlling reputation, the financial dimension of which would appear to be expanding? Before image rights are completely transformed into a means solely intended to protect interests other than those attached to the control of one’s own representation, a less resigned avenue may yet be explored.

B – Expectations as to the survival of image rights

The tide of defiance with regard to the Web, that both the French (39) and European (40) legislatures have sought to stem, raises questions as to the possible disappearance of (non-pecuniary) image rights. In this regard, consumer law techniques may contribute to their survival.

Firstly, it is class actions that open the way to such a scenario. While France finally inserted them into the Consumer Code (41), the relevant conditions nevertheless currently exclude any likelihood that a class action be deployed in defence of image rights. Such actions may in fact only be brought in respect of “the remedying of pecuniary damage resulting from material damage” (42). However, several national legislations are not as restrictive: an Austrian student who has become famous was thus able to bring a class action against Facebook’s data controller, located in Ireland, for the purposes of ensuring that the right to respect for personal data be respected. It was also this “power to initiate collective legal actions” that the European data protection authorities called for in a joint statement (43).

Secondly, the proposal for the European Data Protection Regulation provides another avenue, inspired by consumer law, to foster the protection of images of individuals. The initial draft of the Regulation provided that “a significant imbalance between the person concerned and the data controller” removed any effect from the former’s consent to the processing of their personal data. This audacious borrowing from regulations on unfair (contractual) terms was all the more remarkable given that the inequality here related not to rights and obligations but to individuals themselves. The taking into account of an imbalanced power relationship would have improved the protection afforded to individuals twice over. On the one hand, it would have strengthened the right to protection, which is currently more of a right to protect oneself by refusing beforehand to consent to the processing of one’s data and the exercise of individual rights thereafter. On the other hand, it could have moderated the hegemony of some online players who turn the acceptance of their general terms and conditions into a real Pandora’s box. By rejecting the value of consent in such cases, as well as allowing it to be withdrawn “at any time”, the proposal also went back over the “contractualist” conception of consent to data procession which prevails in practice, favoured by the use of the notion of consent in the relevant legislation.

However, the significant imbalance provision was removed in the Resolution adopted by the European Parliament on 12 March 2014. According to the Committee on the Internal Market and Consumer Protection, the expression was the source of potential “legal uncertainty”, which is readily acknowledged, but also useless, “the legislation in contractual matters, including that concerning consumer protection, providing sufficient guarantees against fraud, threats, unlawful exploitation, etc.”. This stance, based as it is on a contractual approach to data procession and thus assuming their marketability, is thankfully not set in stone. The proposal is destined to
undergo a great many more amendments; it can therefore be hope that the final version of the Regulation will not ignore the non-pecuniary dimension of data as personal as images.

Notes:
(1) Court of Cassation decisions published in the Bulletin are indicated by *
(2) Trib. civ. Seine (1st ch.), 16 June 1858, D. 1858. III. 62.
(3) Despite proposals presented before the National Assembly on 16 July 2003.
(5) Which lays down the principle that "everyone has the right to respect for his private life", since Law n° 70–643 of 17 July 1970.
(6) Cass. 1st Civ., 12 December 2000, n° 98–21161*: "the infringement of the right respect for private life and the violation of each person’s right to their image constitute separate sources of damage, conferring the right to separate remedies".
(7) Cass. 1st civ., 15 February 2005, n° 03–18302*: the right to respect for private life having already been ruled non-transferable.
(8) ECHR, Schüssel v Austria, Application n° 42409/98, 21 February 2002.
(9) Cass. 2nd Civ., 19 February 2004, n° 02–11122*: "the principle of freedom of the press implies the free choice of examples of a general discussion on a social phenomenon".
(10) Cass. 1st civ., 5 July 2005, n° 04–10607*, on the photograph of a police officer discovering damage to a vehicle; Cass. 1st civ., 7 March 2006, n° 05–16059*, on the photograph of the widow of a police officer killed whilst on duty, at the funeral.
(11) ECHR, Hachette Filipacchi Associés (Ici Paris) v France, Application n° 12268/03, 23 July 2009: an artist’s publicity snapshots re-used in an article on the marketing of his image in order to fund his lifestyle; Cass. 1st civ., 9 April 2015, n° 14–13519*: ineffectiveness of making the distribution of his image subject to a preview, the filmed interview concerning a debate on ideas of general interest.
(12) Cass. 1st civ., 13 April 1988, n° 86–15524* and 27 February 2007, n° 06–10393*
(13) But without "official functions" – ECHR, Von Hannover v Germany, Application n° 59320/00, 24 June 2004, para. 72.
(14) ECHR, Von Hannover v Germany (n°2), Application n°s 40660/08 and 60641/08, 7 February 2012, para 120.
(15) ECHR, Von Hannover v Germany (n° 3), Application n° 8772/10, 19 September 2013, para. 53.
(16) Contributions to general interest debates (broadly understood), the person’s fame and the subject of the report; their previous behaviour; the content, form and repercussions of the publication; the circumstances in which the photographs were taken; see also ECHR, Axel Springer AG v Germany, Application n° 39954/08, 7 February 2012.
(17) Cass. 1st civ., 13 May 2014, n° 13–15819*: snapshots relating to the "trivial" comments on their relationship "officialised" by poses where they were "embracing at various public events".
(18) Cass. 2nd civ., 18 March 2004, n° 02–12743*
(19) ECHR, von Hannover v Germany, n°s 2 and 3, above.
(20) Cf. in particular, ECHR, L. L. v France, Application n° 7508/02, 10 October 2006.
(22) Cass. 1st civ., 31 October 2012, n° 11–17476*
(23) Cass. 1st civ., 10 September 2014, n° 13–22612*
(24) Art. 226–1, Penal Code
(25) ECHR, De La Flor Cabrera v Spain, Application n° 10764/09, 27 May 2014.
(28) Legal obligation, exercise of public authority, enforcement of a contract to which the person concerned is party or pre–contractual measures they have requested.
(29) Vital interests of the person concerned or general interest
(31) La personne humaine dans le commerce juridique, Dalloz 1932, p. 1
(32) Cass. 1st civ., 11 December 2008, n° 07–19494*
(33) Cass. 1st civ., 4 November 2011, n° 10–24761*
(34) Cass. 1st civ., 14 February 2015, n° 14–11458
(36) Cass. 1st civ., 28 January 2010, n° 08–70248*
(38) For images of sportsmen, see Law n° 2004–1366 of 15 December 2004
(39) See Law n° 2004–575 of 21 June 2004 pour la confiance dans l'économie numérique (on confidence in the digital economy)
(40) See proposed EU Regulation 2012/0011 (COD)
(41) By Law n° 2014–344 of 17 March 2014 on consumption
(42) Art. L. 423–1, para. 2 of said Code
Honorary Board:
Stephen G. Breyer
Olivier Dutheillet de Lamothe
Guy Canivet
Michel Fromont

Hélène Gaudemet-Tallon
François Tulkens
J. H. H. Weiler

Scientific Board

Chairs:
Jean-Bernard Auby & Mireille Delmas-Marty

Gordon Anthony
Michel Bouvier
Pierre Brunet
Giacinto della Cananea
Vlad Constantinesco
James Crawford
Joachim Englisch
Frédérique Ferrand
Jean-François Gaudreault-DesBiens
Jean-Louis Halpérin
Herwig Hofmann
Pascale Idoux
Jean-Pierre Laborde
Li Bin
Kathia Martin-Chenut
Laurent Pech
Marie-Claire Ponthoreau
Nikos Scandamis
Jean-Michel Servais
Denys Simon
Giovanni Tuzet
Pierre-Yves Verkindt
Zhang Li
Jacques Ziller

Editorial Board:

Aurélie Bergeaud-Wetterwald
Laurent Bloch
Jean-François Brisson
Pascal Combeau
Florence Deboissy
Sophie Delbrel
Amane Gogorza
Adeline Gouttenoire
Jean Hauser
Marie Lamarche
Leila Lankarani
Florence Lerique
Valérie Malabat
Sébastien Martin
Philippe Mozas
Alain Pariente
Gaël Piette
Sébastien Platon
Jérôme Porta
Christophe Radé
Aude Rouyère
Frédérique Rueda
Jean Sagot-Duvaux
Jean-Christophe Saint-Pau
Sandrine Sana Chaille de Néré
Sébastien Saunier
Laura Sautonie-Laguionie
Florian Savonitto
Stéphane Schott
David Szymczak
Anne-Marie Tournepiche
Patrick Troude-Chastenet
Guillaume Wicker
Alexandre Zabalza

Managing Editor:
Olivier Dubos

Editor in Chief:
Rachael Singh