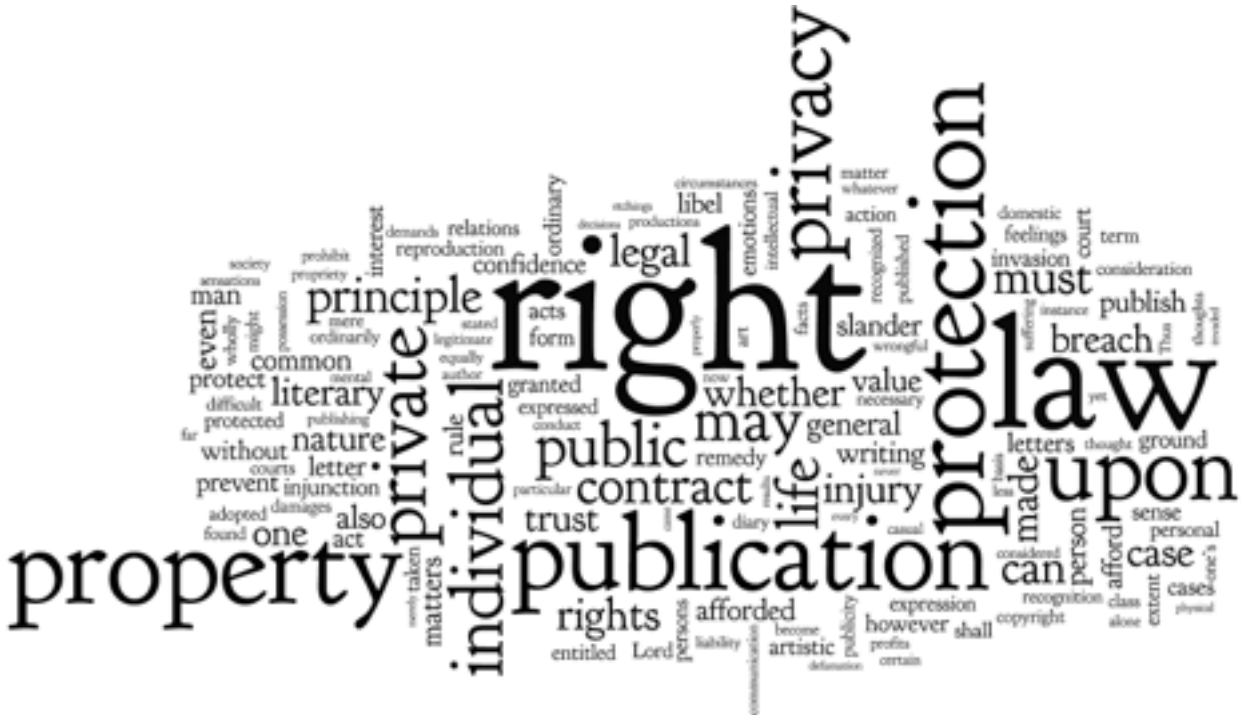
UNIVERSITÉ DE STRASBOURG

The right to privacy



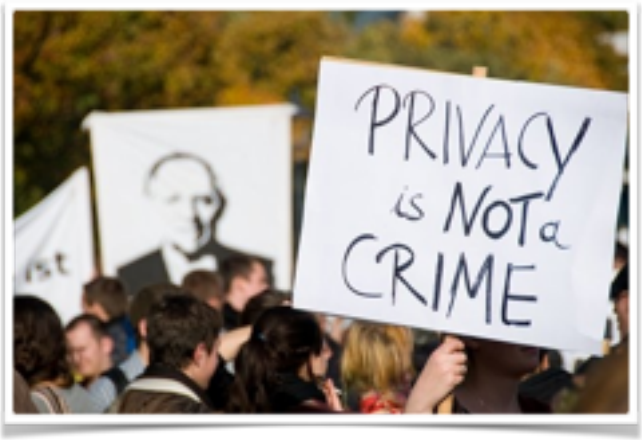
Julie Campagnol
Thérèse Lallart
Johanna Calvel
François Xavier Legrand

EWL 2017

Table of contents

Introduction, general remarks and sources of law

1. Definition of the « *right to privacy* »



What is meant by the expression « right to privacy » is very difficult to define. Even though the concept is included in many texts, such as Article 12 of the Universal Declaration of Human Rights, Article 8 of the European Convention for the Protection of Human Rights and Fundamental freedoms, Article 9 of the Civil Code, it is nowhere defined.

According to Professor Pierre Kayser, the right to privacy is « *the right of a person to be free to pursue his own life as he sees fit, with minimal external interference* ». The right to privacy is thus a right recognized to individuals.

From a legal point of view, therefore, there is no definition of « private life ». However, the judges delineated the contours of this notion by considering as infringements of privacy all information intruding into the privacy of the person, in particular :

- Sexual relations : everyone has the right to organize their sexual life freely. As such, information on homosexuality falls within the framework of respect for privacy and non-discrimination ;
- The sentimental life : the interference in the sentimental life of a person (liaison, divorce, rupture, etc.) can be prosecuted ;
- Family life : interference in family life, and in particular the disclosure of information such as correspondence, domiciliation, holidays, maternity, PACS, is prohibited ;
- Financial situation : the disclosure of information about the financial situation of an individual and his / her family falls under the protection of privacy
- Personal memories : anecdotes and confidences belong to the domain of private life. Only the person concerned has the right to decide on their publication ;
- State of health : medical confidentiality, applicable to all healthcare professionals, is a duty of discretion aiming to respect the privacy of patients ;
- Political or religious convictions : the political opinions and religious beliefs of persons are subject to an obligation of secrecy.

However, the right to privacy is not absolute; it is imbued with the necessary flexibility to « balance the interests involved ». Thus, no one can complain of an infringement to which he has previously expressly consented, and if the legitimate interest of the information justifies the publication in dispute.

However, protection ceases whenever the public has a legitimate interest in knowing the activities, behavior, situation, condition and manner of being of a person. Public power intrudes into private life, most often because of its own right to proof : investigations, right of communication, searches, seizures, excavations, control of identity … These exorbitant powers are in conformity with the Constitution and the European Convention if they are recognized in a law and are imperatively necessary for one of the purposes stipulated by the European Convention.

While it is now possible to consider that the right to privacy is part of human rights, it should also be noted that this recognition was very late in France, in that it was not until 1970 for it to be enshrined by the Civil Code, and until 1977 for it to be integrated into the block of constitutionality.

The recognition of the right to respect for private life has historically been the result of international law, which has not failed to exert a decisive influence on our domestic law.

2. Constitutional recognition of the right to privacy

The right to privacy has a constitutional basis. In a judgment dated from July 23rd of 1999, the Constitutional Council gave the right to privacy a constitutional value on the basis of Article 2 of the Declaration of the Rights of Man and the Citizen. In its decision, the Constitutional Council states that :

« The freedom proclaimed by Article 2 of the DDH which states that the aim of any political association is the preservation of the natural and imprescriptible rights of man and that these rights are freedom, property, safety and resistance to the Oppression, involves respect for privacy ».

The right to privacy thus appears as a derived constitutional principle.

It had also been proposed, in the context of the report submitted to the President of the Republic on February 15th, 1993 by the Advisory Committee on the Revision of the Constitution, to include the principle of the right to privacy in the Constitution by adding a new paragraph to article 66, which would have provided that « *everyone has the right to respect for private life and the dignity of the person* ». However, this suggestion was not accepted.

Today, the right to privacy occupies the highest place in the hierarchy of norms, whether national or international.

3. Statutory recognition of the right to privacy

The Civil Code of 1804 contained no provisions protecting private life, but only a few very punctual provisions relating to the law of property ; these provisions were not intended as rights of the person.

In the absence of specific provisions on privacy, the civil court began by making use of the provisions of ordinary law, ie article 1382 of the Civil Code. The fault then consisted in infringing the privacy of the person, and the result was prejudice.

However, since the judge could not create incriminations on his own, the most serious breaches of privacy could not be criminalized in the absence of any particular text.

It is in these circumstances that the Law of 17 July 1970 introduced in the Civil Code an article 9 which states that « everyone has the right to respect for his private life ». This article also specifies what measures can be taken by the judge, especially in cases of emergency, to stop or prevent a breach of privacy.

Furthermore, France has adopted, the 6th of January of 1978, a law in relation with computing, files and liberties. With that law, France showed its will to protect personal and individual datas, faced with the danger that their use could cause to privacy. This law is clearly against the surveillance of the person at every moment of his life. The first article of that law states that « *Computing must be at the service of every citizen. Its development must operates within the framework of international cooperation. It cannot (porter atteinte) to the human identity, nor to the human rights, nor the the right to privacy, nor to the individual or public liberties* ».

4. The recognition of the right to privacy through national case law

According to a case law dated October 23rd, 1990 by the First Civil Division of the Court of Cassation, « *every person, regardless of rank, birth, fortune or present or future duties, has the right to respect of his private life* »

Jurisprudence sanctions all modes of disclosure: display, public exhibition of the portrait, distribution of the newspaper, magazine or book, projection on screen, on television, on a website, in a computer game, and Of collecting information in a lawful manner does not ensure the immunity of the perpetrator.

The jurisprudence is constant : like any other person, one who is known to a wide public has the right « to be left alone » in his private life.

In France, the case law introduced a difference in terminology between « personal life » and « private life ».

The expression of personal life has been used since 1997 by the jurisprudence of the Court of Cassation. One finds the origin in a study of Professor Waquet "Personal life and professional life of the employee ».

It has succeeded, without replacing them completely, the expressions "private life" of the employee, or "life extra-occupational" of the employee. It had long been recognized that, in principle, the authority of the employer was exercised only at the time and place of work.

The traditional dualism retained legally and opposed the private life of the employee and professional life was perfectly adapted to a productivist conception of work. Out of the factory where he carried out repetitive and daily tasks, the employee could devote himself outside his place of work to activities purely private and devoid of any professional coloring. It was then easy to clearly identify the actual working time as a time when the employee was performing his work. The legal qualification of actual working time was clearly opposed to the time of rest in which the private sphere of the employee could be delimited.

Therefore, outside the company, the employee was, in principle, free to do or say what he wanted. Extra-professional conduct was not theoretically controlled by the employer and could not justify a disciplinary sanction or dismissal[1].

But this separation of private and professional life was, nevertheless, very imprecise.

In many cases, extra-professional behavior, without any connection with the company or with the work performed, was retained as a cause of dismissal, or even as characterizing an employee's fault[2].

Technical development during the 20th century greatly changed the working relationship. As machinery imposes human surveillance, new forms of work performance have been developed, including on-call time, during which the employee is engaged in technical maintenance and not in an uninterrupted manual task . The rise of the Internet and the information society then took over from this progressive modification of the work imposing a new definition of the effective working time, according to which the employee works when he is at the disposal of his employer And conformed to his instructions without being able freely to go about his personal occupations. This conception, because it makes it possible to apprehend the actual working time in which the employee is not productive but simply available, disturbs the boundary established between private and professional life. The definition of actual working time therefore no longer fails to ensure that the employee is available and complies with the employer's instructions in a place other than his / her place of work.

On the occasion of the famous affair of the homosexual sacristan of Saint-Nicolas-du-Chardonnet, the Court of Cassation had to accentuate the protection of the employee[3].

The solution was extended with the Léger judgment: « *In principle, an employee may not be dismissed for a cause deriving from his private life* »[4].

From 1997, the Court of Cassation no longer speaks of private life, but of personal life. On the one hand, the expression "private life" necessarily refers to Article 9 of the Civil Code and Article 8 of the European Convention on Human Rights. However, these texts protect the intimacy of private life, that is, the sphere of life of an individual who escapes all publicity: his home, his correspondence, his loves. Part of the activity of the employee who, although not under the authority of the employer, is open to the public: sporting, cultural, associative and even political activity. These behaviors, which do not fall strictly within the intimacy of private life, nevertheless escape the link of subordination. They are part of the employee's personal life

On the other hand, this personal life is not confused with extra-professional life. Indeed, personal life remains, at least partially, in the company. When the employee exchanges a few words with a colleague, when he goes to the bathroom, when he receives a telephone call from his wife, he is in his personal life and not in his professional life.

E

[1] *Social chamber, 25 juin 1980, n°79-40.292 ; 30 mars 1982, n°79-42.107 ; 8 juin 1983, n°80-41.803*
[2] *Social chamber., 9 oct. 1980, n°78-41.567 ; Plenary chamber., 19 mai 1978, n°76-41.211*
[3] *Social chamber, 17 avr. 1991, n°90-42.636*
[4] *Social chamber, 20 nov. 1991, n°89-44.605*

5. The influence of article 8 of the European Convention of Human Rights

The right to privacy has been recognized in France by the Law of July 17th, 1970. However, this rights had already been recognized by International Law (article 8 of the ECHR in 1950), but also the article 12 of the Universal Declaration of Human Rights, which states that « *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or damage to his honor or reputation. Everyone has the right to the protection of the law against such interference or interference* ».

The article 8 of the European Convention of Human Rights states that every person has a right to respect of her privacy, her family life, her home, and her correspondance. But this article also organises some restrictions, if they are planned by the law, and only if these restrictions are necessary, in a democratic society. This article clearly establishes a protection against illegal immixtion in the privacy of the person.

The decisions of the European Court of Human Rights evidently have an impact in French law. Specifically, the article 8 of the European Convention of Human Rights has an impact on Labour law in France.

As per example, in the Nikon judgment in 2001, the Court of Cassation explained that « *an employee is entitled, even at the time and place of work, to respect for the privacy of his private life* ». This respect « *involves in particular the secrecy of correspondence »* and therefore « *the employer can not take note of the personal messages issued by the employee and received by him through a computer tool placed at his disposal for his work* ». Even if the non-professional use of the computer tool is prohibited in the company …

The Court of Cassation judged this case on the basis of article 9 of the Civil Code, the Labour Code, but also the article 8 of the ECHR. The European Court of Human Rights already had used the article 8 for employment relations.

By using the article 8 as a basis for the decisions, the Court of Cassation gives this european norm an horizontal effect.

Surveillance at work

1. The legality of surveillance at work

The employer can control the activity of employees during working time. But he must obligatorily inform the works council and the employees of the establishment and the use of the means and the techniques of control. Failing that, he may not use the findings made by these means and techniques as evidence. In other words, the disciplinary sanctions taken on this basis are illegal.

Articles of the Labour Code : L.1121-1 ; L.1222-4 ; L.2313-2 ; L.2323-47

The employee is placed under the legal subordination of the employer, who has the power to give him orders and directives, to supervise the execution thereof and to punish the breaches of his subordinate. The employer can therefore control and monitor the activity of employees during working time and it is on this basis that he can sanction the wrongful behavior.

The control of the activity of the employees may be carried out by means and techniques, but these are illicit if they are clandestine.

Indeed, if the right of supervision of the employer is recognized, it is bounded by limits:

- Respect for individual rights and freedoms of the employee, which do not disappear within the company;
- A transparency requirement: the control system must in principle be the subject of information to employees, a consultation of the works council and, where appropriate, a declaration to the CNIL;
- A proportionality requirement: control must be justified by a legitimate interest (productivity, safety, image of the company, etc.) and not excessive. This is not the case when cameras are constantly pointed at employees when no safety considerations justify it and the employer's real concern, particularly suspicious, is to prevent theft by his staff.

On the other hand, the day-to-day monitoring by the employee's supervisor or an internal control department of the company dedicated to this assignment cannot be assimilated to a technical monitoring device.

- **Proportionality**

As regards an invasion of employees' privacy, any measure of control or surveillance must be justified by the nature of the task to be performed and proportionate to the aim sought[5].

Thus, the setting up of CCTV cameras must be justified by a security objective of goods and people.

Control must be strictly limited to time and place of work.

- **Conditions**

In addition to compliance with the principle of proportionality, the employer, if he wishes to set up a technical system for monitoring or controlling the activity of employees, must comply with several conditions.

The employer must inform and consult the works council on the means or techniques used to supervise the employees[6]. Otherwise, he is liable to a conviction for the offense of obstruction, punishable by a fine of

[5] *Article L.1121-1 of the Labor Code*
[6] *Article L.2323-47 of the Labor Code*

7,500 euros[7]. Moreover, the evidence obtained by the supervisory system will not be taken into account by the labor court and the dismissal pronounced solely on the basis of the clandestine control procedure will be judged without a real and serious cause.

Consultation with the CHSCT is not expressly mandated by law, but in view of its growing importance in occupational health and safety, it is advisable to involve it in the employees. If surveillance, for example by cameras or geolocation, is considered to be a source of stress, its consultation is all the more justified.

In accordance with the principle of transparency and loyalty, each employee must be informed about the supervisory arrangements in place[8]. Information must be provided even if the means of surveillance are materially visible. If the employee has not been informed beforehand, the evidence resulting from the clandestine surveillance will be considered as unlawful and rejected by the labor tribunal judge. According to the CNIL, employees must be informed of the purpose of the device, the recipients of the images and the concrete modalities of the exercise of the right of access that they have.

Certain supervisory procedures are accepted by the judges as proof, even though the employees have not been notified beforehand of their establishment. This is the case when the employer's primary motivation is not to monitor and record the activity of employees assigned to their jobs. For example, evidence of an abnormal use of the telephone by an employee could be reported using a telephone report provided by France Telecom. Indeed, the intention of the employer was simply to control the cost of communications and not their content. Recordings of surveillance cameras placed by the employer in warehouses or other storage rooms in which the employees do not work may also be used as evidence.

- **CNIL**

A prior declaration to the CNIL is required before an "automatic data processing system for personal data" is put into service. This is the case, for example, for a telephone tapping system, a software for managing working time or monitoring the connections of employees on the Internet (sites visited, duration of connection, etc.) or any file containing Personal information about the company's personnel.

Where the employer fails to make his declarations, he is liable to a fine of up to € 300,000 and five years' imprisonment[9].

2. Different types of surveillance at work

- **The use of badges**

Some companies implement a system for controlling access to establishments (electronic badge, smart card, etc.). This system can be set up to ensure safety in the company. Failing this, the Cnil allows a simple control of the authorizations of inputs and outputs in certain premises without recordings which would allow them to be memorized. This system can also be set up in companies to facilitate the management of work schedules, when there is a system of flexible schedules.

The Cnil recalls that this system allows the physical identification of the wearer. Therefore, it is a nominal treatment and its implementation is permitted but must be the subject of a prior declaration with the CNIL. In the absence of such a declaration, the system put in place is unenforceable to the employees. They can not therefore be penalized for refusing to use it

- **Video surveillance at work**

Cameras can be installed at a workplace for purposes of safety of the properties and goods and the people, in dissuasive intent or to identify the authors of thefts, damages or attacks.

The employer is authorized to set up a video surveillance system allowing the control of his employees, by respecting certain prerequisites :

[7] *Article L.2328-1 of the Labor Code*
[8] *Article L.1222-4 of the Labor Code*
[9] *Article 226-16 of the Criminal Code*

- he has to respect personal freedoms and private life of the employees,
- he has to consult the staff representatives and inform the employees,
- he has to plan an access right in the visual recordings concerning them

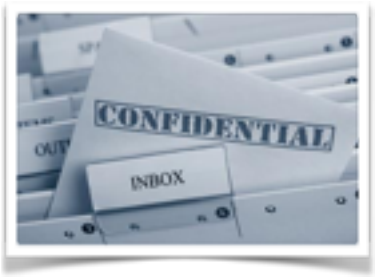
The use of the video surveillance in the company must be justified by a dominating justifiable interest of the company.

Cameras can be installed at the level of entrances and exits of buildings, emergency exits and traffic lanes. They can also film the zones where the goods or the valuable properties are stored. They should not film the employees on their job, except in particular circumstances. Indeed, in the workplace as somewhere else, the employees are entitled to the respect for their private life. Cameras should not either film the zones of break or rest of the employees, nor the toilet. Finally, they should not film the trade-union premises or the staff representatives, nor their access when it leads only to these only premises.

Only the authorized people and within the framework of their functions can view the recorded images.

The preservation of the images should not exceed one month.

- **Control of the use of internet and mail box**



On the ground of the respect to privacy of the employee and the infringement on its fundamental liberties, the Court of Cassation considers that files created by him thanks to the IT tool provided by the company are presumed to have a professional character ; thus, the employer can have there free access[10].
So, a USB key, belonging to the employee, connected to the IT tool intended for the execution of the work is, just like the computer itself, presumed to be used for professional purposes. The employer can thus have there access outside the presence of employee, safe for files clearly identified as staff.

It is unless the employee does not identify these files and documents as personal or does not classify them so that they can be considered as such. If that is the case, except risk or particular event, the employer can open the aforementioned files only in the presence of the employee[11].
The employer has no access to e-mails exchanged on a personal e-mail address, different from the professional messaging, even if the employee uses his professional computer to send and receive messages on this address.

The case law had been fixed by the Nikon judgment of 2001. There, the Court of Cassation explained that « an employee is entitled, even at the time and place of work, to respect for the privacy of his private life ». This respect « involves in particular the secrecy of correspondence » and therefore « the employer cannot take note of the personal messages issued by the employee and received by him through a computer tool placed at his disposal for his work ». Even if the non-professional use of the computer tool is prohibited in the company …

Except this frame, an investigation of the computer of the employee, in particular personnel messages emitted and received by him, will be likened to a violation of the secret of correspondence

- **Control by system of phone-trapping**

From the point of view of the criminal law, the listening of the phone conversations of the employees constitutes an invasion of privacy.

It is repressed by the article 226-1 of the Penal code which plans a detention of one year and a 45 000 € fine for every person who is engaged in the listening or in the recording of words pronounced in a private place by a person, without the consent of this one.

A ministerial answer specifies that « t*he only fact of informing in advance an employee that his telephone communications may be listened to or recorded shall not allow the employer to escape his penal responsibility if the employee did not previously give his consent, if only in a tacit way. The breach could also*

[10] *Social chamber, 30 mai 2007 ; 18 octobre 2006 ; 21 octobre 2009*
[11] *Social chamber, 17 mai 2005*

be characterized as far as the phone correspondent of the employee is not warned that his conversation, which can be personal nature, is recorded or listened to by a third party ».

If the recording of phone conversations in the workplace is forbidden on principle (Article 226-15 Penal code), it is authorized exceptionally, on the condition that it answers the principles regarding surveillance of the salaried employees.

- **Control of SMS**

The High jurisdiction considers that written messages (SMS), sent or received by the employee by means of the telephone, provided by the company for the needs for his work, are presumed to have a professional character and does not constitute a private mean of communication. Therefore, the employer is entitled to consult them without the presence of the interested needed.

- **Geolocalisation**

Some companies use geolocation systems to gain insight into the geographical position of employees' vehicles. The use of such a system is justified only if it pursues one of the following purposes :

- compliance with a legal or regulatory obligation requiring the implementation of a geolocation device because of the type of transport or the nature of the goods transported;
- the monitoring of a transport service for passengers or goods or services directly linked to the use of the vehicle, as well as the justification of a service with a customer;
- the safety or security of the employee himself or of the goods or the vehicles for which he is responsible, in particular the fight against vehicle theft;
- better allocation of resources for services to be provided in scattered locations, in particular for emergency response;
- monitoring compliance with the rules for the use of the vehicle defined by the employer, provided that it does not collect location data outside the driver's working time.

The geolocation may have as a purpose the monitoring of working time when this cannot be achieved by another means, provided that it does not collect or process location data outside the working time of the employees concerned. The data collected must be adequate, relevant and not excessive in relation to the purpose pursued.

The CNIL has also issued a global ban on geolocation outside working hours in order to protect the privacy and privacy of employees. It is therefore not possible to collect location data outside the employee's working time, particularly when traveling between work and home, or during breaks. Employees must therefore be able to disable the geolocation function of vehicles.

3. Data protection relating to health

- **Doctor-patient confidentiality**

Article 226-13 of the Penal Code punishes those who violate professional secrecy as follows: « *The disclosure of secret information by a person who is in possession of it by state or profession or by reason of a temporary function or mission is punishable by one year's imprisonment and 15,000 Euros of fine ».*

The professional secrecy can be found in many situations : banking secrecy, manufacturing secret etc. This paper will only focus on the doctor-patient confidentiality.

Article L.1110-4, paragraph 1 of the Public Health Code states that « *Any person assisted by a health professional, institution or department, professional or organization involved in prevention or care whose conditions of practice or activities are governed by this Code, the Armed Forces Health Service, A professional in the medico-social or social sector or a social or medico-social institution or service referred to in I of Article L. 312-1 of the Code of Social Action and Families has the right to respect for his private life and Of the secrecy of the information concerning him »*.

Article R.4127-4 of the Public Health Code provides further details about the doctor-patient confidentiality : « *The professional secrecy instituted in the interest of the patients is imposed on any doctor under the conditions established by the law.*

Secrecy covers all that has come to the knowledge of the physician in the exercise of his profession, that is to say not only what has been entrusted to him, but also what he has seen, heard or understood ».

When someone starts a new job, he has to see a specialist physician named «***occupational health doctor*** » to ensure that the patient is physically and mentally capable of doing this job. After this medical approval, the specialist will create a ***medical file***. This medical file is defined in article L.4624-8 of the Labor Code :

« An occupational health medical file, drawn up by the occupational physician, shall trace the information concerning the health status of the worker, the exhibitions to which he has been submitted and the opinions and proposals of the doctor Including those made under Articles L. 4624-3 and L. 4624-4. This file can only be communicated to the doctor of his choice, at the request of the person concerned. In case of risk to public health or at his request, the occupational physician transmits it to the medical inspector of labor. This file may be communicated to another occupational physician in the continuity of care, unless the worker refuses. The worker or, in the event of his death, any person authorized by Articles L. 1110-4 and L. 1111-7 of the Public Health Code may request the disclosure of this file ».

The medical file includes all information about the health status of the worker, the risks to which he is exposed, and the notice and proposal from the occupational health doctor. This file can be forwarded to another doctor choose by the worker, but only to another doctor. Moreover, when the occupational health doctor changes, the file is automatically transmitted to the new doctor, unless the worker formally refuses.

According to a case law dated July 2002 by the Social Court, the medical file is covered by the Doctor-Patient confidentiality and can not be communicated to the employer. The latter can not blame the occupational health doctor for not transmitting the information of this file. Furthermore, the Court said in 2015 that the employer can't use a certificated from the occupational health doctor based on information from the medical file.

However, the occupational health doctor can, without the agreement of the employee, transmit the file to the Medical inspector if he asks for it or it presents a potential risk to the public health.

The civil and criminal liability of the doctor can be engaged according to the article 226-13 of the penal code in case of violation of the Doctor-Patient confidentiality about the medical file.

After we exposed the speciality of the Doctor-Patient confidentiality, clarifications need to be made about the data protection relating to the health during the execution of the work contract and at the hiring.

- **<u>At the hiring stage</u>**

According to the principle of non-discrimination founded in article L.1132-1 of the Labour Code, the employer can't refuse to hire someone because of his health status or his genetics characteristic. All the criterion on which one none discrimination can be based can be found in article 1 of the Law n°2016-1547 of November 18 2016. The exception of the health status is when the employee is unfit, according to the occupational health doctor.

- **During the execution of the work contrat**

The employer can't know the details about the health of his employee. But after the hiring and during the career, the employee must see the occupational health doctor to make sure he is able to work. The employer will only know if the employee is able to work or not. If the employee is unable to work, the employer won't know the details of the health issue or the disease.

During the execution of the work contract, the employer can ask to his employee to see the occupational health doctor. But he will never be able to ask medical tests.

- **The surprise about the salivary test**

According to the State council December 5 2016, the employer can ask an employee a salivary test for drug detection, without a specialist intervention.
Conditions:

- This test's terms and conditions must be in prior defined in the company rules.
- This detection will be only for the employees who are exposed to risk
- Those employees can ask a medical second-opinion

First, the Court of Appeal considered that this salivary test was a biologic test within biologic and clinic data which must respect Doctor-patient confidentiality, and then, it can't be used by the employer.
Moreover, the results can't be used against the employee because they aren't liable. This is a disproportionate violation of the personal rights and individual and collective liberties compared to the research goal.

However, the State Council has judged, in contrary, that the employer can ask a salivary test because:

- This test, that we can found in the company rules in question, only reveals if there were a recent drug consumption.
- This is not a biologic medical test so a specialist doesn't have to do this test

The Council accepts the company's rules after having checked that the rule is justified and proportionated to the research goal. It considers that there were some guaranties:

- The employee could have a second medical opinion
- This test was reserved to the employee for whom the drug is particularly dangerous for them and other people, due to their job.
- The employer has to respect the doctor-patient confidentiality with the results.

This does not limit people rights and individual and collective liberties.

4. The role of collective representation bodies in regard of secret or open surveillance measures

The surveillance and the control of the employee in the company and during the working time, and the possibility to sanction bad behavior are some prerogatives of the employer. This is justified by the subordination link. However this control is not absolute. There are some conditions and procedures to safeguard employee's fundamental rights.

- **The company rules and regulations**

Some elements of the surveillance can be found in the company rules and regulations : they can be applied only if the work council has given his notice, and if there isn't work council, this will be the staff representative. For some subjects, the employer will need the notice of the security and working committee.

- About the work council, or the staff representative's notice

The notice will be delivered in the meeting's minutes of the work council, or in a written document of the consultation of the staff representative.

In the firm where there is neither work council nor staff representative, the law does not introduce other obligation of staff consultation. In that case, the work inspector can proceed to investigation if he considers this is necessary. Moreover, even if there is no representative staff elected, the employer must create the company's rules and regulations.

If the employer doesn't ask the notice, the rules and regulations won't be applicable.

Moreover, every dismissal based on the disrespect of those rules won't be justified. Moreover, the employer can have penal sanction according to the article R.1323-1 of Penal Code for the offense of interfering with the functions of the works council.

It is important to know that this is simply notice. If the work council refuse to approved the rules and regulations, the employer may still apply them.

- About the security and working committee

This committee must be consulted on measures about hygiene and security rules in the company. According to a case law in February 2015, company rules and regulations can be modified only after the notice of the security and working committee for matters within its competence. For example, when security cameras or geolocation are considered to be a source of stress.

- **Other surveillance measures exist but each of them must respect some procedures :**

  - Prior information of the concerned employees

The new technologies offer to the employer new way to control their salaries. However, according to articles L.1121-1 and L.1222-4 of the Labour Code, whatever the means of control implemented in the company (badges, telephone tapping, video surveillance ...), the employer must inform the employees in advance

In 1991, the Court stated that if the employer used as a proof this kind of control implemented without having beforehand inform the employees, this proof will be not acceptable. Moreover, those ways to control the activity of the salaries must be proportionate to the research goal. For example : control the access to the company for security goal.

However, the simply surveillance of an employee on the premises isn't a criminal way of proof, even without the prior information of the employee.

  - *Prior obligatory information and consultation of the work council*

The work council must be consulted beforehand about the measures of the control of the worker's activity, according to the article L2323-47. This is not an obligation when the employer put surveillance processing in the premises where there is no employee. For example : Warehouse.

If he doesn't respect the prior obligatory consultation, he could have penal sanction for illegal interference.

On the other hand, an employer wishing to carry out an audit to evaluate the organization of a service at any given time may do so without prior authorization from the employee representatives.

Finally, according to the article L2313-2, employees may refer to their staff delegates, who have a right to alert, in the event of an infringement on the rights of individuals or individual freedoms. For example, if there is discrimination, or sexual or moral harassment.

Moreover, the right of alert can be used against irregular decision, when there was not any staff representative consultation, or violation of the private employee life. When there is an activity control without consulting ou informing the work council, the staff delegates can demand the withdrawal of the proof which

have been obtain in a fraudulent way. For example, a staff delegate can pursue the employer to delete the video the employee was not aware of

- **The data protection's delegate**

The "computing and freedom's correspondent" makes sure of the legal and computing security of his organization. In 2018, he will become the "data protection's delegate".

His Missions and his benefits:

- More computing security: he advises his organization about the new way to run the data. This spares the organization from doing strategic mistakes about the product or service launched, to maximize investment and implement an archiving policy ;
- More legal security: he checks the European regulation and national laws about the data protection: this prevents from being pursued ;
- More trust: he reassures both external people of the organization (clients, suppliers, control authorities…) and intern people about their rights the collection of personal data ;
- More data valorization : having a delegate is more liable and the data are managed in a more effective and timely manner (file transmission, etc.).

His appointment is mandatory for:

- Public organizations ;
- The organizations which need a follow up ;
- The organizations which have sensitive data or data about criminal sentence or breach.

The organization can appoint an intern or external delegate. He can work for several organizations but under some conditions. I.e.: Company group.

It is important to know that the delegate isn't personally responsible if the organization doesn't respect the regulation.

5. Executive and/or indépendant authorities occupied with data protection

Faced with the evolution and the important use of computing, the legislator has had the objectif to protect individual liberties ; but, at the same time, he didn't want to hinder the development of computing technics, which are considered as participating in economical and social progress.

That's in these circumstances that the CNIL has been created, to control and protect the liberties faced with surveillance systems.

The CNIL (Commission Nationale de l'Informatique et des Libertés – The National Commission for Data protection and Liberties) is an administrative independent authority who's occupied with data protection.

The CNIL follows professionals for compliance to French law, and help the private individual to control their private data and to exercise their rights. The CNIL also analyses the impact of technologies innovations and their utilization over private life and liberties. This body works in collaboration with the European and international counterparts for the development of harmonized regulation.

The CNIL has 4 principal missions which are the following:

1. The i**nformation and the protection** of professionals and private individuals through digital information ;
2. **Supporting and advising for compliance** to French law: the CNIL gives its opinion about a project of law or executive regulations, and gives the authorization for a specific treatment of data ;

3. **Control and condemn through on-site-control, documentation's control and audition**. The CNIL can control the system of video protection allowed by the prefecture. In case of a on-site-control, the CNIL will have access to all the professional locations and can ask all documentation which are necessary and take a copy of them. It can also collect all useful information and hear any person. It can access to program and data. The control operated by the CNIL is very strong and extended to prevent a possible violation of data.
4. **Anticipate** through a legal detect or an analyzing of technologies and new innovations which can have an impact on private life. The CNIL has its own laboratory allowing experimentation of products and innovative applications. The CNIL also contributes to development of technology solutions which are protecting private life through advising companies the more upwind than possible. A council was created for appealing experts who advise the CNIL for the elaboration of an annual program of studies and explorations. The mission, in this case, follows a reflection about ethic problems and about questions of companies through the evolution of technology.

The CNIL can condemn someone who used or processed Data in violation of the protective provisions at the end of the control or a complaint. The restricted formation of the CNIL composed by 5 members and a President who's not the CNIL's President can pronounce penalties against the author of illegal treatments of Data. The sanctions are the following:

- A caution who can become public
- In case of a prior formal notice gave by the President of the CNIL and for which the author didn't comply, a penalty amount 150 000 € applies (300.000 € in case of recidivism). The decision can become public and insert in a newspaper. The amounts are received by the Treasure Public (= the government treasury)
- An injunction to stop the treatment
- A recall of the Authorization of the CNIL in application of t*he article 25 of the law on data processing, data files and Liberties.*

Furthermore, the CNIL is provided with the faculty to apply other sanctions in particular circumstances:

- To prevent an immediate and serious damage on rights and liberties, the President of the CNIL can ask to the competent jurisdiction through an interlocutory proceeding that it orders any safety and necessary actions. The CNIL can denounce to the public prosecutor an infraction to the law on data processing, data files and liberties, infractions listed from *the article 226-16 to 226-24 of the penal code (infractions on humans rights resulting of data and IT processing).*
- In case of emergency or of damage on the rights and liberties, the restricted formation can pronounce at the end of the contradictory procedure:
  - An interruption of the treatment
  - A caution
  - The locking of the data for 3 months
  - Inform the Prime Minister for some sensitive files to take actions that are necessary to end the violation act. Faced with the evolution and the important use of computing, the legislator has had the objectif to protect individual liberties ; but, at the same time, he didn't want to hinder the development of computing technics, which are considered as participating in economical and social progress.

6. The use of material obtained through illegal surveillance measures as evidence

In principle, an employer can't use material obtained through illegal surveillance measures for dismissals, without taking prior measures upwind. But this kind of system can be allowed if it is proportional to the intention[12] and if it respects the image rights and the private and intimacy life[13].

According to French law, some formalities must be accomplished:

- ***ask a declaration to the CNIL***: the CNIL takes action in case of automatic treatment of the nominative data and the employees must obtain a copy of information concerning them. The installation of a system of video surveillance takes legal place if the employer obtains an authorization from the CNIL in case of record and transmission of the images.

[12] *Article L.1121-1 from the Labour Code*
[13] *Article 226-1 from the criminal code*

- ***inform the work council and require it advice*** about the ways of the activity control upwind the decision of the CNIL[14] and inform the personnel representative.

- ***Information to the employees[15]*** through a notice or any document. They must establish the valuable video surveillance in the location. This information is submitted to the procedure of the intern regimentation. In case of dismissal proved by a video surveillance without any prior information to the employee, a judge can condemn the employer for unfair dismissal based on an illegal proof.

The video surveillance takes place in a public location or in a location particularly exposed to a risque of infraction like a stealing or for a personal safety and asset protection intention.

According to the french jurisprudence:

- The social chamber of the Court of Cassation affirmed that a control is legal on the work location if a prior information is given to the employees who work there. On the contrary, it would be an illegal proof[16].
- The criminal chamber of the Court of Cassation judged that the recording could be a legal proof for claiming an insurance fund operated by an employee[17].
- The employer has the obligation to inform the employees about the utilization of the images which could be used against them, in other terms, it speaks about the possibility for the employer to have a large control of professional activity and work hours only if the information is given[18]. The same rule applies when it concerns employees from an other location (the client company).
- In other locations, the employer can use recordings without information to his employees. It concerns **locations where they have not access.** it's a kind of proof in case of a fault. In this situation, there is no obligation for the employer to inform and consult the personnel representative and the employees. This situation takes place for example for the storage where employees don't have access[19].

But important is to be conformed to the actions given by the CNIL. A violation of one of a rule edited by the CNIL can engage the employer's responsibility, for example when he doesn't want to compliance his system judged abusive and intrusive to the rules[20].

[14] *Article L.2323-32 from the Labour Code*
[15] *Article L.1222-4 from the labour code*
[16] *Social chamber, 20th of November 1991, N°88-43.120*
[17] *Criminal chamber, 6th of April 1994, N°93-42.717*
[18] *Social chambre, 10th of January 2012, N°10-23.482*
[19] *Social chamber, 31th of January 2001, N°98-44.290*
[20] *CNIL, deliberation N°2013-139 from the 30th of May 2013*

Whistleblowing

1. Before SAPIN's Law from December 9th, 2016

Before SAPIN's law II, there were no global legal basis about whistleblowing issues. Nevertheless, France has adopted six ethics laws between 2007 and 2015:

- Act No. 2007-1598 of 13 November 2007 on the fight against corruption provided for a protection regime for employees denouncing acts of corruption[21].

- Act No. 2011-2012 of 29 December 2011 on strengthening the health safety of medicinal products and health products provided that no person may be discriminated against for reporting or giving evidence in good faith[22].

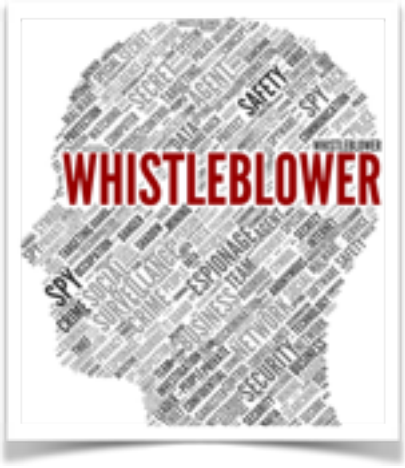
- Act No. 2013-316 of 16 April 2013 on the independence of expertise in the field of health and the environment and the protection of whistleblowers provides that every person (moral or physical) has the right to diffuse in good faith information relating to a fact, data or action, provided that the knowledge of that fact, data or action appears to him to be a serious public health or the environment risk. It establishes a protection of workers in the field of public health and the environment[23].

- Act No. 2013-907 of 11 October 2013 on the transparency of public life provided[24]. Any person who relates or reports in good faith to his employer, to the ethics authority within the organization, to an anti-corruption association or to the judicial or administrative authorities about facts relatives to conflict of interest, concerning public officials of which the person would have been aware in the exercise of her functions.

- Act No. 2013-1117 of 6 December 2013 on combating tax fraud and serious economic and financial delinquency included an article in the Labour Code for the benefit of the employee who, in good faith, relates facts constituting an offense or a crime of which the person would have been aware in the exercise of her functions.[25]

- Act No. 2015-912 of 24 July 2015 on intelligence provides protection for intelligence officers who believe that a clear violation of the use of intelligence techniques would be committed within the intelligence service where they Are assigned[26].

2. After SPAIN's Law from December 9th, 2016



Act No. 2016-1691 SAPIN II creates a set of rights common to all warning alert launchers, regardless of the scope of the alert. The system adopted remains complex and limited, in particular the Senate fears unfounded alerts designed to destabilize certain companies.

◆ **Definition of whistleblowing**

Article 6 of Act No. 2016-1691 of 9 December 2016 provides that "*An alert launcher is a natural person who discloses, in a disinterested and bona fide manner, a crime or an offense, a serious and an international undertaking duly ratified or approved by France, a unilateral act of an international organization made on the basis of such an undertaking, the law or regulation, or a serious threat or General interest, of which he had personal knowledge* ».

[21] *Labour Code, article L. 1161-1, abrogated by the law No. 2016-1691, Art. 15-III*
[22] *Labour Code, Art L. 4133-1 to L. 4133-5, the latter abrogated by the law No. 2016-1691, Art. 15-II*
[23] *public health Code, article L. 5312-4-2, abrogated by the law No. 2016-1691, article 15-V*
[24] *Article 25, abrogated by L. No. 2016-1691, art 15-II*
[25] *Labour Code, Article L. 1132-3-3, edited by L. No. 2016 -1691, Article 10*
[26] *CSI, article L. 861-3*

The Constitutional Council considered that these criteria for defining the alert launcher are not imprecise[27].

- **Criminal irresponsibility**

A criminal irresponsibility is instituted in favor of a person who infringes a secrecy protected by law, provided that such disclosure is necessary and proportionate to the safeguarding of the interests concerned, that it intervenes in accordance with the reporting procedures defined by the law and the person meets the criteria for defining the alert launcher[28].

- **Exclusions**

Are excluded from the alert system facts, information or documents, whatever their form or medium, covered by the secrecy of national defense, medical secrecy or the secrecy of relations between a lawyer and his client. In general, difficulties may persist as long as the obligation of professional secrecy

- **Reporting procedure**

The law provides a three level system[29].

- In principle, the reporting of an alert is brought to the attention of the supervisor, direct or indirect, of the employer or a referrer designated by him
- Only in the absence of the due diligence of the person to whom the alert is to be sent, within a reasonable period of time, the admissibility of the alert shall be addressed to the judicial authority, the administrative authority or the professional associations.
- Finally, in the absence of treatment by one of these organization within a period of three months, the signal may be made public.

It is only in the case of a serious and imminent danger or in the presence of a risk of irreversible damage that the signal may be brought directly to the authorities or the orders mentioned above. It may be made public[30].

The Constitutional Council, however, clarified that the scope of this article 8 is confined to whistleblowers making an alert about the organization employing them or the organization to which they collaborate in a professional setting[31]. It follows from the law that it does not apply to "external" alert launchers.

- **Protection by the Labour Code**

Prohibition of possible reprisals against the whistleblower and a reversal of the burden of proof is provided in the event of a dispute, since it will be for the employer to prove that his decision is justified by objective factors, alien to the declaration or testimony of the person concerned[32].

The protection doesn't work in case of the intent to harm.

- **Diversity label**

The "diversity label", created by a decree of December 2008, aims to promote diversity and prevention of discrimination at workplace and to promote best practices in recruitment and professional development within organisms

Organizations or companies which apply for the "diversity label" must comply with a specification which recommends the establishment of tools to identify internal and external complaints and, in general, to ensure the traceability of reports of discriminated employees.

It is therefore necessary to have rules about whistleblower in the company to obtain this label.

[27] *CC, decision 2016-741 DC, 8 Dec. 2016*
[28] *L. No. 2016-1691, article 7, Penal Code, Article 122-9*
[29] *L. No. 2016-1691, Article 8-I*
[30] *L. No. 2016-1691, Article 8-II*
[31] *Decision No. 2016-741, December 8th, 2016*
[32] *Article L. 1132-3-3 of Labour code*

Social media in the working relation

1. Legal regime

The Social Chamber sets out the legal rules governing the freedom of expression of the employee and indicates the two rules to which his normal practice is subject:
« *if the employee enjoys, within and outside the company, of his freedom of expression, to which restrictions may be imposed only if they are justified by the nature of the task to be performed and proportionate to the aim sought, he may not abuse this freedom by insulting, defamatory or excessive remarks* »[33].

On the one hand, the restriction is the exception and is subordinated to the principles of justification and proportionality. On the other hand, the exercise of freedom of expression can exceed the limits, which takes the form of abuse.

Therefore, the Social Chamber states regularly that « the exercise of freedom of expression for employees both inside and outside the company can justify dismissal only if it degenerates into abuse »[34].

In this regard, « abuse is the only limit to freedom of expression outside the enterprise »[35].

2. Social network

The distinction « in the company » and « outside the company » seems to be not relevant anymore with the use of the social network and media. The two big issues are, in this case, centred on the question of proof and on the public or private character of these networks.

To that purpose, it was judged that Facebook "can constitute either a private space or a public space, depending on the settings made by its user"[36].

Example: The Paris Labour Court, in the case of petiteanglaise.com, in which an English employee expatriate in France was dismissed for calling her employer a "twunt" on her blog, invalidated the dismissal because the employer was not identifiable[37].

3. Privacy character of the social network

The question is whether or not what is "written" on a Facebook wall has a public character or a private character? The judge made it depending on the existence or absence of a community of interests. Then the public nature or not of the insult will be retained.

Thus, when comments are posted on accounts opened on the Facebook site as well as on the MSN site and are accessible only to the persons authorized by the person concerned, in very limited number, the latter form a community of interests. It follows that the statements made in these accounts do not constitute public insults[38].

[33] *Social chamber, October 30th, 2002, n° 00-40.868 : JurisData n° 2002-016283*
[34] *Social chamber, January 25th, 2000, n° 97-45.044 : JurisData n° 2000-000423*
[35] *Social chamber, february 4th, 1997, n° 96-40.678 : JurisData n° 1997-000583*
[36] *Appeal Court of Rouen, November 15th, 2011, n° 11/01830*
[37] *Social chamber 5, mars 29th, 2007, n° F06/08171*
[38] *Civil chamber 1st, april 10th, 2013, n°11-19.530, Mme D. c/ Mme V. :JurisData n° 2013-006693*