

Protection of Employee's Personal Information and Privacy in France

Benjamin Dabosville
Université de Strasbourg

Introduction

Protection of employees' personal information and privacy is one of the central issues of employment relationships in the twenty-first century. Since several decades, technologies have given the employer the opportunity to make more enquiries about the workers' personal life and to record many data. On the other hand, protecting individual liberties from management authority has been a greater concern since the 1980s. This dilemma to manage the employer's and employee's interests is altogether enhanced by the difficulty in drawing the boundaries between "personal" and "professional" life. It is now common that an employee uses his house as workplace or asks his colleagues as "friend" on Facebook.

French law has been paying attention to this topic for a long time. The framework of the legislation results from two important Acts voted on January 6, 1978 and on December 31, 1992. Since then, the law has been adapted to the evolution of technology and management by the interpretation of an independent authority, the "*Commission Nationale de l'Informatique et des Libertés*" (CNIL), and by the case law of both the "*Cour de cassation*" and the "*Conseil d'Etat*", which are the highest civil and administrative courts. The protection has also been reinforced due to the impact of the European Union, especially the directive 95/46 of October 24, 1995.

Nevertheless, having regards to the paramount importance to this theme, the consideration on employee's personal information and privacy protection seems to be insufficient in France, especially by comparison with Germany and other European countries. Of course some scandals, such as Ikea's illegal spying¹, have drawn the attention of the press. Newspapers and TV shows also provide explanations about the appropriate way to use professional e-mail addresses or personal Facebook's profiles. Meanwhile, there are no substantial discussions in the global media or in the academic literature about a better way to protect legally the individuals against the danger of new information technologies. The government seems to focus on the applications developed by Google, Facebook or Apple concerning consumers' personal data. Moreover, French employees and trade unions seem to be more preoccupied by the social dimension of the employment relationship and the reform of labor market than by the protection of worker's information and privacy. So far, no government bill and no trade-union's proposal have been planned on the topic of employee's information and privacy.

Despite this lack of controversies, the examination of the French law highlights many

¹ *Le Monde*, July 27, 2013.

interesting issues of this topic. First, the analysis of the regulatory schemes shows the existence of a dual protection system that may be substantially changed in the coming years (I). Secondly, it seems that various methods are used to strike a balance between the interests of the employer and the interests of the employees (II). Lastly, the provisions regarding the employment relationship point out several difficulties, related to the role of the duty of transparency, the implementation of the proportionality principle and the gradation of the protection of employees personal information and privacy (III).

I. Regulatory schemes for the protection of the employees' personal information and privacy

The primary basis for the protection of the employees' personal information and privacy is not the French constitution, but international treaties (A).

Concerning the detailed arrangements for this protection, it should be noted that, even if national legislation and case-law originally played a major role, the impact of European rules has been steadily increasing (B).

A. Primary basis of the protection

The French constitution does not mention anything important about the employees' personal information and privacy, neither about the right of privacy nor about the protection of personal's data information. This lack has been filled by the constitutional judge, the "*Conseil constitutionnel*", that recognized the right of privacy in 1996² and started to develop the protection of personal information in 2004³. In recent years, the opportunity to change the Constitution in order to explicitly guarantee the right of privacy and the protection of personal data has been discussed. However, the Committee on the Preamble of the Constitution considered in 2008 that this modification should not be a priority⁴. The guarantees arising from the case-law of the constitutional court and from the international instruments are considered as sufficient.

Indeed, several international instruments protect privacy and personal information. The most important are those elaborated within the context of the Council of Europe and within the context of the European Union⁵.

In the Council of Europe, mention must be made of article 8 of the European Convention on Human Rights, which protects the right of privacy. Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data dated January 28, 1981 should not be forgotten as well. Not only because this text played a major role over the last century in the elaboration of the guidelines of the personal information protection, but also because many states are now member of this Convention. All the Member States of the European Union and the European Union itself have signed the Convention. Countries like Ukraine, Russia or even Uruguay have also signed the Convention recently⁶.

² Conseil Constitutionnel, July 23, 1999, decision n°1999-416. The Right of privacy is provided for in Article 9 of the "*Code civil*" (Civil Code) since 1970 (Act n° 70-643 of July 17, 1970).

³ Conseil Constitutionnel, July 29, 2004, decision n°2004-499.

⁴ *Rapport Veil sur le préambule de la Constitution*, La documentation française, 2008.

⁵ Article 12 of the Universal Declaration of Human Rights of December 10, 1948 and Article 17.1 of the International Covenant on Civil and Political Rights of November 16, 1966 should be mentioned too.

⁶ Adhesion of Morocco is in progress.

The EU also has a great influence on this topic. The directives about non-discrimination and equal treatment⁷ of course have some impact on this theme, protecting some characteristic of the individuals, like age, gender, sexuality preference. Nevertheless, the most important instrument is no doubt the directive 95/46/CE of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data⁸. Protection of privacy and personal information has also been later reinforced by the Charter of Fundamental Rights of the European Union signed in 2000. Article 7 of this text states that “everyone has the right to respect for his or her private and family life, home and communications” while Article 8 §1 provides that “everyone has the right to the protection of personal data concerning him or her”.

B. Protection rules

Regarding the rules governing the protection of employee's personal information and privacy, two periods may be distinguished. From 1978 to 1992 was the time for legislative action. Two important Acts have been adopted, one in 1978, the other one in 1992. Since 1992, major change came rather from the action of the EU, meanwhile national judges and administrative authorities adapted the legal provisions to the problems caused by new technologies or new management's methods.

The French law is now characterized by a dual system (1) that has already been modified by the European legislation and that could be changed by the proposal from the European Commission in progress (2).

1) A dual system

Two mechanisms have been set up by legislation in order to protect the employee's personal information and privacy.

The Act n°78-17 of January 6, 1978 on “Information Technology, Data files and civil Liberties”⁹ had the ambition to solve most of the problems resulting from the use of computer. A wide debate and intensive work of a commission took place before the vote in Parliament¹⁰. Although this piece of legislation is considered as one of the most symbolic Acts of the French legislation, it may be noted that it is mainly a defensive law, which primary aimed at preventing the emergence of a Big Brother State. Neither the more frequent use of new information technology in the labor relationships nor the development of the “information society”, in which individuals use Internet to collect and send information, had been imagined and anticipated. Nevertheless, Directive 95/46/CE of October 24, 1995 led to modifications to this Act by providing a more suitable legal framework to these societal developments. In addition, it seems that, even if this Act has been elaborated to be used in the public sector, its provisions are pretty adapted to the private sector and the employment relationship.

The Act n°92-1446 of December 31, 1992 had a different ambition. Only five articles

⁷ Especially the Council Directive 2000/78/EC of November 27, 2000 establishing a general framework for equal treatment in employment and occupation.

⁸ Directive 95/46 and Convention 108 have the same guidelines.

⁹ “*Loi du 6 janvier 1978 relative à informatique, aux fichiers et aux libertés*”. The current and full version of this Act can be consulted by connecting to www.cnil.fr. Quotes in this contribution are from the unofficial translation provided by the CNIL.

¹⁰ *Rapport de la Commission informatique et liberté*, dir. B. TRICOT and P. CATALA, La documentation française, 1975.

of this patchwork piece of legislation deals with employee's rights and liberties¹¹. Meanwhile, these articles had a major purpose. Their enactment has been preceded by an important work of a Commission¹² that aims to protect employees' privacy and personal information from employer's power¹³. Those 5 articles have been codified in the "*Code du travail*" (Labor Code) and, symbolically, they were placed among the firsts in the new Code voted in 2008.

Act n°78-17 of January 6, 1978 and Act n°92-1446 of December 31, 1992 have different scopes. The first Act applies when anyone processes personal information, be it the employer or anybody else¹⁴. The second Act applies when an action of the employer creates a danger for the employee's rights and liberties. In addition, even though both Acts deal with the protection of the employees' personal information and privacy, they each develop different protection mechanisms. We should therefore examine the Information Technology, Data files and civil Liberties Act (i) and the special provisions of the Labor Code separately (ii).

i) Protection by the Information Technology, Data files and civil Liberties Act

When the employer uses a technology in order to collect or save personal information, he must comply with several conditions, enumerated in the 1978 Act¹⁵, and he must also perform some formalities, like notifying the processing of personal data to an independent administrative authority or obtaining its agreement¹⁶. If these requirements are infringed, criminal penalties are provided for¹⁷. In practice, these sanctions are rarely applied¹⁸. The most useful remedies are the order to comply with the provisions of the Act and the prohibition to use the data illegally collected as evidence in a disciplinary action or

¹¹ Articles 25 to 29. Other articles of this law deals with various subjects about the employment relationship.

¹² *Les libertés publiques et l'emploi, rapport pour le ministre du Travail, de l'Emploi et de la Formation professionnelle*, dir. G. LYON-CAEN, La documentation française, 1992.

¹³ The Commission's researches were inspired by Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data of January 28, 1981 and by Act n°78-17 of January 6, 1978 on Information technology, Data files and civil liberties.

¹⁴ Article 2 of the Act states that it shall apply to any processing of personal data. Processing of personal data "means any operation or set of operations in relation to such data, whatever the mechanism used, especially the obtaining, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction".

¹⁵ Article 6 states that "Processing may be performed only on personal data that meet the following conditions : 1° the data shall be obtained and processed fairly and lawfully; 2° the data shall be obtained for specified, explicit and legitimate purposes, and shall not subsequently be processed in a manner that is incompatible with those purposes (...); 3° they shall be adequate, relevant and not excessive in relation to the purposes for which they are obtained and their further processing; 4° they shall be accurate, complete and, where necessary, kept up-to-date (...) 5° they shall be stored in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed". Article 7 provides that "Processing of personal data must have received the consent of the data subject or must meet one of the following conditions: 1° compliance with any legal obligation to which the data controller is subject; 2° the protection of the data subject's life; 3° the performance of a public service mission entrusted to the data controller or the data recipient; 4° the performance of either a contract to which the data subject is a party or steps taken at the request of the data subject prior to entering into a contract; 5° the pursuit of the data controller's or the data recipient's legitimate interest, provided this is not incompatible with the interests or the fundamental rights and liberties of the data subject".

¹⁶ About these formalities, see Articles 22 to 31 of the 1978 Act.

¹⁷ Article 50 of the 1978 Act, which refers to Articles 226-16 and seq. of the "*Code pénal*" (Criminal Code).

¹⁸ C. BLOUD-REY, "Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles?", *Recueil Dalloz* 2013, pp. 2795-2801, pt. 20.

a lawsuit.

The French data protection authority, called the *CNIL*, which is an independent administrative authority, plays a major role in the enforcement of the Act. The *CNIL* has two missions¹⁹. Its members and officers control if the “data controller”, namely the employer who processes of personal data, complies with the law. Therefore, a worker who faces difficulties about his personal data may submit his case to the *CNIL*. Nevertheless, the action of the *CNIL* is not significant on this point. The *CNIL* has got only limited prerogatives: in case of minor violation, the commission may send formal notifications and impose financial sanctions, but in case of major violation, it falls under the jurisdiction of the public prosecutor and the criminal courts²⁰. Moreover, the *CNIL* doesn't have sufficient resources. In 2012, the commission was composed by 171 members who had to deal with more than 6000 complaints. As a small organization, the *CNIL* cannot face all the problems generated by the enforcement of the 1978 Act. Above all, the *CNIL* doesn't consider the repression of prohibited behavior as its major mission. Therefore, the most appreciable impacts of *CNIL*'s activity might be actually linked to his second mission, that is the advice given to the companies, the employees and the citizens. With its “Deliberations”²¹, the *CNIL* contributes to regulate the use of new technologies. Even if these “Deliberations” are not compulsory, this “soft law” has a substantial influence on the legal practices, especially because members of the *CNIL* may give an opinion right away without having to wait for litigation. In a word, the *CNIL* is nowadays more an organization that elaborates a doctrine on the topic of personal information and privacy protection than an authority that controls the behavior of the employer.

Within the firm, the action of the *CNIL* is relayed by the personal data protection officer, called the “*Correspondant Informatique et Liberté*” (*CIL*). That is worth noticing that the 1978 Act does not give a significant role to the traditional checks and balances: trade unions and elected staff representatives are ignored. This choice to create a new institution within the firm can be questioned²². The *CIL* has to control the employer's behavior²³ but in order to accomplish this task, he needs to display many qualities: computer skills, good knowledge of the law and of the firm's organization as well as a patent independence from his head-manager. This collection of qualities is hard to find. In addition, the legislative has not provided the *CIL* with a status similar to the status of employee representative bodies. The *CIL* is most of the time an employee of the firm and is not granted legal protection against the employer. In practice, the *CIL* is able to propagate the doctrine of the *CNIL* rather than control the action of the employer. Consequently, compliance of the practice with the Information technology, data files and civil liberties Act can't be guaranteed.

ii) Protection by the Labor Code

The protection created by the 1992 Act is only relevant when workers' liberties are in danger. For instance, the rules apply when an employer plans to introduce a close circuit

¹⁹ Article 11 of the 1978 Act.

²⁰ It shall be note that this situation is evolving since a few years: the *CNIL*'s sanctioning power is constantly reinforced.

²¹ A “deliberation” is an interpretation of the law and a recommendation about its implementation.

²² R. De QUENAUDON, « La cote mal taillée du salarié correspondant à la protection des données à caractère personnel », *Revue droit du travail* 2006, p. 32.

²³ Article 24 of the 1978 Act.

television (CCTV) in the firm²⁴ or when an employer takes an individual decision based on the employee's privacy.

In this situation, the employer must demonstrate that the interference with employee's rights and liberties is justified by a legitimate aim and is proportionate to that aim²⁵. In many cases, he must also comply with a disclosure duty²⁶.

The most important civil remedies are the nullity of the employer's decision, the award of damage and the impossibility for the employer to use information illegally collected as evidence. Criminal penalties may also be imposed to the employer²⁷, but these sanctions are in practice rarely adopted.

The enforcement means of the Act n°92-1446 of December 31, 1992 are more traditional than those of the Act n°78-17 of January 6, 1978. If the Act is infringed, the workers could refer to the civil judge - in case of an individual decision or if an employee has suffered from a personal damage - or to the administrative judge - in case of a decision concerning all the employees -. On the top of the judicial system, the rulings of the two highest civil and administrative courts, the *Cour de cassation* and the *Conseil d'Etat*, contribute to define the meaning of this legislation regarding the development of new technologies or the use of new management methods.

Within the firm's premises, a representative elected by other employees, called the "*Délégué du personnel*" (DP), plays the most important role²⁸. The DP is not able to veto the employer's decision. However, he could question the employer about his aim and methods. If the DP is not convinced by the employer's arguments, he can refer to a judge by a summary procedure²⁹.

Voting the Act n°78-17 of January 6, 1978 and the Act n°92-1446 of December 31, 1992, the French legislative has created a dual protection system. The criteria developed for the application of the two acts are quite different. That's why, in many cases, the two texts shall be applied together. In such situations, both the *CNIL* and the judge have to ensure that the employer's action complies with the provisions of the law.

This dual organization may change if the proposal of the European Commission to modernize the directive 95/46 is adopted.

2) A "Europeanized" protection

The impact of the European instruments on the legal protection of employee's personal information and privacy has been increasing for many years. The incidence of the European Convention on Human Rights and of the Convention 108 is rather indirect. Those texts are often mentioned by the judges, the *CNIL* and the legal literature to justify their reasoning and solutions. The impact of the directive 95/46/EC of October 24, 1995 is easier to find out. This Directive has been implemented in France in 2004 in the Information Technology, Data Files and Civil Liberties Act³⁰. By this implementation, the

²⁴ In this case, the 1978 Act also applies.

²⁵ Article L. 1121-1 Labor Code.

²⁶ Article L. 1222-4 Labor Code provides that « employee's personal information must not be collected by a device that has not been previously brought to his attention ».

²⁷ Article 226-1 to 226-7 Criminal Code. These sanctions apply if the employer has illegally collect or use personal information about the employee.

²⁸ The "*comite d'entreprise*", a group of representative elected by the workers shall also be consulted in many cases.

²⁹ Article 29 of the 1992 Act, now codified in article L. 2313-2 Labor Code.

³⁰ The modifications have been introduced by the Act n°2004-801 of August 6, 2004 relative to the

repressive powers of the *CNIL* have been reinforced and the *CIL* has been created. The Information Technology, Data Files and Civil Liberties Act has to be interpreted according to the directive now.

New changes may be done in the coming years due to European instruments. Modernization of the Convention 108 is in progress since 2010 and modernization of the directive 95/46 since 2012³¹.

The combination of these two projects will be interesting to follow. On the one hand, many countries are affected by the Convention 108. Therefore, a modernization of this Convention may have a larger impact. On other hand, the rules created by the directive 95/46 are more efficient, because the implementation of its provisions is made under the control of the Commission and the European Court of Justice. It may also be easier to have cooperation between the supervisory authorities within the EU.

Having regards to the French system, the proposal of the Commission seems to modify the missions of the supervisory authorities, which would have in the future more powers in the repression of law infringements. Such evolution would impose a significant change in the organization and the action of the *CNIL*. Until now, the *CNIL* has always preferred handling pedagogically than punishing breaches of law³².

II. The balances of interests

Various methods are used to strike a balance between the interests of the employer and those of the employees. If, like in other countries, the proportionality principle plays a seminal role, other approaches are sometimes developed. Once explained the balance achieved when the employer seeks to obtain employee's personal information (A), the solution adopted when the employer wants to make a decision related to the personal life of the employee will be set out (B).

A. The collect of the employees' personal information

When the employer seeks to collect personal information, the guiding principle of the French law is quite simple: the action of the employer must have a legitimate aim and the interference with employee's liberty must be proportionate to this purpose.

Article L. 1121-1 of the Labor Code provides that "no one may restrict personal rights nor individual or collective liberties if this restriction is not *justified* by the nature of the work to be performed and *proportionate* to the aim pursued" and article L. 1222-2, al 2 of the Labor Code states that the information requested from an employee "must have a *direct* and *necessary* link with the evaluation of his professional skills". In addition, Article 6 of the Information Technology, Data Files and Civil Liberties Act provides that the personal data "shall be obtained for specified, explicit and *legitimate* purposes..." and "shall be adequate, *relevant and not excessive* in relation to the purposes for which they are obtained and their further processing...". Even if the texts are drafted in different ways, they have a common thread: the decision of the employer shall be legitimate and

protection of individuals with regard to the processing of personal data and modifying Act n°78-17 of January 6, 1978.

³¹ On this theme, see N. MARTIAL-BRAZ, J. ROCHFELD, E. GATTONE, "Quel avenir pour la protection des données à caractère personnel en Europe ? », *Recueil Dalloz* 2014, pp. 2788-2794 ; C. BLOUD-REY, "Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles ?", *Recueil Dalloz* 2014, pp. 2795-2801.

³² C. BLOUD-REY, pt. 12.

proportionate³³.

The legitimacy of the purposes is usually not difficult to prove. The employer can easily demonstrate that his action may protect the firm against thefts or may improve the company's performance³⁴. The key concept in order to strike a balance between the interests is therefore the proportionality principle. The proportionality of the interference with employee's liberty is assessed on a case by case basis. This approach gives a central role to the case law. That's why we could regret that there are only a few judgments on this topic.

B. Decision related to the personal life of the employee

When the employer seeks to make a decision related to the personal life of the employee, the French legislation tries to strike a balance by defining a principle and some exceptions³⁵. The proportionality test is less important here.

The principle is that the employer has to do "as if" he ignores everything about the worker's "personal life"³⁶. This guideline is reinforced by the rules regarding the prohibition of discrimination. The law establishes a list of themes that must not be taken in consideration by the employer³⁷. These criteria are, on one hand, the state of the person (health, color, sexual preference etc...) and, on the other hand, his/her activities (politics, trade-union or religious preferences). It shall be noted that, even if those rules are made in order to protect the employees' personal life, there is no contradiction with the protection of the firm's interests: such criteria are not involved in profit maximization.

Nevertheless, two exceptions may be invoked by the employer. The first is linked with the proportionality principle, but not the second.

The first exception is related to the employee's task within the firm. The employer is entitled to consider some aspects of the identity or personal life of the employee when

³³ This common thread is due to the impact of European instrument. Article 5 Convention 108 stated that "Personal data undergoing automatic processing shall be (...) b) stored for *specified and legitimate purposes* and not used in a way incompatible with those purposes; c) *adequate, relevant and not excessive* in relation to the purposes for which they are stored...". Article 6 § 1 Directive 95/46/EC of October 24, 1995 provided that "Member States shall provide that personal data must be (...) (b) collected for *specified, explicit and legitimate purposes* and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards ; (c) *adequate, relevant and not excessive* in relation to the purposes for which they are collected and/or further processed...".

³⁴ Advice of the *CNIL* may help employers and employees to know if an aim is legitimate or not. For example, Article 2 Deliberation 2006-067 of March 16, 2006 enumerates purposes relevant to monitor employees with GPS.

³⁵ See M. DESPAX, « La vie extraprofessionnelle du salarié et son incidence sur le contrat de travail », *JCP* 1963, I, 1776 ; P. ADAM, « Sur la vie personnelle : cinquante ans après Despax », *Revue de droit du travail* 2012, pp 100-104.

³⁶ The highest civil Court distinguishes the "protection of privacy", which is a civil law concept, and the "protection of the personal life", which is a labor law concept. By using the term "personal", the judges refer to everything that is not "professional". Thus, an employer is not allowed to take any disciplinary measure against the worker based on the worker's behavior outside the firm, even if many people have observed the worker. This behavior might not belong to the "privacy" in the strict sense of the civil law but remains "personal" – and not "professional" – in the sense of the labor law. (On this distinction between « privacy » and « personal life », see Ph. WAQUET, "La vie personnelle du salarié", *Droit social* 2004, pp. 23-30 ; A. LEPAGE, « La vie privée du salarié, une notion civiliste en droit du travail », *Droit social* 2006, pp. 364-377).

³⁷ Article L. 1132-1 Labor Code.

there is a close link between the employee's work and these elements. This exception has a broad scope, but is expressed differently in the law depending if the decision of the employer is favorable or unfavorable to the employee.

For new job opportunity (as recruitment or promotion), the employer can consider the employee's features if they constitute "a genuine and determining occupational requirement, provided that the objective is legitimate and the requirement is proportionate"³⁸.

For a disciplinary action against a worker, the employer shall demonstrate that the behavior of the employee is "an infringement of an obligation related to his mission in the firm"³⁹. Only very few situations satisfy this criteria. The most frequent case where an employer seeks to blame an employee because of the violation of a professional obligation is the revocation of his driving license while the worker needs this license to accomplish his job. Meanwhile, both the *Cour de cassation* and the *Conseil d'Etat* decide that the dismissal of an employee because of the revocation of his driving license does not have to be disciplinary⁴⁰.

The second and most important exception is linked to the global functioning of the company. When an important disorder within the firm results from the behavior of an employee - situation called in the case law as an "objective and characterized disorder" - the employer is allowed to take a non-disciplinary decision against the worker⁴¹. A decision of the *Cour de cassation* of May 18, 2007 illustrates this situation. In this case, an employee received a newspaper of a swinger's community at his professional postal address⁴². The employer wanted to sanction the employee, but the judges estimated that he could take only a decision based on the "disorder" created within the firm⁴³.

The balance between the interests of the employer and the interests of the employee is here found in the exceptional nature of this second exception. The personal life of an employee rarely causes significant damage to the company.

Finally, it should be noted that the employee's consent has not been important until now in the French law. This role may increase in the future, despite its questionable value, because of the subordination of the employee to the employer. If such evolution is adopted in French labor law, it will be necessary to clarify the relationship between the request of the employee's consent and the control of the legitimacy and proportionality of the employer's decision: are they alternative requirements or additional conditions? The last solution seems to be the most appropriate. Personal information and privacy are not only protected in the interest of the individuals. This protection also ensures that the rule of law and principles such as freedom of opinion and expression are respected. Therefore, the

³⁸ Article 4 of the Council Directive 2000/78/EC of November 27, 2000 establishing a general framework for equal treatment in employment and occupation.

³⁹ *Cour de cassation*, May 3, 2011, case n° 09-67464 ; *Conseil d'Etat*, December 15, 2010, n°316856.

⁴⁰ *Cour de cassation*, May 3, 2011, n°09-67464. In this case, in accordance with the second exception, the employer is only entitled to take a decision based on the disorder created by the employee's behavior within the firm.

⁴¹ *Cour de cassation*, January 22, 1992, case n°90-42517 ; *Cour de cassation*, March 9, 2011, case n°09-42150.

⁴² *Cour de cassation*, May 18, 2007, case n°05-40803.

⁴³ In another decision of March 9, 2011, the court reaffirmed the principle that only a dysfunction within the firm could justify the employer's decision (*Cour de cassation*, March 9, 2011, case n°09-42150). It shall be noted that in such cases, the employer never tries to collect information or to be informed about the worker's life.

consent of the individual should remain insufficient to justify the employer's action. The control by a judge of the legitimacy and proportionality of the employer's decision also seems to be required.

III. Personal information and privacy protection in the employment relationship

Employee's personal information and privacy is protected in the hiring process (A), during the employment relation (B) and after the termination of the employment contract (C).

A. Personal information protection in the hiring process

About the hiring process, the first point that must be paid attention to is the prohibition of employer's decisions based on non-professional criteria (1). Then, a gradation in the protection of the employee's personal information and privacy is brought into focus (2).

1) Control of the employer's decision

The legislative aims at avoiding employer's decisions based on non-professional criteria. Many provisions are inspired by this purpose.

Article L. 1221-6 of the Labor Code, created by 1992 Act, provides that "information requested (...) to the job applicants could not have any other aim than assessing their ability to hold the job offered or their occupational functioning. The information must have a direct and necessary link with the job offered". Article L. 1132-1 of the Labor Code also prohibits any decision excluding applicants based on a list of characteristics, like their origin, sex, morality, sexual orientation, age, marital status or pregnancy, genetic characteristics, political opinions, etc... However, this article is not applicable when the employer could demonstrate that this feature constitutes "a genuine and determining occupational requirement" for the job⁴⁴. Article 8 of the Information Technology, Data Files and Civil Liberties Act should also be taken into consideration. This article prohibits processing of sensitive categories of data, as racial origins and political opinions. Lastly, article R. 4624-11 of the Labor Code provides that the medical fitness to do the proposed job must be examined only by an occupational health doctor.

2) Gradation of the protection

In accordance with the provisions stated above, it seems that three categories of personal information could be identified. They do not show just one but different levels of protection.

For a first group of information, prohibition of collecting inquiries about the workers is not absolute. The employer is allowed to collect information if he could demonstrate that it is proper and reasonable to consider this to choose the best applicant. For the employer and the employees, the core question is to assess whether the information is relevant or irrelevant for a job in accordance with article L. 1221-6 of the Labor Code. The advice of the *CNIL* may help the actors but not solve all the problems⁴⁵. Will an applicant looking for

⁴⁴ Article 4 Directive 2000/78/EC of November 27, 2000.

⁴⁵ In his "Guide pour les employeurs et les salariés" (Guide for employers and employees), that can be found on the internet address of the *CNIL* (www.cnil.fr), a list of prohibited questions is drawn up (page 9 of the

a job since months or years refuse to answer a question if the employer thinks that the question is relevant to appreciate his professional skills? Article L. 1132-1 of the Labor Code, and Article 8 of the Information Technology, Data Files and Civil Liberties Act avoid this ambiguity for some aspects of the life and identity of the employee. These provisions enumerate characteristics that must not be taken in consideration by the employer, except for some specific organizations. For instance, a question about the religion of the employee is only relevant in religious organization. A question about the political opinions is only relevant when the applicant seeks to obtain a job in a political party. This clarification reinforces the position of the employee.

Beside this category of information, we find situations where data are relevant for the job although employer's knowledge of this information must be avoided. This dilemma explains the specific mechanism regarding applicant's health. Even when it is necessary to appreciate if an individual is medically fit for a job, an employer is not entitled to ask a candidate about his health. The mission is the hands of a third party, the occupational health doctor.

In the third and last category, prohibition of processing personal information is absolute because in all cases, no link can be found between the job and the candidate's characteristics. For instance, the employer is never allowed to reject a candidate because of his skin colour⁴⁶, nor allowed asking anyone for his password of social networking.

This gradation in the protection of employees' personal information and privacy has two explanations. First, it seems that the link between some information and the individual is sometimes so close that some special protection is required. In other words, such information doesn't just belong to the "privacy" of the individual, but also to his "intimacy", which is the core of privacy. For example, the link between the individual and his body is so particular and so strong that it requires a specific protection. Second, global issues justify more intensive attention from the legislative power too. For example, collecting political opinions or trade-union activities is mentioned by article L. 1132-1 of the Labor Code and by Article 8 of the Information Technology, Data Files and Civil Liberties Act because such information doesn't only deal with the privacy of the employees. Freedom of opinion and freedom of association may also be at stake.

In conclusion, it may be added that both applicants and elected staff representatives have to be informed by the employer about the technologies or methods he will use to appreciate the professional skills of the candidate⁴⁷. With this transparency's duty, the legislative hopes that a control of the hiring process will be made within the firm. Unfortunately, despite these provisions, the application of the rules is not fully satisfying. Recruitment is considered basically as a choice of a personality and employers often take into account criteria prohibited by the law. Nevertheless, this legislation seems to preserve the candidate's dignity by avoiding major abuses during the hiring process.

B. Personal information and privacy protection during the employment relations

In order to give an exhaustive panorama of the rules regarding the employment

Guide). We doubt that most employers do comply with this list. Do the employers agree with the opinion of the *CNIL* that the "association's activity" of the applicant is not relevant to appreciate his professional skills?

⁴⁶ The principle confirmed by the labour law in 2012 (article L. 1221-7 Labor Code), is to preserve as long as possible the candidate's anonymity in the hiring process.

⁴⁷ Article L. 1211-8 Labor Code and article L. 2323-32 Labor Code.

relationships, two kinds of actions could be distinguished: those that aim at or result in collecting personal information about the worker (1) and those concerning an employer using his knowledge about the personal life of the employee (2).

1) The collect of personal information

There are different ways for an employer to collect information about a worker. The simplest is to ask directly the employee. The provisions are here the same than the ones that apply during the hiring process. Pursuant to the Labor Code, “information requested to an employee (...) must not have any other aim than assessing his professional skills”⁴⁸.

The other actions have not been specified by the legislative. Following the distinctions used in criminal law⁴⁹, it seems relevant to separate to types of actions: the inspection of premises or objects within the firm (1) and the surveillance of worker’s activity (2).

i) Inspection

By using the term “inspection”, we refer to the action where an employer searches to identify the content of an object or the content of a closed place: for instance, the inspection of the desk of an employee, the inspection of his computer or the inspection of his e-mails.

Historically, the first decision of the highest civil court about inspection was the decision “*Nikon*” in 2001⁵⁰. The right of privacy was mentioned in this ruling but the judges acknowledged that they were not sure about the opportunity of their solution. In 2005, the court adopted another position with the decision “*Klajers*”. This new solution is less protective towards the employees’ interests⁵¹. Nowadays it is necessary to identify the realm to which the objects or premises inspected belong in order to determine the rules that the employer must comply with. Three realms may be distinguished.

Some elements seem to be strongly protected. For the search of the personal bag of the employee, the employer shall of course demonstrate that the interference with employee’s privacy has a legitimate aim and is proportionate to that aim but, except in case of emergency, he must also prove that the worker consented to this search⁵². The reason for this specific legal regime remains unclear: is this element stronger protected because it belongs to the employee’s “intimacy” realm or because it’s the employee’s legal property? The legislation and the case-law did not rule on this point, probably because this kind of claim is uncommon.

On the opposite, the protection of an object that belongs to the “professional” realm⁵³ is very weak. Indeed, the employer can conduct the inspection of the object without complying with substantive or procedural rules.

⁴⁸ Article L. 1222-2 Labor Code.

⁴⁹ In the Criminal procedure law, one must distinguish, on one hand, operations of “*perquisition*” and “*fouille*” (article 94 and seq. of the “*Code de procédure pénale*” – Code of Criminal Procedure) and, on other hand, operations of “*interceptions de communication*” and “*captation d’images et de paroles*” (Article 100 and seq. Code of Criminal Procedure ; Article 706-96 and seq. Code of Criminal Procedure). “*Perquisition*” means search of an enclosure place and “*fouille*” means body search or search of an object. “*Interpection*” and “*captation*” refer to the operation where sounds or images are recorded.

⁵⁰ Cour de cassation, October 2, 2001, case n°99-42942.

⁵¹ Cour de cassation, May 17, 2005, case n°03-40017.

⁵² Conseil d’Etat, July 11, 1990, case n°86022. Cour de cassation, February 11, 2009, case n°07-42068. The judges watch carefully the consent of the employee. The employer must inform the employee about his right to refuse the inspection and about his right to require the attendance of a witness.

⁵³ Or the “not personal” realm as stated by the Cour de cassation.

Finally, about things falling under the employee's "personal" realm, the judges, inspired by criminal law, have decided that the employer has to warn the employee about his inspection⁵⁴. Although the employee's agreement is not required, the worker has the possibility of discussing with the employer the opportunity of this inspection. This rule has one exception: in case of emergency⁵⁵, the employer is entitled to search for anything that belongs to the personal realm of the employee without telling him. For instance, this exception applies when the detection of a computer virus that could make important damage to the firm's intranet requires searching into the personal files of an employee immediately. It should be also noted that it remains undecided if the action of the employer must or not have a legitimate aim and be proportionate to that aim. According to article L. 1121-1 of the Labor Code, the employer should demonstrate that his action complies with these two requirements. Nevertheless, there is no decision of the *Cour de cassation* about this.

This outline of the rules regarding inspection pointed out that the legal characterization is decisive: opening a file on the professional employee's computer or reading a mail received by the employee at his professional address requires the employer to determine whether the box, file and mail belong to the "professional" or to the "personal" realm. The judge uses of a formal criterion: only if the employee has characterized the box, files or mail as "personal" are these elements related to the personal realm⁵⁶. By comparison, neither the file called "my documents"⁵⁷, nor the file identified by the employee's initials⁵⁸ belong to the personal realm. A USB stick connected to the professional computer of the employee also belong to the professional realm⁵⁹. In these cases, the employer is therefore allowed to conduct a thorough search without having to warn the employee.

Rulings concerning inspection are open to criticism. The criterion used by the *Cour de cassation* in order to distinguish « professional » and « personal » realms is controversial. Moreover, the fact that an employer may inspect personal objects or premises without the consent of the employee or without having to demonstrate that this inspection is justified by a legitimate aim and is proportionate to that aim is questionable. The employer should not have more leeway to collect personal information about the employees than the police do⁶⁰. At least, comparison between labor law and criminal law suggest a proposal: privacy of the citizen against police's inquiries is protected by distinguishing in some situations preventive and repressive action⁶¹. Why not applying such criterion in the employment context⁶²?

⁵⁴ Cour de cassation, May 17, 2005, case n°03-40017.

⁵⁵ "Particular risk or event" according the case law (Cour de cassation, May 17, 2005, case n°03-40017).

⁵⁶ In this situation, the employer can contest this personal use of professional instruments. If the use is abusive, the employer is entitled to punish the employee. Nevertheless, he is not entitled to disqualify the element from the "personal" to the "professional" realm.

⁵⁷ Cour de cassation, May 10, 2012, case n°11-13884.

⁵⁸ Cour de cassation, October 21, 2009, case n°07-43877.

⁵⁹ Cour de cassation, February 12, 2013, case n°11-28649.

⁶⁰ According to article 76 Code of Criminal Procedure, the consent of the concerned citizen is required for a police inspection, except if this inspection is done under the authorization and control of the judge or in the special case of "*enquête de flagrance*" (article 53 and seq. Code of Criminal Procedure).

⁶¹ Conseil d'Etat, May 11, 1951, *Dame Baud*, *Recueil du Conseil d'Etat*, p. 265 and *Tribunal des conflits*, June 7, 1951, *Époux Noualek*, *Recueil du Conseil d'Etat* p. 636. This distinction is, for instance, used about body

ii) Surveillance

By using the term “surveillance”, we refer to the action where an employer seeks to know employee’s activity at a certain point of time or in a certain location. For instance, the employer surveys his employees by using a CCTV device or a global positioning system⁶³.

Historically, the first important rules about surveillance came from case law. Cases of employees who had been subject to disciplinary actions have been brought to the judges. These employees denied the lawfulness of the evidence adduced by the employer, claiming that the monitoring system was unfair. With the emblematic decision “*Neocel*” dated November 20, 1991⁶⁴, the *Cour de cassation* forced the employer to comply with a disclosure duty when using a surveillance device. A year later, by the 1992 Act, the legislative expanded on this ruling and established the conditions under which the employer may control the employees. In addition, *CNIL*’s deliberations often give instructions about the use of such devices. Most of the time, *CIL*, members of Trade Unions and staff representatives who have a doubt about the lawfulness of a surveillance system refer their case to the *CNIL* and not to the judge.

The current rules are the following: as for the inspection, three kinds of situations should be distinguished.

First of all, the employer is never entitled to monitor employees outside working hours and outside the working place. An employer spying on his employees at home will be guilty of a violation of privacy and will be punished in accordance with the criminal law⁶⁵ and civil law⁶⁶.

The situation is different when the employer monitors his employee in order to control the quality of work.

In such a case, he has to demonstrate that this monitoring complies with the substantive rules from article L. 1121-1 of the Labor Code. According to this text, the use of a technological system to control the employees’ activity must have a legitimate aim and be proportionate to that aim. Although there is no problem with this first requirement⁶⁷, compliance with the second condition is harder. For instance, using GPS in order to monitor employee’s activity is disproportionate if the employment contract recognizes to the employee a large autonomy in his work’s accomplishment⁶⁸. Unfortunately, there are so far few decisions regarding this condition.

In addition to these substantive rules, the employer has to comply with procedural guarantees. Using a surveillance system is only permitted after having informed the staff representative⁶⁹ and the employees⁷⁰. One can expect that an employee who knows he is monitored will act in a way that protects his privacy. By the way, the scope of this

search. In case of preventive action, the policemen are only entitled to palpate the body of the individuals, but are not allowed to conduct an authentic body-search.

⁶² Such a distinction was used in an administrative text, the Circulaire DRT n° 5-83 of March 15, 1983. Nevertheless, the judges didn’t refer to this distinction in labor law.

⁶³ We exclude here the direct surveillance, without the help of technologies.

⁶⁴ Cour de cassation, November 20, 1991, case n°88-43120.

⁶⁵ Article 226-1 and seq. Criminal Code.

⁶⁶ Article 9 Civil Code.

⁶⁷ It is of course legitimate to control the quality of work.

⁶⁸ Cour de cassation, November 3, 2011, case n°10-18036.

⁶⁹ Article L. 2323-32 Labor Code.

⁷⁰ Cour de cassation, November 20, 1991, *Neocel*, case n°88-43120 and Cour de cassation, May 22, 1995, case n°93-44078. Article L. 1222-4 Labor Code.

obligation to inform is stronger than in other European countries: the employer is never entitled to use hidden cameras. By comparison with the criminal law, such a rule seems to be justified. A judicial authorization is required to entitle the police to use a hidden data-collecting technique⁷¹. It is appropriate that the employer doesn't have more prerogatives than the police: his mission is not to conduct criminal investigation within the firm.

The third and last situation concerns the employer using a surveillance system for other purposes than controlling employee's work.

In this case, the monitoring system has to pursue a legitimate aim and must be proportionate to that aim. According to the *CNIL*, if an employer uses CCTV in order to prevent thefts caused by the customers inside the firm, he cannot use this monitoring system on the floors where the customers are not allowed to go. If he does, the employer's behavior is considered as disproportionate⁷².

The scope and incidence of the disclosure obligation are open to debate. First of all, the *Cour de cassation* denies the employer the right to use a monitoring system in order to control the activity of the employee when it was initially dedicated to another aim⁷³. On the other hand, the employer does not have to comply with a disclosure duty if he uses a CCTV in premises where the employees are not allowed to go⁷⁴.

2) The use of personal information

For the employer, his knowledge about employee's personal life may have an incidence on three categories of actions.

First, the employer could have the intent to make a management decision such as dismissal, disciplinary sanction or promotion, based on the personal life of the employee. In this case, as explained above, the principle is that the employer is not entitled to do so. By exception, the behavior of the employee could be taken in consideration only if it has caused an "objective and characterized disorder" within the firm or if it is "an infringement of an obligation related to his mission in the firm"⁷⁵.

Secondly, the employer may wish to reveal information regarding the personal life of an employee to other workers or outside the firm. Such a revelation is prohibited for it breaks the protection of privacy according to article 9 Civil Code.

Lastly, the employer may want to record personal information about his employees in a file. In this case, information is transformed into "data" and the information technology, data files and civil liberties Act applies. Therefore, the processing of personal data is entitled only if the employer has a legitimate aim and if the storage is proportionate to that aim. In addition, the employee is allowed to access to his personal data and, if these data

⁷¹ Articles 706-96 et seq Code of Criminal Procedure.

⁷² *CNIL*, April 16, 2009, Deliberation n°2009-201.

⁷³ *Cour de cassation*, November 3, 2011, case n°10-18036 (a GPS system may not be used by the employer for other purposes than those declared to the *CNIL* and brought to the attention of the employees"). We should nevertheless note that in a previous decision, less important, the solution was quite different. In this decision, dated February 2, 2011 (case n°10-14263), a CCTV system had been implemented in a casino for the safety of people and property. A barman was dismissed, because of major faults committed on his job : video shows that he didn't collect revenue for many drinks. He contested the right for the employer to adduce the video record as evidence. The *Cour de cassation* rejected his demand, meanwhile the employer didn't demonstrate that he had informed the employees that he will use CCTV in order to control their activity.

⁷⁴ *Cour de cassation*, January 31, 2001, case n°98-44290.

⁷⁵ On this point, see "II. The balance of interests".

are inaccurate, a correction has to be done. The *CNIL* sometimes reminds these rights in the scope of the employment relationship⁷⁶.

C. Personal information and privacy protection after the employment relations

After the dismissal of the contract, the employee has to face two sorts of problems regarding his personal information and privacy.

The transfer of data between the former and the prospective employer is one of these problems. On this topic, the French Labor Code states that “information about a person applying for a job cannot be collected by a device that has not been brought to his attention”⁷⁷. Therefore, the application of this rule is tricky. The breach of the law is hard to prove. In addition, a candidate has few incentives to sue the employer when he has been illegally excluded from the hiring process. Even if the irregularity of the process is recognized, the judges will not force the employer to recruit the candidate.

The course of the “individual file” of the employee proceeded by the former employer is another problem. In many firms, information about the employee’s career (*curriculum vitae*, mutations, promotions, disciplinary sanctions etc...) is gathered in a file. This information is used by the employer during the employment relationship⁷⁸. After the dismissal of the contract, the employer often keeps some documents in order to prove his assertions in case of judicial action initiated by the employee. The rules relating to these files are still fuzzy⁷⁹, especially about the duration of the storage. A clarification of the legal regime of this file would be convenient.

IV. Conclusion

As a conclusion, three points should be brought into focus about the protection of employee’s personal information and privacy in France.

The framework of this protection, especially about the rules governing the action of the employer, seems to be quite sufficient. Basis assertions, as the prohibition of decisions based on employee’s personal life or the double test of and proportionality required when an employer seeks to collect personal information, attract a broad consensus. The remaining problems are due to the vagueness of the law or result of the hardness to find the appropriate yardstick. For instance, there is no discussion about the opportunity to distinguish “professional” life and “personal life”, but the choice of the pertinent criterion remains contested.

⁷⁶ For instance, the deliberation n°02-001 dated January 8, 2002 about « Automated processing of personal information concerning implementation in the workplace for the management of access to premises, schedules and catering » states the right for the employee to access to his personal data saved in this file.

⁷⁷ Article L. 1222-4 Labor Code.

⁷⁸ The employer doesn’t use this information only for his own interest, but needs it sometimes to comply with the law. For instance, the employer has to know the employee’s address to send him his pay slip. When an additional health insurance or complementary welfare and pension scheme exist in the firm, its management also requires information about the employee, like his marital status, the number of dependent children, the beneficiaries of the funds.

⁷⁹ By comparison, the rules in the public sector have been specified by the law. The article 18 of the Act n°83-6354 of July 13, 1983 about the rights and obligations of the employees in the public sector claims that all administrations have to possess an individual file for each employee. The contents of this file and its use are determined by the law. On this theme, see also Article 26 of the Staff Regulations of Officials of the European Union and the Conditions of Employment of Other Servants of the European Union.

On the law enforcement topic, discussions are more intense.

Within the firm, the role and the status of the *CIL* should be reviewed. We doubt that the *CIL* is actually able to control employer's activity. Therefore, the articulation with traditional check and balances system within the firm should be reexamined, in the direction of a closer link with the staff representative. At least, some better legal protection of the *CIL* remains indispensable.

The role of both the *CNIL* and the judge should also be clarified. According to the last European Commission proposal, the role of the *CNIL* may evolve and be more repressive. Such evolution will make a major change in the organization of the *CNIL* necessary and question the allocation of competences between the *CNIL* and the judge.

In addition, one can suspect that the articulation between a protection by the individual and protection by a third party will be disputed in the coming years. That points out the role of the consent of the employee and its consequences. We reject the idea that the individual is the only one concerned by the protection of personal information and privacy. This question is again of paramount importance for freedom of opinion and expression of the individuals⁸⁰. That's why the employer should in every case act for a legitimate aim and in a proportionate way. Only an independent authority should estimate if the employer complies with these requirements.

Finally, it seems that the French law will have an important choice to make in the next few years between a "passive" and an "active" protection of the personal information and privacy.

By "passive protection", we refer to a system under which the decisions taken by the employer cannot be linked with the personal life of employees. For instance, an employer should not transfer an employee because of his sexual orientation.

By "active protection", we refer to a legal system under which the employer has to consider the personal imperatives of the employees, for instance childcare issues, when taking a decision, as a transfer⁸¹.

It raises a tricky dilemma. Of course one can state, as the French legislation does, that the employer has to take into consideration the personal characteristics of the employees only in some cases. However, once personal information falls into the employer's knowledge, it is difficult to prevent the employer from a later use of this information.

The trade-off between passive or active protection is therefore determining, since it has a decisive impact on the elaboration of the law about the gathering of personal information.

⁸⁰ On this point, see the utmost decision "Voklzählungsurteil" of the German Constitutional Court dated December 15, 1983.

⁸¹ On this point, it should be noted that Act n°2013-504 of June 14, 2013 provides that, in case of concluding a specific collective bargaining, called "accord de mobilité interne", the employer shall comply with a preliminary dialogue phase. In this phase, the employee may bring to the attention of the employer their personal and familial duties and the employer shall take in consideration these duties (Article L. 2242-23 Labor Code).