Mathilde Houet-Weil
Avocat (Paris)
Attorney at Law (NY)
Weil & Associés
26 avenue de la Grande Armée
75017 Paris, France
mhweil@weil-paris.fr

American Bar Association
Labour and Employment Law Section, International Committee, Berlin, May 2011

DATA PROTECTION AND PRIVACY IN THE WORKPLACE – EUROPE AND FRANCE

The right to privacy is a highly developed area of law in Europe. Europeans are vividly aware of the dangers associated with unchecked use of personal information, as learned from their experiences in World War II – fascist governments, and post-War - communist regimes, where disclosure of race, ethnicity or political views led to secret denunciations that caused many to be persecuted and assassinated. In the digital age, Europeans' mistrust of secret government files translated into a mistrust of corporate databases, and thus governments in Europe took decisive steps to protect personal information from abuses in the years following World War II.

This paper will discuss the following points in connection with the development of data protection and privacy in the European and French workplace:

1. Because of the above-mentioned historical and cultural background, data protection is more regulated in the European Union ("EU") than in the US. The European privacy legislation is regarded as even more rigorous than that found in many other areas of the world.
2. US companies who collect and process information relating to individuals in Europe, including employees, customers, and/or suppliers, should be aware of the different approach taken by member states of the EU with respect to data privacy in order to avoid the detrimental consequences of any non compliance.
3. France, where individual freedom is highly praised, is a bastion of workplace privacy. Article 8 of the *European Convention on Human Rights,* which is applicable in France, provides the "right to respect" for one's private and family life, his home and his correspondence, subject to certain restrictions**.** Article 9 of the *French Civil Code* further provides that everyone has the "right to respect" for his private life. Both provisions apply to employees in the workplace and during working time. As a result, monitoring of employees in France must not violate their right to privacy.

4. US companies with employees in France, who try to impose their world-wide social media policies on such employees, or ask them to "blow the whistle" on wrongdoings by fellow employees, may find that their social media policies and whistleblowing schemes that are valid in the US may not be as effective in France.
5. Finally, in France, the employee's right to privacy extends to conversations and communications which take place at work or within work systems. As a consequence, the collection and use in court of employee's emails and digital data is subject to strict prerequisites.

1. Personal data and privacy are broadly protected in the European Union.

In 1981, the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* was negotiated within the Council of Europe. Pursuant to this Convention, most EU member states enacted legislation concerning the automatic processing of personal data.

In order to avoid diverging data protection legislation amongst EU member states, the *Data Protection Directive*[1] (the "Directive") was passed in 1995. The Directive regulates the processing of "personal data", regardless of whether such processing is automated or not.

"Personal data" include emails and is broadly defined as "any information relating to an identified or identifiable natural person". Data is personal when someone is able to link the information to a person, even if the person holding the data cannot make this link. Some examples of personal data are: address, credit card number, bank statements, and criminal record.

Pursuant to the Directive, each member state must set up a supervisory authority, i.e., an independent body that will monitor the data protection level in that member state, give advice to the government about administrative measures and regulations, and start legal proceedings when data protection regulations have been violated. The majority of the supervisory authorities have released codes of practices with regard to the rights of the individual.

Interestingly, years before the Directive was passed, France had already adopted its current law[2], which created a data protection or supervisory authority, the *Commission Nationale Informatique et Libertés,* (the "CNIL") in 1978.

According to the Directive, the responsibility for compliance rests on the shoulders of the "controller", meaning the natural or artificial person who determines the purpose and means of the processing of personal data. The data protection rules are applicable not only when the controller is located within the EU, but also whenever the controller uses equipment situated within the EU in order to process data.

Personal data may be processed only under the following circumstances:

- the data subject has given his consent;
- the processing is necessary for the performance of or the entering into a contract;
- the processing is necessary for compliance with a legal obligation;
- the processing is necessary in order to protect the vital interests of the data subject;

[1] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[2] Law n° 78-17 of 6 January 1978 concerning information technology, files and civil liberties.

- the processing is necessary for the public interest; or
- the processing is necessary for the legitimate interests pursued by the controller or by the third party to whom the data is disclosed.

The European Commission is currently working on amending the Directive in a way that would reinforce the independence and harmonise the powers of national data protection authorities. The considered amendment is also for the purpose of addressing US social network companies, such as Facebook or Twitter.

Transfer of personal data within EU member states does not raise any particular issue since the transfer would occur between countries that apply a harmonized level of protection – although local regulations may differ from one another.

Transfer of personal data from an EU member state to a country outside the EU can only occur if that country provides an adequate level of protection. This is one of the issues US companies who have employees in Europe have to deal with in order to comply with European data protection legislation.

2. <u>US employers must comply with European data protection legislation for their workforce located in Europe</u>.

The Directive and its implementing legislation throughout the EU affect US employers who collect and/or process personal information about employees or potential employees in Europe.

The most important restriction for US companies under the Directive is the prohibition against transferring personal information out of Europe to countries that do not have adequate or equivalent protections for personal information. The US is not considered to be a country which offers adequate protection.

There are a few exemptions to that restriction, with respect to the US:

a. The data subject can consent to the transfer (although in some countries such as France, an employee is not deemed free to give such consent to an employer).

b. The US transferee of personal data can voluntarily agree to comply with the Safe Harbour principles. The Safe Harbour principles, negotiated between US representatives and the "Working Party"[3], allow US companies to register their certification if they meet the European Union requirements. Because certification is based on self-assessment, some critics have voiced concern as to the reliability of this certification.

c. Model clauses have been approved by the European Commission, which clauses can be added to transfer contracts to cover data protection safeguards.

d. "Corporate Rules" is a new approach that some large companies, such as G.E., have started to take which establishes corporate policies intended to deal with intra-group transfers. Any such proposed policies will require individual approvals by the European Commission.

[3] Also known as "Article 29 Working Party" because, as created in article 29 of the Directive, the Working Party gives advice about the level of protection in the European Union and non EU countries.

In sum, a US company that has employees in Europe must be careful about the information it obtains and controls about those individuals. If the data is to be transferred to the US or made available to individuals in the US electronically (even if the information technically resides on a server in the EU), the US transferees must meet one of the four above-mentioned exemptions to the prohibition against transferring such data to a country without adequate protections.

Moreover, if data is to be transferred from France to a non-EU country, a transfer request must be notified beforehand to the CNIL, explaining how data protection will be guaranteed. The transfer can only occur following authorization of the CNIL.

Otherwise, if the information remains in Europe and is not accessible from the US, the local entity must at least comply with that jurisdiction's legislation on data protection, typically involving:

i) registration with appropriate regulatory authorities;
ii) fair and lawful processing;
iii) collection of data only which is adequate, relevant and not excessive ;
iv) no retention of data for any longer than necessary for the purposes for which it is collected;
v) taking of appropriate steps to safeguard against accidental or unlawful loss;
vi) advising subjects about the information the data controller has about them, and the purpose of that collection;
vii) giving subjects the right to access and rectify information which the organization controls about them.

Violations of employee data privacy and non-compliance with EU regulations may have adverse implications, such as monetary fines for infringement, which fines vary from one EU country to another. Violations may also be used as a bargaining tool in negotiations on other workers issues. Non-compliance can result in bad publicity, which can damage share prices. Moreover, if a company violates personal data protections, it may see adverse consequences in any pricing discussions arising from the sale of a European subsidiary

Given the complexity of data protection regulations in the workplace with varying degrees of flexibility within Europe, US companies with operations in Europe should be prepared to not only create and enforce suitable policies but also to carry out internal proportionality checks as part of a more substantial privacy impact assessment. A unique definition of workplace privacy has not yet been developed in Europe, although there have been attempts to amend national data protection laws to this end.

Moreover, data protection must be taken into account by US practitioners and litigants that send discovery requests to companies based in Europe, which requests frequently call for the production of personal data about employees. A compromise must be found between a company's obligation to respond to US discovery requests and its obligation to comply with EU data protection laws. The European proportionality requirement is often inconsistent with the American practice of demanding "any and all" documents, even within a defined category.

3. <u>Privacy and employees monitoring are strongly protected in France.</u>

The right of the employee to dignity and therefore to a private life has been implemented into strong workplace privacy protections through the French Labour Code and through guidelines released by the CNIL. These regulations are strictly applied by the French Supreme Court.

Generally speaking, any activity that restricts employees' rights and freedom must be proportional to and justified by its purpose[4]. As a consequence, surveillance in the workplace, inherently suspicious as posing a threat to employees' privacy, must be transparent, proportional and justified. In all cases, the fundamental right of an individual's privacy must be balanced against the purpose for which the monitoring activities are being proposed.

Pursuant to the provisions of the French Labour Code, worker information can only be collected after prior advising and consulting of the employee representatives ("Works Council")[5]. An adverse reaction from the Works Council could significantly delay a project, and alternative solutions might need to be considered.

Any monitoring activities, and any email archiving, must be notified to the CNIL. When the information collected through surveillance and monitoring may qualify as personal, the employers must also notify the employees prior to installation and use of any surveillance or monitoring devices[6]. For instance, an Appellate Court rejected evidence collected using a Global Positioning System device embedded in a company car on the grounds that the employer had failed to notify this data processing activity to the CNIL and had not given proper notice to employees regarding the use of this device in company cars. As a consequence, the termination of an employee who had used the company car for personal reasons and committed serious traffic violations is found wrongful for lack of admissible evidence.[7]

With regard to internet monitoring, it is generally recognised that employees may use the internet for non-professional purposes, provided it does not affect their performance in the workplace (see 5.2. below). Upfront content monitoring of emails is not permitted in France, even if the employer has specifically prohibited non-professional emails in the workplace. For security purposes, some monitoring may be carried out, but always subject to Works Council consultation, and individuals must be informed about the possibility of such monitoring. If an employee's loyalty is in question, any consultation of emails sent or received by such employee must follow certain prerequisites set by case law (see 5.1. below).

Accordingly, the use of the internet may be monitored if it is for security purposes, but the CNIL specifically recommends using a global tacking mechanism rather than individual monitoring.

Stringent sanctions may be imposed for violating French data protection laws. The CNIL can impose administrative fines amounting to 5 percent of the company's gross revenue, presently capped at 300,000 euros. To date, few controls are in practice. If a company is found to be non-compliant, the CNIL will start by issuing an injunction to comply. It is only if the company fails to comply following an injunction that a fine may be imposed.

In addition, processing personal data in breach of French data protection laws constitutes a criminal violation punishable by five years imprisonment and a fine of 300.000 euros, or up to five times that amount for companies[8]. More importantly, under French law, individual employees and unions have standing to initiate a criminal action for violation of the French data protection laws. This ability of disgruntled employees or unions to do so makes it difficult for French companies to insulate themselves against criminal actions.

[4] Article L. 1121-1 of the French Labor Code
[5] Article L. 2323-32 al. 3 of the French Labor Code
[6] Article L. 1222-4 of the French Labor Code
[7] Cour d'appel de Dijon, 14 septembre 2010, Mille Services c. Rémi X.
[8] Articles 226-16 to 226-24 of the Criminal Code

4. <u>Social media policies and whistleblowing schemes may be less effective in France.</u>

Social media policies and whistleblowing schemes are beginning to receive attention in France due to the US influence. However, these tools are not always adapted to the French employment environment and may not be as effective as a US employer would expect.

➢ "Social media policies" are meant to clearly define the use of networking websites such as LinkedIn, Facebook, Twitter, etc.

This is a relatively new arena so it remains to be seen how enforceable such policies will be. It is already clear in France that the provision of a social media policy, stating that the use of social networks during working time is grounds for immediate dismissal, will not be binding on an employment court. A judge will take into account the circumstances of the alleged violation of the social media policy to appreciate whether there is sufficient cause for dismissal.

In other words, an employment court can always decide that a dismissal based on failure to comply with a social media policy does not have a sufficient cause, and therefore can grant damages for wrongful termination to the employee sacked.

➢ "Whistleblowing schemes" are deemed suspicious in France for the historical reasons mentioned above. Co-workers making anonymous calls reporting bad behaviours to a hotline conjures up images of collaborators' denouncing neighbours in the not-so-distant past. Whistleblowing schemes are under strict scrutiny from the CNIL and from the French Supreme Court because they are considered to be a potential threat to individual freedom. Thus, a Code of Conduct containing whistle blowing obligations may be perfectly legal in the U.S. but invalidated in France. Foreign subsidiaries of companies listed in the U.S. may find themselves between a rock and a hard place, with the obligation to comply both with Sarbanes-Oxley Act ("SOX") provisions and with local regulations.

The CNIL has set forth the conditions under which a whistleblowing scheme can be implemented:

- the scope must be limited to corporate fraud;
- whistleblowing must never be mandatory (even if it is mandatory for the company to implement a whistleblowing scheme);
- whistleblowing must be the last recourse after the employee has tried to report to his superior, to the auditor or to anyone entrusted to deal with the matter; and
- the whistleblower must disclose his/her identity to the investigators but can ask to remain otherwise anonymous.

The French Supreme Court, in its ruling of December 8, 2009[9], invalidated the whistleblowing scheme contained in Dassault Systèmes'[10] code of business conduct, because:

[9] Cour de cassation (chambre sociale), 8 décembre 2009, n° 08-17.191, arrêt n° 2524, PBRI

[10] Dassault Systèmes is listed at the NYSE as well as at the Paris Stock Exchange

- The scope of whistleblowing was not limited to corporate fraud but also included any serious shortcomings, such as breach of intellectual property rights, disclosure of privileged information, insider trading, discrimination, or moral or sexual harassment, thereby putting at stake the interests of the company and the physical or moral integrity of an employee. The scheme was therefore prone to encourage invasion of privacy.

- The code failed to provide that any employee involved in the whistleblowing process had the right to access his/her personal data and demand that such information be amended or deleted if inaccurate or outdated.

In sum, to be valid in France, whistleblowing schemes must have at least a limited scope (corporate fraud only) and the whistle blower cannot remain entirely anonymous. Schemes that do not comply with these requirements must seek prior approval from the CNIL. As a result, US companies cannot simply "copy and paste" their own whistleblowing schemes and impose them on employees based in France.

5. France: employee's right to privacy v. company's right to access digital data created by the employee.

With the rise of new technologies, the debate on privacy in the workplace increasingly concerns data stored in an employee's computer used for professional purposes.

Over the past decade, French employment courts have seen an ever-growing range of employment litigation in which digital evidence is key. This typically occurs, for instance, in unfair competition cases where an employee sets up a competing business during work hours, using an employer's assets to poach clients.

When an employee has engaged in such disloyal activity, the critical steps taken by an employer of searching, examining, collecting and preserving evidence found on an employee's computer may likely determine the outcome of any resulting employment litigation. The French courts have provided significant guidance on each of these critical steps as the admission of hard drives, internet files and emails as courtroom evidence in employment disputes has become increasingly common.

The admissibility of digital evidence is a particularly sensitive issue in French civil procedures where evidence is almost exclusively in a written format. Court testimony is seldom used and instead witness statements are submitted. Witness depositions/examinations and discovery are unheard of in the French system.

Therefore unfair competition cases in an employment context rely heavily on digital evidence available in an employee's computer. Moreover the concept of employment at will does not exist in France and thus failure to prove that an employee's dismissal is well grounded exposes an employer to damages for unfair dismissal. Such damages can reach 2 to 3 years of salary, depending on the seniority at hand. Accordingly, an employer who discovers an employee's disloyal activity and wishes to sack the employee on the spot should take time to elaborate a strategy that will enable it to secure available digital evidence before declaring war on the employee.

Computers placed at the employee's disposal by the employer remain the employer's property and are supposed to contain only limited information related to the employee's private life. However, personal use of the company's computer is allowed provided that such use is reasonable and does not affect the employee's work and the company's activity.

This situation raises the question of ownership of the data stored by an employee on a computer placed at his disposal by his employer and highlights the need to balance the personal dignity of employees with the proprietary interests of employers.

In France, as opposed to the United States, computer data stored on a corporate asset and created using corporate systems does not automatically qualify as company property.

The French Supreme Court, based on the starting point that workers have a right to privacy even in the workplace – although this principle is not cited as such in the French Labour Code - , has developed case law on digital evidence over the past ten years, setting precedents which may disconcert an American observer. Particularly noteworthy is a recent court ruling, which, for the first time, rendered a decision on the admissibility of messages posted on the Facebook wall of an employee.

5.1. The collection and use in a courtroom of digital data created by a disloyal employee

5.1.1. Employers must respect the privacy of disloyal employees, according to the French Supreme Court

During working hours, sitting in his company office and using the tools put at his disposal by his employer, an employee sets up and operates a competing business, poaches his employer's clients, thereby generating shadow revenues to his benefit. The employer becomes suspicious, searches the corporate computer and prints out volumes of digital data proving the employee's disloyalty and terminates the employee. In a wrongful termination suit, is this evidence admissible? According to the French Supreme Court in a 2001 decision,[11]the answer was "no." The Court determined that the employer violated the privacy to which an employee is entitled even when working. The fact that a corporate policy forbids any private use of the company computer was irrelevant. The employer was ordered to pay the employee(i) wages for what would have been the notice period prior to cessation of employment,(ii)wages for paid holidays, (iii) a severance indemnity and (iv) damages for non justified loss of employment.

With this ruling, the French Supreme Court established a strong precedent that favoured employee's privacy over the protection of the company's interests and left employers somewhat at a loss.

In a 2005 case, an employer found erotic pictures in an employee's office drawer. The employer then searched the employee's computer and opened a file flagged as "personal." The employee was sacked for gross misbehaviour on the basis of the non-professional data stored in the personal file opened by the employer. According to the French Supreme Court, however, this digital data was deemed inadmissible evidence. The French Supreme Court adopted an analysis used in an earlier case involving the personal locker of an employee. The Court analogized that the

[11] Cour de cassation (chambre sociale), 2 octobre 2001, n° 99-42.942, JSL n° 88-2

same privacy protection applies to personal computer files as it does to a personal locker.[12] The Court further indicated that erotic pictures found in the employee's drawer did not create a particular risk allowing the employer to open personal computer files.

While this decision favoured the employee, the French Supreme Court nevertheless created an exception to its stringent 2001 precedent[13]:the employer can access and use the private files of an employee if the company is facing particular risks.[14]

The French Supreme Court provided further guidance in 2006 when it determined that emails and files stored in an employee's work computer or in the office are presumed to be work-related – and therefore accessible by the employer and admissible in court, except if they are flagged as "personal" or "private"[15]. With this new precedent, the French Supreme Court further softened the effects of its 2001 ruling ,[16]which had been criticized as over-protective of disloyal employees.

As a consequence of the 2005 and 2006 rulings, any email or document that is not labelled "personal" or "private" – either by its name or by the file where it is stored – can be opened and used in court by the employer. Moreover, emails and documents that are flagged "personal" or "private" can be opened when the company is facing particular risks.

It should be noted, however, that whether a document label is sufficiently marked as "personal" is decided by the courts on a case-by-case basis. For example, the French Supreme Court held in 2009 that a file named "JM" after an employee's initials (Jean-Marc) was not sufficiently labelled as "personal"; its content was therefore admissible evidence[17]

Opening a private email is a criminal offence known as violation of private correspondence, which is sanctioned by one-year imprisonment and a 45,000 euros fine[18]. Nevertheless, employees seldom seek redress in the criminal court because the employment-law procedure – in which an employee may also seek damages – might be adjourned until the criminal judge renders a final decision.

5.1.2. Best practice to collect and preserve digital evidence created by a disloyal employee

When an employer collects digital evidence to be used against an employee, the employee may question the authenticity of the collected data and claim that the employer planted evidence in his work computer.

It is therefore advisable to request in court the appointment of a bailiff who will be assigned, with the assistance of an IT expert, to collect all relevant data in the employee's computer. This procedural route was expressly set forth by the French Supreme Court in 2005.[19]

[12] Cour de cassation (chambre sociale), 11 décembre 2001, Juris-Data n° 2001-012121 ; Bull. civ. 2001, V, n° 377
[13] See note 3 above
[14] Cour de cassation (chambre sociale), 17 mai 2005, n° 03-40.017
[15] Cour de cassation (chambre sociale), 18 octobre 2006, n° 04-48.025, F-P+B, Le Fur / SARL Technisoft, Juris-Data n° 2006-035418
[16] See note 3 above
[17] Cour de cassation (chambre sociale), 18 octobre 2009, n° 05-38.492
[18] Article 226-1 of the French Criminal Code
[19] See note 5 above

With this procedure, the court will precisely delineate bailiff's assignment, adapting the description requested by the plaintiff in his brief, in order to ensure that an employee's privacy is protected. The bailiff's assignment will be strictly limited to the disloyal activity presumably carried out by the employee and the bailiff will not be able to collect any other private data.

The bailiff will then issue a certified report with a print-out of all relevant data which authenticity is thereby guaranteed.

Once the employer becomes suspicious of an employee's activity and begins to anticipate litigation, it is advisable to immediately remit the computer to the bailiff who will sequester it during the time of the procedure. The procedure further reduces the risk of the employee successfully arguing that evidence was planted in the computer.

Some particular situations may be encountered, jeopardizing the outcome of such procedure:

- What if the computer is in the hands of the employee, as is commonly the case with a laptop? A summons to appear in court may certainly lead an employee to delete all relevant data from the computer before submitting it to the court-appointed bailiff.

  In that case, the employer can file a "one-sided" motion to the court, that is a motion that is not disclosed to the other party. If the motion is granted and a bailiff is appointed by the court, the bailiff will seize the computer without providing advance notice to the employee. At that time of seizure, the bailiff notifies the employee of the employer's motion and of the court order granting such motion. The employee can then challenge the court order and seek the annulment of the motion and the subsequent seizure. In order to obtain such annulment, the employee will have to prove that the facts presented by the employer in his "one-sided" motion are inaccurate or were not serious enough to justify the seizure of the computer.

- What if the employee works from a home office and the computer is therefore located in the home? Can a court-appointed bailiff enter an employee's home without consent and seize the company computer?

  Yes, when the employee has a dedicated room for a home office and the employer pays an indemnity for the professional use of this room. In that case, the home office space is regarded as a professional space from which the bailiff can seize the computer.

  In such an instance, a court will usually order that the bailiff be assisted by a police officer and a locksmith to ensure that the seizure takes place.

- What if the employee, anticipating that the computer may be searched, deletes all relevant data before the bailiff can seize the computer?

  The employer may hand the computer over to a private IT firm who will be able to restore the data. An employee is likely to dispute the authenticity of any damaging evidence found since the private IT firm is not an independent third party, but is instead hired and paid by the employer in anticipation of litigation.

  This situation can be avoided if an employer asks the court to appoint an independent expert who will restore the data deleted by an employee pertaining to the disloyal activity.

As mentioned above, digital evidence pertaining to the employee's disloyal activity is key to avoid payment of damages for unfair dismissal. It is also key in an unfair competition claim brought before the commercial court against a competing company established by an employee with the use of a former employer's assets.

5.2. An employer can use as court evidence the list of websites browsed by his employee

The internet activity of an employee on a company computer can tell a lot about whether the mind of the employee is focused on professional tasks or on personal business.

For this type of evidence, the French Supreme Court has ruled in favour of employers and has found that websites browsed by an employee with a company computer are presumed to have a professional nature. Therefore, an employer can access a history of sites browsed even in the absence of the concerned employee presence.[20]

In one noteworthy case, an employee spent more than 40 hours per month on the internet, visiting websites with content unrelated to work. Following the above mentioned precedent, the French Supreme Court found that the browsing history, including dates and times, was admissible evidence. The employer was therefore able to prove that the employee abused the right to use the internet for personal purposes, laying cause for dismissal.[21]

In another instance, an employee used the company computer during working time to access pornographic websites, store a wide amount of explicit data and exchange many emails with internet-users met on these websites. The employer filed a criminal complaint against the employee for misuse of corporate assets. The French Supreme Court found for the employer and declared that the use of corporate tools for a time-consuming activity unrelated to the employee's professional tasks constituted the criminal offence of misuse of corporate assets.[22]

In cases involving visits to child pornography websites, such activity of an employee is criminal and the employer bears an obligation to report such offence to the Public Prosecutor. Therefore it is the duty of an employer, when he has reasonable suspicion that an employee is engaged in such criminal activity, to investigate and collect digital evidence of said activity.

Generally speaking, it is recommended that a bailiff collect the data pertaining to browsed websites in order to ensure authenticity of such data.

5.3. Facebook: friends of your friends may not be your friends

A French saying goes "*The friends of my friends are my friends.*" This may not be true on Facebook.

Three employees of the same company carry on a discussion on the Facebook wall of one of them. The discussion takes place on a Saturday night from the employees' respective homes. Two of the employees welcome the third one in a "club", the purpose of which is to "make fun" (in slang language) of their boss all day long without her noticing, and more generally to be a real pain in the

[20] Cour de cassation (chambre sociale), 9 juillet 2008, n° 06-45.800, L. v. Sté Entreprise M., Jurisdata n° 2008-044801
[21] Cour de cassation (chambre sociale), 18 mars 2009, n° 07-44.247, X v. Sté Lauzin
[22] Cour de cassation (chambre criminelle), 19 mai 2004, n° 03-83.953

neck for her. The privacy settings of the employee hosting the conversation enable his friends and his friends' friends to have access to the wall.

One of his friends' friends comes across the conversation, prints it out and hands it over to the employer.

All three employees are dismissed on the spot (a severe measure under French employment law because usually a notice period is granted).

The dismissed employees sought redress in an employment court and claimed that it is the employer who misbehaved when it peeked on the Facebook wall because it "introduced" itself in a private space without being invited. Furthermore, they argued that the conversation was of a humoristic nature, as shown by the slang language used and the "smileys" posted in their messages. The employees asserted that their actions constituted joking, from their homes and in their private time.

The employer replied that it did not peek at the wall but that a print-out of the conversation was handed over to it by someone who had authorized access to the wall, in his capacity as "friend of a friend". The employer also noted that eleven employees had access to the wall and that the reported conversation was detrimental to the company's interests. According to the employer, the three employees abused their freedom of speech and could legitimately be dismissed without notice.

In this case at hand, a 2010 decision of the employment court held that the evidence found on the Facebook wall was admissible.[23] By granting access to his wall to his friends' friends, the employee hosting the conversation made his wall a public space – or rather a semi-public one. Moreover, the court determined that the content of the messages was abusive and therefore not protected under freedom of speech; the dismissals without notice were grounded.

This 2010 decision is the first decision rendered in France on Facebook evidence. The employees have appealed this lower court decision. The decision of the Appellate Court is much anticipated by employment-law practitioners. The Appellate Court may be tempted to reverse the lower court decision which ruling appears to be quite harsh on the employees in the French employment-law environment where employees' rights are carefully protected.

Facebook conversations among colleagues are the virtual equivalent of casual conversations around the coffee machine. Facebook users as well as email users exchange informal comments in writing, typing as quickly as they would speak and without thinking of the consequences. The line between speaking and writing is blurred as one writes instead of speaking. The line between private and professional time is also blurred as emails or Facebook messages carelessly written from home outside working time may under certain prerequisites be admissible as court evidence against the employee. While a conversation at the coffee machine may be overheard by a handful of colleague and soon be forgotten by all, new technologies and social media in contrast turn informal conversations into written evidence that can be brought into the courtroom. Blogs, trivial social interactions, emails and "LOL" moments are preserved indiscriminately and may be examined by a judge outside their context.

[23] Conseil de prud'hommes de Boulogne Billancourt, 19th November 2010, Mme S v. Sté Alten Sir, Juris-Data n° 2010-021303