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
Social Networking and the Global Workforce

SOCIAL NETWORKING IN THE WORKPLACE – FRANCE

Internet is a place of limitless freedom and carefree entertainment, or so it seems. Unfortunately, few internet users bear in mind that while they sit comfortably in front of their screen and explore the virtual world, their responsibility may be triggered in the real world. While no employee in his right mind would stand in front of a crowd with a megaphone, provide his name and his employer's name, disparage the company, insult his boss, and give away trade secrets, such type of communication is not uncommon on the internet.

Employees posting material on social networks may not be aware that their mouse clicks can affect several important legal issues:

- Right to privacy: Article 8 of the *European Convention on Human Rights* 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. The right to privacy includes the privacy of correspondence. Invasions of privacy and violation of correspondence privacy are both criminal offences and extremely well respected in France, the country of individual freedom and bastion of workplace privacy.

- Freedom of speech: the still-enforced *1881 Act on Freedom of Press* protects the freedom of speech of journalists. This Act is also applied to internet users and bloggers and, more particularly, to employees who publicize work-related comments on the net. In addition, a provision of the *Labour Code* sets forth that all employees have the right to express themselves on the contents, the conditions and the organization of their work[1]. Another

[1] Article L. 2281-1 of the Labour Code

provision of the same Code provides that employees cannot be disciplined for opinions they express pursuant to their freedom of speech.

- Limits on freedom of speech: the above-mentioned *1881 Act on Freedom of Press* sets forth that a speech containing injurious or defamatory comments is not protected under freedom of speech. Injurious comments may be either expressed in public or in private. Those made in public are more seriously sanctioned. It is therefore important to determine whether an internet posting is made on a public or a private virtual space. As for defamatory comments, the author can assert the "truthfulness defense", i.e. his liability won't be triggered if he can prove the truthfulness of the so-called defamatory comment.

- Duty of loyalty of employees towards employers: the employment contract, like any contract, should be performed in good faith and each party should refrain from any action that may cause damages to the other party.

- Company's legitimate interests: employers have the right to protect their trade secrets and their e-reputation. However, an employer can only restrict employees' rights and freedom insofar as these restrictions are proportional and justified by their purpose.

This article will address (1) the impact of social networks in the French workplace at the recruitment stage, (2) the risk of disciplinary actions based on social media postings, (3) the employer's right to access electronic communications on the employee's computer, and (4) social media policies.

1. Can non-professional material posted by an applicant on the internet be taken into account in the recruitment process?

These days, head hunters and HR managers are more and more tempted to browse the internet for additional information on applicants. This trend is understandable: material posted by a would-be employee on various online networks is bound to provide a more comprehensive and accurate picture than the stereotypical resume and the equally stereotypical message delivered during a job interview.

It seems clear that between two equivalent profiles, a recruiter may choose the applicant whose internet image is neat and reassuring over another who has engaged in careless or hurtful online communications or postings, just as the recruiter would normally prefer an employee with clean living over another who overtly indulges in wild parties and heavy drinking.

Some voices have expressed concern that such practices of considering an applicant's internet image could lead to taking into account private aspects of the applicant's life, which may never have been meant to be viewed by a potential employer.

In this respect, a distinction should be made between private social networks, such as Facebook or Twitter, and professional ones, such as LinkedIn or Viadeo. Professional networks are precisely meant to enhance business interactions among its members and to provide a legitimate source of information in any recruiting process.

The question remains open, however, for "pure" social networks, primarily meant to connect friends, family and relatives – and sometimes co-workers: is it fair that an applicant be rejected

because of old pictures taken in a non-professional context which may provide a misleading view of the applicant's past behaviour as a younger and possibly more reckless self?

This issue is all the more relevant since the "right to be forgotten" seems to be denied by social networks which do not make it possible at this point for individuals to permanently retrieve or delete their personal data. Even convicted criminals can expect a right of rehabilitation, but cutting ourselves loose from our digital baggage is proving to be a challenge. The European Commission is currently focusing on the right of digital self-determination by individuals online.

Meanwhile, until the "right to be forgotten" can effectively be exercised, if ever, one should assume that the material released online by each individual was voluntarily released and that it must have been clear to that individual, at the time of the release, that the material would be widely and quasi-permanently accessible. Therefore, there is no invasion of privacy when the individual publicly and knowingly exposes himself or herself.

However this assumption may not be entirely true now with the arrival of new e-tools such as Facebook's facial recognition system that can tag faces automatically. This new system, applicable by default unless the user opts out, automatically goes through uploaded photos and offers up suggestions of who it thinks the people are, based on a comparison with pictures of Facebook friends of the user that are already available in his albums. This new application will make it even more difficult for Facebook users to control their digital image.

In France, where potential invasions of privacy are closely watched, a code of conduct has been recently signed by various companies and headhunting firms, providing guidance as to the use of internet and social networks in the recruiting process. The goal is to avoid recruitments being influenced by subjective considerations – personal tastes, friends, non-professional activities - over a rational assessment of the applicant's skills. The goal is also to avoid discrimination based on information about the applicant found on-line.

This code of conduct sets forth that the selection of applicants must rely solely on their education and skills, to the exclusion of any criteria pertaining to their private lives. All signatories of the code declare that they will refrain from searching information on applicants using search engines or social networks, even when the material available online has been released by the applicant. The only exception is when the applicant signs in on pages created by the recruiters.

Further, signatories commit to using professional networks only for the purpose of their online researches.

The signatories of the code of conduct will be subject to an annual audit in order to check that the provisions of the code are being respected and that the business is not engaging in discriminatory practices.

However it is, in practice, impossible to check whether a company actually collects information about applicants online, and if so, on which websites or networks. Therefore the efficiency of the above-mentioned code of conduct relies heavily on each company's sense of responsibility.

The major contribution of the code of conduct is to draw attention to the pitfalls of internet in the workplace, but no law will ever prevent people from collecting available information from the internet. Social network users should therefore sanitize their personal pages when job hunting, lest potential employers spot an inappropriate photo or comment.

2. Can an employee be disciplined for social media postings?

Social network conversations among co-workers 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 co-workers 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, pictures and "LOL" moments are preserved indiscriminately and may be examined by a judge outside their context.

With 20 millions Facebook members in France, more and more cases are arising over communications released by employees on social media. Technology outpaces the law and so far there is no regulation on the use of social media data as admissible evidence. Some talk about a "semi-private" or a "semi-public" space. A few hints as to the direction the courts might take are provided by occasional cases in lower courts. There is still no decision from the French Supreme Court on this topic.

2.1. Messages posted on the Facebook wall of a "friend" are not private correspondence

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

In one case in particular, journalist posted the following message on the Facebook wall of a "friend", a co-worker in real life:

> "*By the way: our boss is really autistic, right? Do you happen to know a specialized center where they could cure him? Anyway, can stupidity be cured*?"

A friend of this friend handed over the post to the employer, who issued a formal warning to the journalist because he claimed the post was injurious and defamatory. The employee applied to the Labour Court in order to have this warning nullified.

The question asked to the Court was twofold:

- Did the post qualify as private correspondence or public communication? If it was private correspondence, the employer violated the employee's right to privacy and freedom of speech and the warning must be nullified.

- If the post was admissible evidence, was its content injurious and defamatory? If so, the warning must be confirmed.

To the first question, the employee argued that Facebook constitutes a private space comparable to a personal email box and that his post was therefore protected as private correspondence. The

employer replied that he had accessed the post legitimately and without the use of force or trickery, therefore the post was admissible evidence. The Appellate Court of Reims [2] followed the employer's argumentation: because the message was posted on a friend's wall, the employee had no control whatsoever over its accessibility by third-parties, such accessibility depending on the privacy settings of the friend. The co-worker could have had hundreds of friends or may not even have limited the access to his profile and wall. Had the employee wanted his post to remain private, he should have sent it to the Facebook personal email box of his friend. A private correspondence is one that cannot be read by someone who is not one of the addressees. Therefore the post was admissible evidence.

To the second question, the Appellate Court of Reims[3] answered that the message was not injurious or defamatory because there was an ambiguity over the identity of the person targeted by the message. The word "boss" was not clear enough in the context and could have referred to someone outside the workplace. Therefore the warning was nullified.

This decision seems to be sending out a message to Facebook users: if you send a Facebook message to your contact's personal email box rather than posting it on the wall, your message will more likely qualify as private correspondence and should therefore enjoy the corresponding privacy protection.

2.2. Messages posted on your own Facebook wall are not private correspondence if accessible to friends of your friends

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 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 was the employer who misbehaved when he looked on the Facebook wall because he virtually "introduced" himself 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 he did not even have to access the wall because a print-out of the conversation was handed over to him 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

[2] Cour d'appel de Reims, chambre sociale, 9 juin 2010, affaire n° 09/03205
[3] See above, note 2

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.[4] 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.

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.

2.3. The hints provided by caselaw so far and the remaining questions

The two above-mentioned court decisions have in common that the evidence was found admissible because the employers had "legitimate" access to it without the use of force or trickery, and therefore the employers did not invade the employees' privacy.

Some voices raised concern that this interpretation will encourage employees to report on their co-workers and hand over incriminating data to their employers, which is reminiscent of the traumatizing events of WWII. After WWII, reporting to the authorities was deemed suspicious *per se* in France.

The same "legitimate access" test applies to emails. For example, the French Supreme Court found[5] that an email sent by an employee to a co-worker, in which he insulted his employer and announced that he would call in sick the next day, was admissible evidence when this email was mistakenly copied by the employee… to the employer! In this case, the email fell in the hands of the employer because of the employee's mistake and the employer did not use force or trickery. The ruling would have been the same had the employee mistakenly copied a co-worker who then gave the email to the employer.

The question of how the data posted on social networks is accessed is therefore a key criterion and it is clear at this point that:

- An employee who posts digital data to be seen by an uncontrollable number of people (friends of friends or, even worse, all public) cannot support a claim for privacy, and should take for granted that not all Facebook users are his or her friends in the real world.

- An employer who creates a Facebook account with a fake identity, the only purpose of which is to be accepted as a "friend" of the employee and access posted data, will not be allowed to produce the collected evidence in court because he used trickery.

- Similarly, an employer who breaks a confidentiality code and hacks into a Facebook page will not be able to use in court the evidence collected with the use of such "force".

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

[5] Cour de cassation, chambre sociale, 2 février 2011, n° 667-1284.90

Many questions remain unanswered however.

For example, will data posted on the Facebook wall of a user, whose privacy settings only allow access to "friends", be considered private correspondence because of the limited number of persons who can have legitimate access to it?

The existing caselaw seems to support this interpretation, by an "*a contrario*" reasoning: a posting is found to be admissible evidence when it is accessible to "friends of friends"; therefore it will not be admissible evidence when access is restricted to "friends".

However, in such case, a court may take into account the number of "friends" and, should this number be high, consider that the space is not private. Some successful Facebook pages have hundreds or thousands of friends, which is too wide an audience for a private conversation.

A court may also take into account the fact that the wider the audience, the more damageable the communication for the employer's e-reputation when the comment is tantamount to disparaging.

Moreover, if most of your co-workers happen to be your Facebook friends, it will be difficult to convince the court that the post on your wall qualifies as purely private correspondence and has no relation whatsoever in the workplace.

At this point and until the rules are clarified, employees will be well-advised to be cautionary when releasing any work-related comments on the net and think twice before posting any material that may be used against them, such as pictures of themselves on the beach when they call in sick.

On the other side, companies that collect digital data on the net to be used against their employees should secure the evidence with the help of a bailiff, a sworn-in officer. The bailiff can issue an official statement on how the data was accessed, describing each step and each mouse click, thereby demonstrating that the data was legitimately accessible to the employer.

2.4. The recommendations issued by the French Data Protection Authority

The above mentioned caselaw, widely reported in the media, triggered many interrogations and created some confusion because of all the – sometimes contradictory – comments that followed.

As a consequence, the French Data Protection Authority ("CNIL", *Commission Informatique et Libertés*") issued an opinion on January 10th, 2011 on communications on social networks[6].

The information and recommendations released by the CNIL are the following:

- Employees can be discharged because of communications made on social networks, according to recent caselaw from a lower court. The court held that the Facebook conversation was public because it was accessible to "friends of friends", i.e., persons who were not concerned by the topic discussed.

- Facebook users should be extremely cautious as to the data they disclose online. Digital data is increasingly used for the purpose of disciplinary measures. Things that people

[6] CNIL recommendation, 10 janvier 2011 : «Maîtriser les informations publiées sur les réseaux sociaux»

wouldn't say in the real world to their family, friends, co-workers or boss, should also not be said in the virtual world.

- Facebook enables one to create different lists of friends for family, close friends, co-workers, etc., and to adjust the privacy settings for each list. It is strongly recommended to make use of this possibility.

Recommendations issued by the CNIL are not binding. However, they provide guidance to all players and are usually taken into account by courts.

2.5 The delicate art of blogging about your employer

In the case of blogs, the question of access to the data is irrelevant because blogs are open to all internet users.

Therefore the question is what freedom of speech is granted to employees for communications about their employers on the internet.

As mentioned above, the provisions of the *1881 Act on Freedom of Press* apply to any blogger – even though blogging was not anticipated by the lawmakers when this law was enacted.

Again, there is very little caselaw on this topic at this point:

- In one decision rendered by a lower Court[7], a female employee with Nissan, Mrs. G, was discharged for serious misconduct a few months after her return from maternity leave. Following her discharge, she created a blog that she called "maternityleaveNissan" on which she told her side of the story. According to her, she had been discriminated against because she had a child.

  Nissan sued her in order to obtain the deletion of some of her statements that Nissan claimed were injurious or defamatory, that is:

  - The title of the blog *"Being a mom at Nissan, forget about equal opportunity*";

  - Assertion that Nissan's Works Council has in reality no real power and deals only with irrelevant issues;

  - Assertion that there is no equal opportunity at Nissan, especially if you are in your 30's, a woman, and have a child; in which case your head will bump the glass ceiling or, even worse, you will be discharged for serious misconduct;

  - Assertion that the HR department violated employment law;

  - Assertion that she was discriminated against.

  Mrs. G. tried to prove the truthfulness of these statements but the court found that she failed to do so as far as the first four statements above were concerned. Mrs. G. was therefore ordered to delete all four statements.

[7] *Tribunal de Grande Instance de Paris, 17ème chambre, 26 octobre 2006*

As to the fifth statement, the court held that Mrs. G. was expressing an opinion and that readers of her blog necessarily understood that this opinion did not necessarily reflect the truth. Therefore the statement could remain on the blog.

Mrs. G. was also condemned for injurious comments for her use of the words “conspiracy of felons” posted on her blog, and “manipulative and liar”, qualifying Nissan’s HR manager. The court found that the injurious comments were held in a public space rather than in a private one, as it was a blog accessible to all.

The lesson is clear: the same laws apply to communications on the internet as to real world communications, despite the deceptive impression of limitless freedom and irresponsibility given by the web.

- In another case, “*Petite Anglaise*” was luckier. A then-anonymous blogger, Mrs. Sanderson, a British citizen, held a blog detailing the tribulations of her expat life in Paris with her three-year-old daughter. Well-written and humoristic, her “Bridget Jones” blog quickly gained popularity. *Petite Anglaise* did not reveal her name or that of her employer, a British accountancy firm, and rarely mentioned her work as a secretary. At some point however she ironically mentioned the fact that one of her bosses had hung a portrait of the Queen in his office and was addicted to tea. This comment could have targeted nearly any British firm in Paris. However, her employer somehow came across the blog and, because “*Petite Anglaise*” had posted an old picture of herself, he identified his employee and dismissed her, despite her 4 years of seniority, for “bringing the firm into disrepute”.

  Once the news of the dismissal broke, comments and support from prominent bloggers catapulted the story into mainstream media, including the Daily Telegraph and The Guardian. The employer, Dixon Wilson, received unsolicited media attention and the dismissal was widely commented on as unfair. It was popularly agreed that the reputation of the employer was hardly hurt by the candid posting of *Petite Anglaise*, and that she certainly didn’t deserve dismissal for such innocent blogs.

  The Labour Court of Paris upheld the complaint of unfair dismissal and awarded damages totalling a year’s salary plus legal costs[8]. Dixon Wilson did not appeal, probably deciding they’d had enough press exposure. The court decision sent out reassuring signals to the millions of people blogging in France; that is, blogging about your employee will not necessarily trigger responsibility, especially when the employer is not clearly identified and when your comments are not damaging to his reputation.

  On another note, blogging sometimes provides a way to recognize hidden talent. The attention Mrs. Sanderson drew earned her a lucrative two-book deal from Penguin. Therefore this is a happy ending for “*Petite Anglaise*”, who still successfully blogs about her life in Paris.

[8] Conseil de prud’hommes de Paris, 29 mars 2007

3. How can an employer collect and use in court electronic communications located on an employee's computer?

When an employee has engaged in a disloyal activity (for example, the setting up of a competing business), 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 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 or 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 has developed over the past ten years case law on digital evidence found in an employee's computer, setting precedents which may disconcert an American observer.

3.1. 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,[9] 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.

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

With this ruling, the French Supreme Court established a strong precedent that favoured an 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 same privacy protection applies to personal computer files as it does to a personal locker.[10] 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[11]: the employer can access and use the private files of an employee if the company is facing particular risks.[12]

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"[13]. With this new precedent, the French Supreme Court further softened the effects of its 2001 ruling,[14]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.[15]

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[16]. 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.

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

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

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.[17]

With this procedure, the court will precisely delineate the 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, which 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.

[17] See note 5 above

- 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.

4. Social media policies in France

"Social media policies" are meant to clearly define the use of networking websites such as LinkedIn, Facebook, Twitter, etc. These policies may seek to do any of the following:

- Inform the employee on new technologies and remind that employees may be held liable for any damage caused in the virtual world as they would be in the real world;

- Prohibit the employee from making disparaging, discriminatory or defamatory comments about their employer, co-workers or competitors;

- Stress the employee's duty of loyalty and protection of trade secrets, and remind that any leak of confidential information via a social network by the employee will trigger his or her personal responsibility;

- Limit the use of social networks during working time and / or allocate time periods during which employees are allowed to access specific websites or their personal email messages;

- Provide guidance as to work-related postings, including what type of information or material pertaining to the company the employee may release;

- Reduce or eliminate the possibility of watching videos, since videos may result in the slowing down of the whole internet network;

- For safety reasons, reduce or disable activities such as the downloading of software or the connection to discussion forums.

In addition, social media policies usually detail the sanctions that will be imposed in case of any contravention of the rules.

Social media policies are beginning to receive attention in France due to the US influence. However, this tool imported from the United States does not quite fit with the French way of thinking and is only slowly making its way inside the French workplace. According to a recent

Manpower survey[18], 97% of the surveyed French employers indicated that their organizations had not yet implemented formal policies regarding social networking.

Since the reach of social networks goes beyond national borders, multinational companies with operations in several countries usually try to coordinate their policies so that all employees worldwide are bound by a single set of rules. Therefore, relevant social media policies are often applied in the French subsidiaries of American companies. However they are not always adapted to the French employment environment and may not be as effective as a US employer would expect.

In France, social media policies (such as any code of conduct) can only be legally binding and enforceable against employees after the employer has informed and consulted the Works Council about the social media policy, sent it to the labour authorities, and individually informed each employee about it.

As to the rules set by social media policies, 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, for example, 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 did not have a sufficient cause, and therefore can grant damages for wrongful termination to the sacked employee.

The reason for the limited popularity and effectiveness of social media policies in France relates to the cultural differences in the respective American and French legal systems. In the U.S., a common law country where rules are developed and elaborated on a case-by-case basis, it is safer to try and anticipate all possibilities beforehand in a binding document. In France, a civil law country, the answers to future legal disputes are already entailed in codes. Caselaw merely decides how a particular legal provision will be adapted or construed in an ever-changing world of new technologies and applied to a case at hand, but the rule is already written and will not be changed by any caselaw.

[18] Manpower Inc., Employer Perspectives on Social Networking Survey, 2011