Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

Volume 13, Number 7 July 2013

Technology and Privacy in the Workplace under French Law

By Olivier Proust, of Field Fisher Waterhouse LLP, Brussels.

Introduction

Computers, smartphones, CCTV cameras, GPS systems, and biometric devices: Technology is omnipresent in the workplace. As technology continues to develop, employees' personal data is more regularly collected and potential threats to their privacy become more commonplace.

While technology has undoubtedly transformed the way we work and improved workplace performance, the risk of employees' privacy being invaded has also grown. The French data protection authority, the Commission nationale de l'informatique et des libertés ("CNIL"), reports that, in 2012, 15 percent of all complaints received were work-related.[1] Thus, employers are faced with the challenge of finding a way to use technology without being privacy-intrusive.

Earlier this year, the CNIL published several practical guidelines instructing employers on how to use technology in the workplace in accordance with the French Data Protection Act and the rules on privacy.

This Special Report analyses the limitations under French labour and data protection law that apply to companies when using technology to monitor employees or to process their personal data, and explains how companies can achieve a balance between using technology and safeguarding privacy in the workplace.

Employee Data Profiling: Is It Allowed?

Employees are being assessed, evaluated, and profiled throughout their careers. Whether it be to evaluate the skills of a candidate or to assess the performance of an employee, companies are drawn towards sophisticated programs that provide valuable information in support of their decisions. In so doing, companies must make sure that they comply with the following legal principles.

Information Collected about an Employee Must Be Relevant

Both during the hiring process and the employment relationship, employers may only collect information about an employee that is relevant.

During the hiring process, a company may only collect information about a job candidate that is necessary to assess that candidate's professional skills and his/her ability to occupy a given position.[2] The CNIL considers that certain types of information may not be collected during the hiring process, unless it is justified for the job being offered. For example, the CNIL considers that employers should not collect any information about a candidate's past nationality (*e.g.*, date of arrival in the country, date of naturalisation, former nationality), prior address, family (*e.g.*, name, nationality, profession and employer of the parents, siblings and children), living conditions, social life, bank account details, and pending credits or loans.[3] Social security

numbers should not be collected during the hiring process, but after a candidate is hired. The law also prohibits the collection of any sensitive personal data (*i.e.*, racial/ethnic origins, political, philosophical and religious beliefs, trade union affiliation, health and sexual life) without the individual's consent, except in cases where the law stipulates that the prohibition cannot be lifted by the individual's consent.[4] In the recruitment context, the CNIL considers that a candidate's explicit consent does not justify the collection of sensitive data, unless the employer can demonstrate that such collection is justified because the information in question impacts on the candidate's ability to do the proposed job.

Similar restrictions apply throughout an employee's work cycle.[5] In the course of employee evaluations and appraisals, employers must make sure to record information about employees with a view to assessing their professional skills. Employers must also make sure to make notes or comments about their employees that are "adequate, relevant and non-excessive" (*e.g.*, in free-text boxes).[6] Employers should abstain, for example, from collecting information about an employee's private life, as this could be deemed inadequate in the context of an appraisal. Comments about employees must remain objective and must not be excessive or insulting.

The CNIL considers that written comments about employees constitute personal data and are therefore subject to the Data Protection Act.[7] Recently, the CNIL issued a warning against a company specialising in private tutoring for storing unlawful comments about its pupils, their parents and their teachers (*e.g.*, insults or excessive comments, health data, information about offences and convictions) in its database.[8]

Methods Used to Process Employee Data Must Be Proportionate to the Intended Purpose

At all times, a balance must be maintained between the use of technology and the rights of employees. A general provision under labour law prohibits all restrictions on the rights and freedoms of employees, unless they are justified by the nature of the tasks undertaken by the employee, or are proportionate to the intended purpose.[9] As a consequence, all methods or techniques used to assess a candidate or an employee must be proportionate to the intended purpose.[10]

The use of automatic data profiling in the employment context is narrowly permitted. Pursuant to the Data Protection Act, no decision about an individual can be made solely on the grounds of automatically processed data intended to define that individual's profile or to assess his/her personality.[11] The individual must have the opportunity to make remarks before a decision is made that has legal consequences for him or her. In other words, an employer cannot rely solely on an automated system to hire a candidate or to promote an employee. The individual concerned must be given the opportunity to express his/her opinion, for example, during a job interview or a meeting with his/her superior manager. There must always be a human intervention before a decision that has legal consequences for the candidate or the employee is taken.

Employees Must Be Informed about the Processing of Their Data

Employers must inform candidates and employees when collecting data intended to assist with hiring or professional assessment.[12] In particular, employers must inform employees about the purpose of the processing, the recipients of the data and how the employee can exercise his/her privacy rights.[13] It is also prohibited to collect any information about a candidate or an employee by using a device that has not been brought to his/her attention.[14] For example, it would be unlawful for an employer to use a recording device to assess the skills of a candidate without informing that candidate beforehand.

Employers are generally required to inform employees individually about the processing of their personal data, for example, by means of a privacy notice that is posted on the company intranet, a privacy clause in the employee's employment contract, or an email sent to the employee.

Companies must also inform and consult the Works Council prior to introducing any new technologies (including methods or techniques used to collect and process personal data) that may have consequences for employment, qualifications, remuneration, training or the workplace conditions.[15]

Employees Have the Right to Access Their Personal Data

Candidates have a right to access their personal data.[16] In particular, they may access and request a copy of any results of tests and assessments undertaken by the company during the hiring process.[17] Employees may also access, and obtain a copy of, their evaluations and appraisals. The CNIL states that the company's assessment of an employee must be disclosed, upon request, when such information has been used to make certain decisions about the employee (*e.g.*, promotions, salary increases, appointments). However, if the assessment only constitutes an estimation of the employee's potential, that information can remain confidential, and the employer is not obliged to disclose it to the employee.[18] Finally, employers should remember that employees can always request access to written notes and comments made about them by their employer.

Geolocation of Company Vehicles: Can a Company Track and Trace its Employees?

Employers frequently install geolocation devices in company-owned vehicles in order to locate them. While such devices are extremely convenient, they also pose a threat for employees if used unlawfully to track their every movement. Therefore, employers must find a fair balance between locating a vehicle and tracking the employees who use that vehicle.

The CNIL recommends using Global Positioning Systems (GPS) in company vehicles for the following purposes:[19]

   ISSN 1473-3579

- to optimise productivity (*e.g.*, to dispatch the closest vehicle in case of an emergency);
- to guarantee the safety of the individuals or merchandise in the vehicle;
- to monitor an employee's working hours (although only if this cannot be measured otherwise);
- to organise transportation services (*e.g.*, ambulance services) and send out invoices; and
- to comply with a legal requirement regarding the use of a geolocation device, for example, due to the type of transportation or the nature of the goods being transported (*e.g.*, public transportation, transportation of dangerous materials).

Geolocation devices must be used fairly and lawfully, and cannot be used to monitor employees on a permanent basis.[20] Employers must make sure not to use geolocation devices in a disproportionate manner, or in a manner that would restrict the rights and freedoms of their employees, without justification.[21] For example, geolocation devices can only be used in limited circumstances to monitor an employee's working hours. In particular, geolocation devices should not be used when an employee is free to organise his working hours as he chooses (*e.g.*, a sales representative). In a recent decision,[22] the French Court of Cassation upheld a decision against a company that unlawfully used a geolocation device to track the company vehicle used by one of its salesmen. Although the company had informed the salesman that a geolocation device would be used to optimise productivity by analysing the time spent on each business trip, the device was in fact used to monitor his working hours, and eventually to reduce his salary. The Court ruled that the use of a geolocation device to monitor the activities (and working hours) of an employee is lawful only if such monitoring cannot be done otherwise. In the given case, the Court found that the use of a geolocation device to monitor the salesman's time on the clock was unjustified because his employment contract allowed him to determine his own schedule as long as he submitted a detailed report of his activities to his employer.

Furthermore, geolocation devices should not be used after working hours. For that reason, the CNIL recommends that employees who use company vehicles for both professional and private purposes must be able to switch off the GPS system at the end of their working day. The use of geolocation devices to monitor the activities of protected employees (*i.e.*, trade unionists or employee representatives) is also prohibited when they are performing their legal duties.

Finally, geolocation devices can collect large quantities of information and, for that reason, must only collect data that is relevant and non-excessive. In particular, geolocation should not be used to monitor a vehicle's speed or to record broken speed limits. The Data Protection Act limits the number of individuals and entities who are authorised to process personal data about felonies and offences.[23] Therefore, a geolocation device should be configured in such a way as to record the average speed of the vehicle, without collecting any information on broken speed limits or other traffic felonies.

Companies must inform the Works Council (or the employee representative body) prior to installing geolocation devices into their vehicles.[24] The company must also provide notice to its employees, either in their employment agreement or by way of a privacy notice.[25]

Employers must grant employees access to any personal data that is stored on a geolocation device.[26] Recently, the CNIL fined a company €10,000 (U.S.$12,829) for refusing to grant an employee access to the data stored in a geolocation device.[27] The employee in question wanted to use that data as evidence to prove his innocence in a traffic accident.

Computer Monitoring: Can a Company Access the Files and Emails of its Employees?

Companies may be required to investigate an employee, for example, when he/she is suspected of fraud or has violated the company's internal policies. In order to obtain and retain evidence of that employee's wrongdoing, the company may need to search the employee's email inbox and computer files. In France, internal corporate investigations automatically trigger the application of several laws: civil law, labour law, criminal law and data protection law. Therefore, when accessing employee emails and files, companies must proceed with caution, as certain restrictions will apply which limit their scope of action, and aim at protecting the right to privacy of the employee.

The rules on privacy in the workplace are largely based on case law, particularly the rulings of the French Court of Cassation. The Court of Cassation ruled in 2001 in a landmark decision that "an employee has the right to the respect of his private life — including the right to the secrecy of correspondence — on the work premises and during working hours".[28] The Court's ruling is based on Article 9 of the Civil Code, which states: "any person has the right to the respect of his private life". Since then, the Court of Cassation has refined its position, and considers that emails and documents stored on a computer owned by the company are presumed to be professional by nature, unless they are identified as being personal.

Access to Employee Files

As a general rule, an employer cannot access files marked "private" stored on the hard drive of a company-owned computer without the employee's presence or informing the employee, unless there is a particular risk or event for the company.[29]

Unless marked by the employee as private, the documents and files created by an employee on a company-owned computer for work purposes are presumed to be professional, which means that the company can access those documents and files without the employee's presence.[30]

In order to limit possible intrusions by the company, em-

ployees must make sure to store their private documents in a folder that is clearly marked "private". An employee's initials,[31] or first name,[32] do not render that folder private, nor does the generic expression "My Documents".[33]

The Court of Cassation also ruled that naming a hard drive "personal data" does not automatically render the files stored on that hard drive private.[34] On the contrary, an employee cannot prevent his/her employer from accessing a hard drive simply by renaming it "private".

The Court's interpretation of the right to privacy in the workplace also applies to other storage devices. For example, the Court of Cassation recently overruled a decision of the Court of Appeal in a case where a secretary had been fired for having stored confidential information about the company, colleagues and its managers onto a USB stick (thumb drive). The Court considered that, because the USB stick was connected to the employee's work station, there was a presumption that the USB stick was being used for professional purposes, and thus the employer was authorised to access the files stored on that USB stick without the employee being present.[35]

In the context of Bring Your Own Device, the Court of Cassation seems to have taken the position that, where an employee uses a personal device for professional purposes, it is presumed that the documents and files stored on that device are work-related, and thus may be accessed and viewed by the company. To prevent a possible breach of privacy, employers are advised to draft clear privacy policies, explaining to employees how to use their personal devices at work and how to avoid private documents from being scrutinised by their employer.[36]

The rules outlined above do not apply in the context of a civil or criminal investigation (*e.g.*, where an employee is suspected of stealing trade secrets), or where the company has obtained a court order authorising it to access an employee's computer. In the latter situation, the Court appoints a bailiff in charge of retrieving and securing any documents, emails or files stored on an employee's computer that may be used as evidence against that employee.[37] On several occasions, the Court of Cassation ruled that a court order granting en employer access to an employee's computer files does not constitute a violation of that employee's right to privacy.[38]

Companies may also need to access an employee's computer files in his/her absence (*e.g.*, when the employee is absent or on sick leave). In that case, a company cannot ask its IT department to disclose an employee's login and password in order to access his/her computer during his/her absence, even if access is limited to professional files.[39] However, an employee has a duty to cooperate with his employer and may be required to disclose in advance his login and password when necessary to maintain business continuity, and when the documents cannot be otherwise accessed.[40]

Access to Employee Emails

Emails that are marked "private" are considered to be private correspondence.[41] As with computer files, the use of emailing systems in the workplace is presumed to be professional; thus, an employer can access an employee's inbox, with the exception of emails that are marked "private" in their subject line, or those that are stored in a sub-folder of the inbox marked "private". These rules also apply during an employee's absence.[42]

The difficulty for companies is to know when they are authorised to access an email that is not clearly marked "private". In 2011, the Court of Cassation ruled that the content of an email alone is not sufficient to categorise it as private correspondence. For instance, even where a conversation between two employees commenting about their boss is private in nature, those emails could not be considered to be "private" because they are still related to work.[43]

However, the Court of Cassation also ruled that, if it appears clearly from the content of an email that it is private in nature, an employer cannot use that email as evidence to sanction an employee's behavior, even if the email is not marked "private".[44] In other words, an employer is authorised to access emails that are not marked "private", but cannot use them in court as evidence of an employee's fault if the content of those emails turns out to be of a private nature. Therefore, employers are banned from using emails against their employees that are not work-related.

To avoid such situations, companies are advised to explain to employees in a privacy policy the rules regarding the use of emails. However, companies must be careful not to be too restrictive when drafting their policies. In a recent decision, the Court of Cassation ruled that an employer was prohibited from accessing all employee emails, including professional emails, without the presence of the employees, because the company's internal policy required the presence of the employees at all times.[45]

Monitoring Use of the Internet

In France, companies cannot prohibit employees from using the internet for private purposes during working hours, because that would be deemed a disproportionate restriction on the rights and freedoms of employees, under labour law.[46] Based on the CNIL's guidelines,[47] companies must authorise a reasonable and proportionate use of the internet during working hours as long as it does not have a negative effect on the security of the network, or on the employees' work productivity.

The Court of Cassation ruled that, when the internet is accessed by an employee from a company-owned computer, there is a presumption that the internet is being used for business purposes.[48] Based on this presumption, employers can monitor use of the internet by their employees, and, in particular, may access a computer's log files in the absence of the employee. The Court also considers that companies have a valid cause of action for laying off an employee who spends a disproportionate amount of time on the internet for private or unlawful

   ISSN 1473-3579

purposes.[49] Furthermore, the web pages that are saved in a web navigator's favourites and bookmarks are not considered as private files; thus, companies can also search within an employee's favourites, without giving prior notice, to see what web pages that employee has visited.[40]

It is generally best practice to explain to employees what restrictions may apply to use of the internet in a privacy policy. Such policies may limit the use of the internet, for example, by prohibiting employees from accessing certain websites, or downloading software onto their computers, without prior approval. However, companies cannot use keylogging[51] software to monitor the activity of their employees on a permanent basis. The CNIL considers the use of such technology to be disproportionate and unlawful, unless it is justified by a high security imperative (*e.g.*, to combat the unauthorised disclosure of trade secrets).[52] Recently, the CNIL sanctioned a company for its covert use of keylogging technology on the grounds that it had violated the employees' right to privacy in the workplace.

Biometrics: Is Security More Important Than Privacy?

The use of biometric devices in the workplace has grown exponentially over the past years. Because biometrics can identify an individual based on his/her physical, biological or behavioural characteristics, the use of biometric devices is carefully scrutinised by the CNIL. In particular, the CNIL monitors the use of biometric devices to ensure that they are not used to track employees unlawfully.

Due to the high risk of intrusiveness, companies must obtain the CNIL's prior approval to implement a system that automatically processes personal data used by biometric devices to verify an individual's identity (*e.g.*, shape of the hand, fingerprint, iris, *etc.*).[53] The CNIL analyses the use of biometrics on a case-by-case basis, based on the documentation and information provided by the company, and determines whether the use of biometrics is lawful in each instance.

In a limited number of cases, the CNIL has adopted a "unique authorisation", describing the authorised use of biometrics in a particular context (*e.g.*, to control access to the work premises). Where the controller meets the conditions set out by the CNIL, it is simply required to adhere to the said authorisation without having to apply for approval.

In the employment context, the simplified approval procedure applies to the following types of biometric processing:

- the recognition of the shape of the hand used to control access to the work premises, including the company restaurant (unique authorisation n° AU-007);
- the storage of the employee's fingerprint on a unique device held by the employee and used to control access to the work premises (unique authorisation n° AU-008); and
- the recognition of the finger veins used to control access to the work premises (unique authorisation n° AU-019).

Recently, the CNIL removed the monitoring of working hours from the list of authorised purposes under its unique authorisation AU-007.[54] The CNIL has granted companies a five-year grace period to amend their biometric systems in accordance with the revised unique authorisation, or they may otherwise obtain the CNIL's *ad hoc* approval.

In accordance with the French Data Protection Act, employees must be informed about the use of a biometric device, whether the collection of their data is obligatory or optional, the identity of the recipients of the data, and how to exercise their privacy rights (*i.e.*, right to object to the processing, right to access and rectify their personal data).[55] The company must also inform and consult the Works Council (or employee representative bodies) about the use of a biometric device, in accordance with the Labour Code.[56]

Due to the high risk of identity theft, the CNIL prohibits the use of biometric systems that store fingerprints in a centralised database, unless it is justified by the need for high-level security to access a restricted area (*e.g.*, a nuclear plant or a vaccine production site). Recently, a supplier of security devices was convicted by several courts in France for having knowingly sold to its customers an unlawful security system based on the use of fingerprints that were stored in a centralised database.[57]

Companies must implement appropriate security measures to authenticate and identify authorised personnel, and to prevent any unauthorised disclosure of the data.[58] For example, the CNIL approved the use of a multidimensional biometric device, based on the recognition of the fingerprints and the veins of the fingers, to control access to the work premises.[59] The CNIL considered that the combined used of two sets of biometric data limited the risk of identity theft. In addition, the company had implemented appropriate security measures because the data was stored on the biometric device, and not on the company's servers.

Non-compliance with these conditions can trigger heavy penalties. In 2010, the CNIL ordered a company to cease all use of its biometric system, which was used to control access to its premises. The company in question had implemented a biometric system, despite not having gained the CNIL's approval due to the lack of appropriate security measures.[60]

CCTV Cameras: Big Brother is Watching You

CCTV cameras are now commonly used in office buildings to ensure the safety of the workers and the premises. The CNIL reports, however, that 15 percent of the complaints received in 2012 concerned threats to privacy in the workplace and, in particular, the intrusiveness of CCTV cameras.

CCTV cameras are subject to two different legal requirements, depending on whether the cameras are placed in a public area or in a private area closed to the public.

When placed in a public area, and if used only to view the images without recording or storing the images, the use of CCTV cameras must be approved by the local state representative ("*préfecture*"). A "public area" is defined as any public area (*e.g.*, a street or public square), or a private area that is open to the public (*e.g.*, a supermarket, a city hall, a gas station, *etc.*). When placed in a private area, the use of CCTV cameras to view, record and store images constitutes a data processing activity, which must be registered with the CNIL. A "private area" is defined as any area belonging to the private or the public sector that is not open to the public (*e.g.*, office spaces, a parking lot reserved to employees of a company, a storage facility, *etc.*).

In the workplace, the use of CCTV cameras is generally justified by the necessity to maintain the security of the people and the premises, or to preserve evidence of any thefts or damage that may occur on the premises. Before installing a video surveillance system, companies must assess the potential risks (depending on the number of cameras used, the areas under surveillance, the hours of use, the purpose of use, *etc.*) to ensure that the cameras are used for a legitimate purpose and in a proportionate manner.

The CNIL underlines the importance of using cameras in a non-intrusive manner and of pointing them in the right direction.[61] For example, CCTV cameras may be used for security purposes and placed at the entrance and exit of a building, in front of emergency exits, or in the main halls and corridors of the building. They may also be used to film storage facilities in order to guarantee the safety of goods.

However, cameras must not be placed inside employee offices, or above the desks of employees working in open spaces. Cameras cannot be used to film employees at their work stations, except in specific circumstances, such as cashiers working in a supermarket (*i.e.*, to prevent thefts), or when employees are exposed to a particular threat. It is also strictly prohibited to place cameras in restrooms, recreational areas, or premises that are reserved for employee representatives and trade unions.

Cameras cannot be used to monitor employees on a permanent basis. In 2010, the CNIL ordered a transportation company to cease using two cameras that were pointing towards employees on the grounds that such use was disproportionate to the intended purpose.[62] Recently, the CNIL fined the co-owner's union of a building located in a busy commercial area of Paris for its disproportionate use of CCTV cameras which were being used to film a shopping arcade.[63] The security guards working in the shopping arcade had complained to the CNIL because they were being filmed on a permanent basis. After inspecting the premises, the CNIL realised that the cameras were not being used for security reasons, but were in fact used to monitor the activities of the security guards during working hours. The CNIL ruled that such use was disproportionate to the intended purpose and ordered the co-owners' union to cease all use of the cameras.

Covert surveillance, without informing the employees, is prohibited. Before installing cameras on the work premises, a company must consult the Works Council and inform it about the purpose of the cameras.[64] The company must also inform the data subjects (*i.e.*, employees and visitors) of the use of CCTV cameras, the recipients of the images and how to exercise their right of access, by posting a notice on the premises where the cameras are placed.

Companies using CCTV cameras must also implement strict security measures. Access to the images must be restricted to authorised personnel only (*e.g.*, security team) with the proper qualifications and training on surveillance methods. The images may not be stored more than a few days and must be deleted at the latest after one month. If an incident occurs, this gives the company sufficient time to view the images, and retrieve those that may be used as evidence in criminal or disciplinary proceedings. Those images may be kept for the full duration of the proceedings.

Conclusion

Inevitably, technology will continue to develop and to present companies with new opportunities for monitoring their employees. However, in the midst of the current debate over a new data protection regulation in the European Union, now more than ever seems to be the time for companies to assess their use of technology and to verify that it is being used lawfully.

NOTES

[1] See CNIL's 2012 Annual Activity Report, available at: http://www.cnil.fr/linstitution/actualite/article/article/bilan-2012-une-activite-en-hausse-et-un-pilotage-de-la-conformite-au-coeur-du-metier-de-la-cni/. See also Olivier Proust, "CNIL unveils 2012 annual activity report", published on April 29, 2013, available at: http://privacylawblog.ffw.com/2013/cnil-unveils-2013-annual-activity-report.

[2] See Article L.1221-6, French Labour Code.

[3] Délibération n° 02-017 du 21 mars 2002 portant adoption d'une recommandation relative à la collecte et au traitement d'informations nominatives lors d'opérations de recrutement.

[4] Article 8, Data Protection Act.

[5] Article L.1222-2, French Labour Code.

[6] Article 6, Data Protection Act.

[7] See "Zones bloc note et commentaires: les bons réflexes pour ne pas déraper", published on October 15, 2012, available at: http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/zones-bloc-note-et-commentaires-les-bons-reflexes-pour-ne-pas-deraper/.

[8] See "La CNIL adresse un avertissement à Acadomia pour des commentaires excessifs dans ses fichiers", published on May 27, 2010, available at: http://www.cnil.fr/linstitution/actualite/article/article/la-cnil-adresse-un-avertissement-a-acadomia-pour-des-commentaires-excessifs-dans-ses-fichiers/.

[9] Article L.1121-1, French Labour Code.

[10] Articles L.1221-8 and L.1222-3, French Labour Code.

[11] Article 10, Data Protection Act.

[12] Articles L.1221-8 and L.1222-3, French Labour Code.

[13] Article 32, Data Protection Act.

[14] Articles L.1221-9 and L.1222-4, French Labour Code.

[15] Article L.2323-32, French Labour Code.

[16] Article 39, Data Protection Act.

[17] See CNIL's guidance on recruitment (supra note 3).

[18] See "L'évaluation des salaries: droits et obligations des employeurs", published on May 11, 2011, available at: http://www.cnil.fr/les-

   ISSN 1473-3579

themes/travail/fiche-pratique/article/levaluation-des-salaries-droits-et-obligations-des-employeurs.

[19] See Délibération n° 2006-066 du 16 mars 2006 portant adoption d'une recommandation relative à la mise en ceuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public, available at: http://www.cnil.fr/documentation/deliberations/deliberation/delib/97/.

[20] See CNIL's guidance on the use of geolocation in vehicles ("La geolocalisation des vehicules"), published in January 2013, available at: http://www.cnil.fr/linstitution/actualite/article/article/protection-des-donnees-personnelles-au-travail-les-bonnes-pratiques/?tx_ttnews%5BbackPid%5D=91&cHash=b44a328a9faa3e742aa760326f3d7f63.

[21] Article L.1121-1, French Labour Code.

[22] Court of Cassation, labour chamber, 3 Novembre 2011, pourvoi n° 10-18036, available at: http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000024761408&fastReqId=1128855373&fastPos=1.

[23] Article 9, Data Protection Act.

[24] Article L.2323-32, French Labour Code.

[25] Article 32, Data Protection Act.

[26] Article 39, Data Protection Act.

[27] See "Un employeur sanctionné pour avoir refusé la demande d'un salarié voulant accéder à ses données", published on July 9, 2012, available at: http://www.cnil.fr/linstitution/actualite/article/article/un-employeur-sanctionne-pour-avoir-refuse-la-demande-dun-salarie-voulant-acceder-a-ses-donnee/?tx_ttnews%5BbackPid%5D=91&cHash=83a9b85fc72923f0bf14c2139aa0a39d.

[28] Court of Cassation, Labour Chamber, October 2, 2001, *Nikon France v. M. Frédéric Onof*.

[29] Court of Cassation, Labour Chamber, May 17, 2005, *Philippe X. v. société Cathnet-Science*.

[30] Court of Cassation, Labour Chamber, October 18, 2006, *M. X v. société Techni-Soft*.

[31] Court of Cassation, Labour Chamber, October 21, 2009, *Jean-Michel X. v. Seit Hydr'Eau*.

[32] Court of Cassation, Labour Chamber, December 8, 2009, *M. X v. FNGDSB*.

[33] Court of Cassation, Labour Chamber, May 10, 2012, *M. X. . . v. Nouvelle communication téléphonique*.

[34] Court of Cassation, Labour Chamber, July 4, 2012, *M. X. . . . v. SNCF*.

[35] Court of Cassation, Labour Chamber, February 12, 2013, *Mme X. . . . v. PBS*.

[36] See Olivier Proust, "Is BYOD secure for your company?", published on May 24, 2013, available at: http://privacylawblog.ffw.com/2013/is-byod-secure-for-your-company.

[37] Article 145, French Code of Civil Procedure.

[38] Court of Cassation, Labour Chamber, May 23, 2007, *M. X. . . . v. société Datacep*; Court of Cassation, Labour Chamber, June 10, 2008, *Mme X. . . . v. société SIMEP*.

[39] See CNIL, "Peut-on accéder à l'ordinateur d'un salarié en vacances?", published on July 19, 2010, available at: http://www.cnil.fr/les-themes/travail/fiche-pratique/article/peut-on-acceder-a-lordinateur-dun-salarie-en-vacances/.

[40] Court of Cassation, Labour Chamber, March 18, 2003, *Mme X. . . . v. Union Mutuelle Solidarité*.

[41] Court of Cassation, Labour Chamber, May 30, 2007, *M. X. . . . v. The Phone House*.

[42] See CNIL, "L'accès à la messagerie d'un salarié en son absence", March 26, 2012, available at: http://www.cnil.fr/les-themes/travail/fiche-pratique/article/lacces-a-la-messagerie-dun-salarie-en-son-absence/.

[43] Court of Cassation, Labour Chamber, February 2, 2011, *Securitas France c/ M. X.*

[44] Court of Cassation, Labour Chamber, July 5, 2011, *Mr. X. v. société Gan Assurances IARD*; Court of Cassation, Labour Chamber, October 18, 2011, *Mr. X. v. société Asco électronique*.

[45] Court of Cassation, Labour Chamber, June 26, 2012, *M. X. . . . v. YBC, Helpevia*.

[46] Article L.1121-1, French Labour Code.

[47] See CNIL's report on cybersurveillance in the workplace, published in March 2004, available at: http://www.cnil.fr/documentation/autres-ouvrages/.

[48] Court of Cassation, Labour Chamber, July 9, 2008, *M. X. . . . v. société Entreprise Martin*.

[49] Court of Cassation, Labour Chamber, March 18, 2009, *M. X. . . . v. Société Lauzin*; Court of Cassation, Labour Chamber, February 26, 2013, *Mme X. . . . . V. Dubus*.

[50] Court of Cassation, Labour Chamber, February 9, 2010, *M. X. . . . v. association Relais Jeunes Charpennes*.

[51] "Keylogging" is the action of recording (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that his/her actions are being monitored.

[52] See "Keylogger: des dispositifs de cybersurveillance particulièrement intrusifs", published on March 20, 2013, available at: http://www.cnil.fr/les-themes/travail/fiche-pratique/article/keylogger-des-dispositifs-de-cybersurveillance-particulierement-intrusifs/.

[53] Article 25, Data Protection Act.

[54] See "L'autorisation unique n° AU-007 ne porte plus sur les contrôles d'horaires des salariés", published on October 23, 2012, available at: http://www.cnil.fr/linstitution/actualite/article/article/lautorisation-unique-n-au-007-ne-porte-plus-sur-les-controles-dhoraires-des-salaries/.

[55] Article 32 of the Data Protection Act and Articles L.1222-3 and L.1222-4 of the French Labour Code.

[56] Article L.2323-32, French Labour Code.

[57] See "Biométrie: condamnations judiciaires en série pour la société Easydentic", published on March 14, 2011, available at: http://www.cnil.fr/linstitution/actualite/article/article/biometrie-plusieurs-condamnations-judiciaires-contre-la-societe-easydentic-1/.

[58] See "La biométrie sur les lieux de travail", published on December 17, 2012, available at: http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/la-biometrie-sur-les-lieux-de-travail/.

[59] See "Première autorisation pour un dispositif biométrique multimodal", published on June 15, 2011, available at: http://www.cnil.fr/linstitution/actualite/article/article/premiere-autorisation-pour-un-dispositif-biometrique-multimodal/.

[60] See "La CNIL ordonne l'interruption d'un dispositif biométrique illégal", published on May 30, 2010, available at: http://www.cnil.fr/linstitution/actualite/article/article/la-cnil-ordonne-linterruption-dun-dispositif-biometrique-illegal/.

[61] See CNIL's guidance on the use of CCTV cameras ("La vidéosurveillance-videoprotection au travail"), published in January 2013, available at: http://www.cnil.fr/linstitution/actualite/article/article/protection-des-donnees-personnelles-au-travail-les-bonnes-pratiques/?tx_ttnews%5BbackPid%5D=91&cHash=b44a328a9faa3e742aa760326f3d7f63.

[62] See "Interruption en urgence d'un système de videosurveillance permanente des salariés", published on May 20, 2010, available at: http://www.cnil.fr/linstitution/actualite/article/article/interruption-en-urgence-dun-systeme-de-videosurveillance-permanente-des-salaries/.

[63] See "La CNIL sanctionne la surveillance permanente de salaries", published on January 23, 2013, available at: http://www.cnil.fr/les-themes/videosurveillance/fiche-pratique/article/la-cnil-sanctionne-la-surveillance-permanente-de-salaries/.

[64] Article L.2323-32, French Labour Code.

Olivier Proust is Of Counsel at Field Fisher Waterhouse LLP, Brussels. He may be contacted at olivier.proust@ffw.com.