NYMITY

Privacy Interviews with Experts
July 2011

Toronto / Washington DC / Brussels
www.nymity.com

Raphaël Dana
Partner
Sarrut Avocats
Paris, France

2011 Overview of Employment and Employee Privacy Laws and Key Trends in France

While employee privacy regulation in France is nothing new, it is becoming more complex as the world becomes more and more digital, the workforce more mobile, economies more fragile and various types of laws within and across economies converging. The French economy and the French worker is no exception to being affected by this phenomenon. It is important for companies resident in France, companies operating web-sites assisting French workers and multi-nationals to understand French labour, privacy and even export laws as they relate to the overall employment life cycle.

Raphaël Dana, attorney and partner with Sarrut Avocats in France, provides with us with an overview about current employment law, related employee privacy laws, impending laws and regulations and the key trends in France. Raphaël highlights the unique aspects of employee privacy and data protection today and in the coming years in France as well as some of the major risks and more importantly mitigating controls that are necessary for those of us that do business in France to understand.

Raphaël Dana is a member of the Paris Bar and a Partner at Sarrut Avocats. He has drafted and negotiated numerous French and English contracts and legal documentation concerning records retention, the internet, whistleblowers, global corporate privacy, and transborder data flow, among others. He has written articles concerning Data Protection Law and policy, and has spoken at various domestic and international panels. His profile can be seen on his firm's website at www.sarrut-avocats.com. He provides us with a data protection backgrounder and addresses the current hot topics in data protection in France. He highlights the unique aspects of data protection in France as well as some of the major risks and more importantly mitigating controls that are necessary for those of us that do business in France.

Nymity: What are the employment related laws and regulations in France that have a direct impact on employee privacy?

Dana: Employment related laws that have a direct impact on employee privacy are mainly:

- The Act 78-17 of 6 January 1978 covering data processing, data files and individual liberties (after Data Protection Act or DPA),
- The European Convention for the Protection of Human Rights and Fundamental Freedoms "ECHR" (notably Article 8),
- The Civil Code (notably Article 9),
- The Labour Code,
- The Penal Code,
- Employment Law 82-689 of 4 August, 1982 related to the freedoms of employees in the work place,
- To be taken into account are the deliberations and reports of the National Commission of Information and Liberties (CNIL),
- And among other EU Directives, the European Directive 95/46 of 23 November 1995 (the Directive).

Nymity: What is the scope of these employment related laws and regulations? What data is covered? What entities does the law apply to?

Dana: The above-referenced legal texts basically apply to individuals and their personal data as defined by the DPA (data that allow the identification of an individual). Article 1 of the ECHR states that the State Parties to the Convention shall secure the rights and freedoms as defined in Section 1 of the Convention (Articles 2 to 18) to everyone within their jurisdiction. The Civil Code has a general scope; the Labour Code and employment laws usually apply when there is an employment relationship.

Nymity: Does the law apply outside of its jurisdiction, be it a state, province or country?

Dana: ECHR applies to all states that have joined the Convention and other laws apply only in the French territory.

Nymity: What are the employee consent requirements?

Dana: To provide an example, per Articles 8 & 9 of the DPA, it is prohibited without the express consent of the individual, to collect and process personal data that reveals directly or indirectly, the racial and ethnic origins, the political, philosophical, religious opinions or trade union affiliation of persons, or anything concerning their health or sexual life.

In the case of refusal, the employer cannot collect this data.

Nymity: In general what does the employee privacy law/regulation require, by privacy principle?

Dana: The right to the respect of privacy and family life (for example for people who work by telecommuting) including home and correspondence.

The five key principles to follow when collecting data are:

- the principle of finality (specific purpose and legitimate use of data)
- the principle of proportionality and relevance of the data (only the information relevant and necessary in the light of the objectives must be processed)
- the principle of a limited duration of keeping of the data
- principles of an adequate level of security and confidentiality
- the principle of respect for the rights of people (employees must be informed of their access, correction and opposition rights)

Nymity: What are the works council and union laws/regulations that relate to employee privacy and data protection?

Dana: The "labour laws" that are related to the privacy of workers mainly consist of:

- Labour Code, Article L.2142-6 and Act 82-689 of 4 August 1982,
- Act 2004-391 of 4 May 2004 on vocational training throughout life and social dialogue.

Also in the instance when an employer's representative has a dedicated e-mail account, special security measures should be defined and implemented to ensure the confidentiality of information exchanged (Internet surveillance in the workplace, summary, 11 February 2002, CNIL).

Nymity: Do you have a Data Protection Authority or regulator and if so who is the Data Protection Authority or regulator?

Dana: In France, the Data Protection Authority and Regulator is the "Commission Nationale de l'Informatique et des Libertés" (CNIL), or National Commission on Information and Liberties. They are an independent administrative authority that protects privacy, personal data and public liberties. Their general mission is to ensure that the development of information technology remains at the service of citizens and does not breach human identity, human rights, privacy or personal or public liberties.

Nymity: Is there a Registration/Notification requirement of a company with the Data Protection Authority or regulator for collecting and/or processing Employee Personal and Sensitive Personal Data?

Dana: Yes - various exemptions exist for common personal data linked for instance to HR management; their collection however requires the filing of specific declarations with the CNIL.

Sensitive data may only be collected for specific and justified purposes, after authorization by the CNIL.

Nymity: If your Data Protection Authority is active, what has been their primary focus relating to employee privacy? What types of fines have they issued during the last calendar year if any?

Dana: The French CNIL is quite active.

Among the recent developments, on 3 March 2011, for the first time, the Commission authorized two companies to develop a "whistle-blowing" system dedicated to professional complaints and claims for discrimination. These systems are part of the "Diversity Label".

One of the latest focus of attention is the issue of biometrics systems in the workplace.

Usually, when the CNIL finds a problem for the first time, it only issues a warning. After that, if the problem continues, it can decide to apply fines. So far the CNIL has pronounced financial sanctions in some cases, not always deciding to make such fines public (nine fines in 2007 ranging from 5,000 Euros to 50,000 Euros).

One of the last fines in relation to work was delivered in late 2009: the CNIL delivered on 16 April 2009 a financial penalty amounting to 10,000 Euros against a "ready to wear" clothing company which was the subject of several spot checks. Under the guise of fighting against theft, this company had set up a video surveillance system, which filmed employees on a permanent basis, including places where no goods were stored and without the employees having previously been informed.

Nymity: Are there laws/regulations regarding international transfers of Employee Personal or Sensitive Personal Data?

Dana: International transfers of personal data are notably regulated by Articles 68 to 70 of the Data Protection Act (DPA).

Data transfers are in principle free to the countries of the European Union and to countries providing an adequate level of protection of privacy and fundamental individual rights (they are so far Iceland, Liechtenstein, Norway, Switzerland, Canada, Argentina, Guernsey, Jersey and the Isle of Man). For the United States of America, only employers that have adhered to the "Safe Harbour" principles to ensure this level of data protection are to be considered.

However, even if data transfers to these countries are possible and do not require special authorization from the CNIL, where the transfer of data is listed in the Article 25 of the "DPA" (genetic data, data relating to breach of the law and convictions, etc.) authorization is still required. The fact remains, however that employers must comply with the obligations in terms of reporting and inform the individuals from whom data is collected.

Conversely, any transfer to a country outside the European Union or not providing a level of data protection equivalent to that provided in the EU is in principle prohibited, apart from the exceptions provided by the Act of Data Protection and Liberties. The application of these exceptions, however, takes place under the strict control of the CNIL by issuing an appropriate authorization. Some of these exceptions are:

- Consent of the person from whom data is collected;
- Safeguarding the interests of the person exercising a right to justice;
- Agreement between two companies involved in contract terms or internal rules (Binding Corporate Rules "BCR").

Nymity: Is there new or pending draft employee related data protection law(s) or regulations? What will they require companies to do? Is there an English version and if so where would it be located?

Dana: There are currently no new employee related data protection law or regulation projects, in France.

However at European level, there is a revision project of the EU directive 95/46/CE on data protection planned for the second part of 2011. The main topics are:

1) strengthening the rights of individuals

2) clarifying and simplifying data transfers rules outside of the EU

3) strengthening the role of national data protection authorities

It will be necessary to be attentive to this evolution as it will concern employees. The national data protection authorities, as well as other stakeholders, are presently being consulted by the services of the Commission.

Nymity: Currently what are the employee privacy and data protection practices that are common in your country?

a. Do most companies have internal employee privacy policies and external privacy notices for their applicants and employees?

Dana: Yes, a large number of large and medium sized companies have internal employee privacy policies and external privacy notices for their applicants and employees.

b. Are there specific privacy related laws that apply to applicants?

Dana: The laws that apply to applicants for employment are: "DPA" especially the Article 8, 9, 22 and 32, the European directive, the Labour Code articles L 1221-6 - L 1221-9, L 2323-32 and the CNIL deliberation 02 - 017 of 21 March 2002.

c. How do most companies address applicant and employee background checks for criminal and credit problem related activities? Are there certain restrictions that apply to the process?

Dana: Employee and applicant background checks for criminal problem related activities: In general the law does not allow employers to check the criminal record of a candidate before recruitment, except for some areas of business (eg security firms and funds transportation companies).

Employee and applicant background credit check problem related activities: The CNIL considers, except in special cases justified (for example by the nature of the work or rules in force in the country) that it is contrary to legal requirements to check the applicant's bank information's, borrowings or payment defaults.

d. How do most companies address various forms of employee testing, be it psychological, skills, drug or alcohol related testing? What employee rights are protected by law related to employee testing?

Dana: The results obtained by recruiting tests and candidates assessment for employment must remain confidential. These methods must be relevant to the aim pursued. The CNIL recommends that the information should be provided prior by written individually or collectively form.

Any **applicant or employee** must be able to request any relevant information about it. And this must be provided within a reasonable time frame. The information may include the results of analysis and test (ie. psychological, handwriting, etc.) and any other professional assessments that may have been carried out.

The right of access applies to information collected directly from the candidate, also to any information collected from third parties as well as information from methods and techniques for recruitment assistance.

The CNIL recommends that the disclosure of candidate information should be in writing. Employees have the right to dispute the accuracy of the information except when it is established that the disputed information has been provided by the person concerned or with their consent.

Communication of test results or assessment may be made by any appropriate methods depending on the nature of the tool.

e. How do most companies address employee data security and eMail and internet monitoring? Have organizations implemented additional employee monitoring measures? If so, what do these monitoring measures included? What employee rights are protected by law from employee monitoring?

Dana: Because of the diversity of new communication tools, the risks to companies have increased. Email may be monitored by the employer provided they meet the transparency requirements imposed by the Labour Code and the Data Protection Law (information to employees, information and consultation of the Works Council and declaration to the CNIL).

Regarding the risks associated with downloading files or external software (pirating), any corporate rules should indicate the internal practices that are prohibited in order to limit the liability of the company.

The collection of data published on the Internet must respect, on pain of criminal penalties, the rules laid down by the Data Protection Act and the Digital Economy Act; for example having to inform all parties concerned about the procedures that have been put in place.

f. How are most companies addressing international transfers and contracting with controllers, service providers (vendors/suppliers and their sub-vendors/suppliers, when it relates to employee personal and sensitive personal data?

Dana: Paragraph 8 of Article 69 provides that there it may be an exception to the prohibition on transferring data outside the European Union "where the process guarantees a sufficient level of protection of the individuals' privacy as well as their liberties and fundamental rights and, in particular regarding contractual clauses or internal rules relating to the process. Thus, two additional exceptions are possible.

First, an agreement to organise the data transfer can be made between two controllers or between a controller and a processor. This agreement must be submitted to the CNIL for validation. To facilitate the work of contractors, the European Commission has provided three sets of standard contractual clauses, one for transfers between controller and sub-contractor and the other two for transfers between controllers (in English).

Although not mandatory, the use of these clauses can reduce the risk of refusal of authorisation from the competent national authorities.

Secondly, any company can transfer personal data to another subsidiary of its group in a country outside the European Union provided they ensure an adequate level of protection. For this to happen, it is a condition that the group must have adopted a Binding Corporate Rules, validated by the CNIL. This alternative to the adoption of contractual terms is for multinationals because only companies belonging to the same group can benefit.

In all cases, the authorisation granted by the CNIL to make data transfers under contractual or internal rules can not in any way relieve the controller from compliance with the formalities of declaration and information.

g. What about whistle-blowing hotline requirements? Are special measures necessary for implementing such hotlines?

Dana: First, the CNIL have refused to authorize the implementation of such devices. In a deliberation on 26th May 2005, they considered such measures to be disproportionate in view of the overall objectives and the possible risks of slanderous denunciations. This raised a problem for the French subsidiaries of American companies which had to respect the contradictory measures of the French law "DPA" and those of the Sarbanes-Oxley Act. That is why in a decision on 8th December 2005, the CNIL authorised these devices. This deliberation was modified by a further deliberation on 14th October 2010 (N°2010-369).

The authorisation concerns only “whistle-blowing” hotlines answering a legislative or statutory obligation of French law in the following domains: financial, accounting, banking and the fight against corruption. The whistle-blowing schemes must be previously declared to the CNIL, which issues a unique authorization numbered AU004 adopted December 8, 2005, thereby recognizing the Sarbanes Oxley Act.

Besides the legal device, a circular of the Direction Générale Du Travail on 19th November2008, relative to “whistle-blowing” hotlines specifies that:

- the use of this device has to remain optional,
- the works council “comité d’entreprise” has to be consulted, according to the article L2323-32 of the French Code du Travail, and the employees have to be informed before the implementation of this device. Otherwise, the device is considered as illegal.

h. What are companies doing about employee privacy issues that arise during e-Discovery and forensic research into security breaches, Foreign Corrupt Practices Act/Briber Act violations, fraud and cyber-attacks?

Dana: It is the responsibility of directors and managers of information systems to manage these risks. But companies also provide themselves with the Internal Corporate Rules: IT Charter or the Charter of good use of resources or Internal Regulation which should predict risks, the methods of prevention and intervention, and the penalties for wrongful use of these tools.

The CNIL considers that companies and governments that provide Internet access to their employees are not concerned by the obligations to retain data traffic on the Internet of its employees. In addition, an employer has the right to develop a monitoring system of the activities of its employees (messaging control, websites accessed, etc.), only when a number of safeguards have been met.

Data can still be shared with third parties allowed under special legislation (labour inspections, tax offices, police, etc.).

Nymity: What are the hot topics in employee data protection and privacy in your country? What are the risks and what are you recommending to clients to address those risks?

Dana: The hot topics are the problems with discovery in the United States of America, video surveillance, the use of biometry, and security breaches.

When handling any of these items without proper local guidance, companies can be sanctioned with the risk of the publication of the sanction (it could affect the image of the company) and also can be sued for damages.

We advise our clients through the various steps which require a case-by-case analysis.

Nymity: In closing, do you anticipate additional significant changes from the authorities relating to employee privacy? If so, what might these changes include and from where will they come?

Dana: There is nowadays, no pending legislative changes related to employee privacy in France. Furthermore, it is necessary to remain attentive to the revision of the directive we have already evoked. Indeed there is a revision project of the EU directive on data protection, planned for the second half-year 2011 by the Commission.

However, we can report on a case law that has been developing these few last months about the dismissal of employees having offended their employer on Facebook.

Three employees fired by their company Alten in 2008 have lost their case at the Employment Tribunal. They had criticized their hierarchy on their respective Facebook walls and had been denounced to the company by a former colleague. The company fired them in 2008, but the employees had subsequently taken the case to the employment tribunal, arguing that the decision was an abusive intrusion into their private life. The employment tribunal dismissed them and stated that the layoffs were justified, as Facebook is “an open space” (subject to private settings which had not been activated in these cases).

The use of comments held by employees on their Facebook page, which had been parameterized to allow the sharing with “friends and their friends”, doesn’t violate the right to respect for their private life. And it is a proof which can be provided in support of a dismissal.