GETTING PERSONAL: THE TENSION BETWEEN SOCIAL MEDIA & WORK

A French Perspective

Stephane Coulaux	Valerie Maricot
Coulaux-Maricot-Georganta (CMG Legal)	Coulaux-Maricot-Georganta (CMG Legal)
coulaux@cmglegal.net	maricot@cmglegal.net

AN INCREASINGLY CHALLENGING ENVIRONMENT

An ever-increasing volume of personal data is collected, accessed, used and transferred as a result of the rapid pace of technological change and globalization. New ways of sharing information through social networks and storing large amounts of data remotely have become part of life for most of the internet users.

At the same time, personal data has become an asset for many businesses but also employers. Collecting, aggregating and analyzing the data of potential customers are often an important part of their economic activities. As employers, businesses may also tend to check on the profile of potential employees as well as try to exercise a control over the information and data that are used, transferred or accessed by their already-existing employees. Traditional concerns for employers in this respect have included e.g. the need to protect trade secrets and concerns about conducts leading to liability to third-parties, or potential criminal activity. In pursuing legitimate interests, employers may come across information and data that would otherwise be considered as belonging to the private sphere.

While technological developments provide employers with new tools to monitor employees' electronic activities in the workplace, they also create new risks of liability for invasion of privacy, sources for silent discrimination as well as potentially adverse impact on employees' trust and comfort inside and outside their workplace.

DISCRIMINATION AT STAKE IN THE HIRING PROCESS

According to articles L.1132-1, L.1221-6, L.1221-8, L.1221-9 and L.2323-32 of the French Labor Code:

- Any potential candidate (as well as employees' representatives as the case may be) must be informed of all the recruitment methods and techniques that may be used by the employer, prior to their implementation;
- The information collected must be in direct connection to the job description and strictly limited to assessing the professional skills in relation thereto;

- Age, gender, family status, origins, political opinions, social conducts, sex orientations, religious convictions, genetics criteria, health, handicaps, physical appearance, pregnancy, union activities must not be taken into account in the hiring process.

Besides, the collecting, processing and storage of personal data are strictly regulated by the Data Protection Act of 6 January 1978 (as amended) which imposes consent of and disclosure to the individual concerned.

When used in order to profile candidates, data collected from social media platforms constitute an intrusion into privacy that may not be balanced by the employer's legitimate interests, and carry serious risks of discrimination.

Criminal sanctions are at stake for the employer.

However, considering that the digital identity of candidates and employees often go far beyond what is strictly connected to a job position, it has proven extremely difficult, if not impossible, for individual to evidence being a victim of discrimination, irrespective of the source of the data, especially at the hiring process stage. The 7 May 2008 Law therefore organized a shift of the burden of proof before civil courts: subject to gathering sufficient fact-elements, the employer bears the burden of establishing the absence of discrimination.

THE USE OF SOCIAL MEDIA AND THE WORKPLACE

In principle, employees have a right to a reasonable use their employer's communication systems and device for private matters. They enjoy a right of secrecy concerning their private correspondence. Unless expressly marked to the contrary, data exchanged by the employee are presumed to be of professional nature hence accessible by the employer without the employee being present (Cass. 15 Dec. 2010). Their contents cannot ground a sanction if they are of a private nature and do not violate the employer's legitimate interests (Cass. 5 July 2011).

International, EU and French legislations protect the employees' freedom of speech. The constitutional right to express opinions about their conditions of employment, inside and outside of the workplace, cannot lead to disciplinary sanctions, subject to the existence of libel, slander, the use of unduly excessive terms or evidence of a disloyal behavior, or the breach of confidentiality provisions. While employers' disciplinary power is traditionally exercised within the frame of the performance of the employment contract, it may also extend beyond such time and place when and where violations of the employment contract's obligations are found to occur. Besides, events drawn out of an employee's private life may give rise to sanctions whenever they incur material and objective adverse consequences on the company's operations or reputation.

Several court decisions considered that terms posted by employees on the "*wall*" of their social media account or other persons' "*wall*" were of a public nature as they could be accessed by a large number of people: "*With respect to its purpose and its organization, Facebook must be considered as a public space; it is the user's responsibility to activate the adequate confidentiality settings*". They recognized the employer's right to issue disciplinary sanctions if the terms used went beyond the limits of freedom of speech, irrespective of whether the social media was used during or outside work hours (Reims 9 June 2010; Boulogne-Billancourt 19 Nov. 2010; Béthune 14 Dec. 2010; Besançon 15 Nov. 2011; Paris 17 Jan. 2012).

PATH TO BEST PRACTICES: PUBLIC AND PRIVATE INITIATIVES

Since 2005, companies have been able to appoint a Data Protection Officer ("DPO"), whose tasks consist, among others, in ensuring in connection with the French Data Protection Authority (DPA) that data protection rules are strictly obeyed. The appointment is not, however, mandatory. There are 2877 DPOs currently in exercise in France and 10266 institutions have appointed a DPO.

In January 2011, the DPA issued recommendations regarding the use of social media platforms by employees. Through a series of reminders the DPA stresses out the employee's responsibility to activate and adapt the minimum adequate security and confidentiality settings. On 11 May 2012, in collaboration with the newly-created "Guardian of Civil Rights" the DPA symmetrically issued a report containing guidelines and analytical tools aimed at employers in order to give them the means to ensure equal opportunities within their organization.

Interestingly, the Law of 31 March 2006 provided for the obligation, for companies of more than 50 employees, to resort only to "anonymous curriculum vitae" (i.e. with contents limited to the assessment of a profile to a given list of professional requirements) in the hiring process. A survey report issued in March 2011 revealed that this practice actually increased the chances of discrimination. On 17 August 2011 a government representative declared that this initiative was therefore not be made binding.

Among private collective initiatives, "EQUAL SKILLS" a private society released for signature a policy charter aimed at companies of the private sector, and especially recruitment companies, setting-up guidelines and commitments to obey:

- To refrain from accessing personally-oriented social networks, use them only in order to post job offers and to contact only those users that gave their prior consent thereto,
- To give preference to the use of professionally-oriented social networks,

- To refrain using search engines and social networks to collect or gather data of a personal nature, even when such data are posted on a publicly accessible space,
- To conduct ongoing information to their employees about the use of social networks,
- To provide information to the social networks users about the necessary precautions to be taken when posting information and about the assurance they must receive that they can subsequently delete any information they posted and therefore the actual exercise of their "right to be forgotten",
- Whenever necessary, take contact with the editors of internet sites that host social networks, blogs, search engines and more generally any personal data of the need to provide full and loyal information to their users about the site's purpose, the persons who may access it and the duration of storage of the data.

To date about 110 companies have signed the charter.

Individual private initiatives with respect to the use of social media involve, for employers, one of three possible attitudes: to ignore it and let go, to forbid it, or to set-up reasonable conditions of use. For obvious reasons, letting go is not the best option, although the most frequent one. To forbid it during working hours may be possible, but under strict information and transparency conditions *vis-à-vis* employees. The third option is not the easiest but the most recommended one. It must aim at determining an incentive policy of use of social media in the interests of the company. The employer must establish clear, readable and simple rules of use, in collaboration with any union or other body representing employees, with a view to:

- Enhancing the obligation of confidentiality contained in the employment contracts and the employment by-laws;
- Recalling and emphasizing the duty of loyalty;
- Detailing the monitoring and controlling means;
- Determining the sanctions in case of violation.

Other actions of this type include the creation of a "Company Social Network", which consists in a private business-oriented declination of any other commonly-known social network, with a view to creating a platform of interaction, exchange of ideas, information and documents.

Beyond security measures designed to protect any strategic information, the employer must take into account the data protection regulation, the duty to ensure mental health and safety to employees, the organization of actions and sanctions in case of misuse, and any collective agreement and disclosure as may be needed *vis-à-vis* the employees and/or their representatives.

PERSPECTIVES

On 25 January 2012 the EU Commission issued a press release quoting a few figures revealed by a survey conducted on *Attitudes on Data Protection and Electronic Identity in the European Union* (Special Eurobarometer 359, June 2011):

- 74% of Europeans see disclosing personal information as an increasing part of modern life.
- The most important reason for disclosure is to access an online service, for both social networking and sharing site users (61%) and online shoppers (79%).
- 54% of internet users are informed about the data collection conditions and the further uses of their data when joining a social networking site or registering for a service online.
- Just over a quarter of social network users (26%) and even fewer online shoppers (18%) feel in complete control of their data.

In the absence of efficient tools to limit the access and use by employers of personal data posted on social networks by their potential or actual employees, the practical control tools are limited to the employees' own initiatives and care, and the confidentiality and privacy policies edited by the social media editors. As Mark Schrems once put it "*the internet is not anonymous and it does not forget*". The EU Commission proposes a comprehensive reform of the data protection rules (EU Directive of 24 October 1995) that may help strengthening online privacy rights while boosting Europe's digital economy. It includes:

- Increasing the responsibility and accountability of those processing data by introducing compulsory DPOs for companies over 250 employees;
- Strengthening the "right to be forgotten", in order to empower people who no longer want their data to be processed while there are no legitimate grounds for retaining it, to delete the data;
- Introducing the principles of "privacy by default" and "privacy by design" to ensure that individuals are informed in an easily understandable way about how their data will be processed.

- Guaranteeing an easy access to one's own data;
- Establishing data portability, i.e. the right for individuals to freely transfer personal data from one service provider to another;
- Ensuring that consent must be given explicitly by individuals when it is required for certain types of data processing;

Since the 27 EU Member States have implemented the 1995 EU Directive rules differently, it resulted in divergences in enforcement. The action proposed by the EU Commission would therefore take the form of a single law that would do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around EUR 2.3 billion a year and more protection and certainty of individuals, including employees.