Mexico-2016

4th Study Commission-Public and social law

Topic 2016: « Social networks and labour relations »

<table>
<thead>
<tr>
<th>Abbreviations</th>
<th>Acts</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Canadian Charter</strong></td>
<td>Canadian Charter of rights and freedom</td>
</tr>
<tr>
<td><strong>Quebec Charter</strong></td>
<td>Charter of human rights and freedom (Quebec legislature)</td>
</tr>
<tr>
<td><strong>C.c.Q.</strong></td>
<td>Quebec civil code</td>
</tr>
<tr>
<td><strong>An act respecting the protection of personal information</strong></td>
<td>An act respecting the protection of personal information in the private sector (Quebec legislature)</td>
</tr>
<tr>
<td><strong>An act respecting access to documents</strong></td>
<td>An act respecting access to documents held by public bodies and the protection of personal information (Quebec legislature)</td>
</tr>
</tbody>
</table>

**Preliminary Remarks:**

Under the Canadian Constitution, jurisdiction over labour relations and working conditions is shared between the provincial and federal legislatures. Legislation regarding labour relations is presumptively a provincial matter. However, the federal government is entitled to regulate labour relations in connexion with employees who fall within Parliament’s competence (navigation, banking, interprovincial transportation, etc.). Approximately 10% of the Canadian workforce is under federal jurisdiction. Federal jurisdiction applies regardless of the province where the employee is located.

The protection of privacy in the workplace, in Quebec, depends on the qualification of the employer as an entity under federal or provincial jurisdiction. Private federal enterprises are mainly covered by the **Canadian Labour Code**, the **Canadian Human Rights Act** and by the **Act on Personal information protection and electronic documents** while provincial private enterprises are essentially subject to the **Quebec Charter**, the **Quebec civil Code** and the **Act respecting access to documents**.
On their part, public enterprises are increasingly subject to the **Canadian Charter**. In addition, for public enterprises under Quebec jurisdiction, the **Act respecting access to documents held by public bodies and the protection of personal information** applies instead of the **Act respecting the protection of personal information in the private sector**. For the federal enterprises, the **Privacy act** replaces the act on **Personal information protection and electronic document**.

In order to simplify the analysis, this questionnaire was completed taking only Quebec legislation into account. Federal legislation and legislation from other provinces is not examined.

[1] **Does your country have laws or regulations that protect the confidentiality of electronic communications?**

The secret of electronic communication is not specifically protected by Quebec legislation, but it is through the right to respect for private life under art. 5 of the **Quebec Charter** and art. 3, 35 and 36 **C.C.Q**. This protection is closely linked to the notion of expectation of privacy without which there could be no violations of the employee’s right to privacy. The expectation of privacy depends on many factors which includes the determination of what is the access and dissemination of the communication, it’s nature, the relation between the person affected by it as well as the subjective expectation of privacy and its reasonableness. The right to privacy, like other fundamental rights, is not absolute. It is limited by art. 9.1 of the **Quebec Charter** (or art. 1 of the **Canadian Charter**, as appropriate) which allows intrusions into the privacy of an employee when they are required by law or where the employer seeks a legitimate and important goal, that the measure is rationally connected to the objective and that there is no other reasonable means of achieving it.

It is worth mentioning that art. 7 and 8 of the **Canadian Charter**, though they apply only in the presence of a governmental intervention (i.e. federal or provincial public enterprise), also protect the right to respect for private life.

The **Act respecting the protection of personal information** and the **Access Act** give the employee a protection. Under these laws, the employer, in order to legally constitute a dossier on a person, must have a serious interest to do so and should only collect information that is necessary for the dossier (Art. 4 and 5 **Act respecting the protection of personal information**; art 64 **Access Act**). He must also inform the employee of the
existence and the purpose of the dossier (art. 6 and 8 of the *Act respecting the protection of personal information*; art. 65 Access act).

Finally, art. 2858 C.C.Q. protects, albeit indirectly, the right to privacy by providing that «any evidence obtained under such circumstances that fundamental rights and freedom are violated and whose use should tend to bring the administration of justice into disrepute» should be rejected by the court. The employee subject to a disciplinary sanction may therefore invoke, in court, his right to respect for his private life and ask for the exclusion of evidence obtained by the employer in violation of this right.

[2] *If so, are these provisions applicable when the information is collected on social networks or blogs?*

These laws apply to information available on social networks and blogs. However, the degree of protection varies according to the reasonable expectation of privacy of the person providing the information. Thus, the protection will not be the same in the presence of a publication accessible to all (on a blog for example) or if the communication is limited to certain people only. In fact, the Quebec (and Canadian) courts recognize that social networks, although generally perceived as a public place, may also be private when the privacy settings restrict access to the publications. Moreover, the Supreme Court of Canada decided that the expectation of privacy may exist even in a public place. We must therefore assess each case on its particular facts and determine whether the person, by communicating this information, could reasonably expect it to remain in the private domain.

The *Act respecting the protection of personal information* and the *Act respecting access to documents* also apply to the dossier established by the employer using information collected on social networks or blogs. Indeed, these laws largely define the concept of personal information without consideration of the media on which the information is kept (art 2 *Act respecting the protection of personal information*; Article 54 *Act respecting access to documents*).

Therefore, these provisions also apply to the collection and use of information available on social networks or blogs.
[3] If so, are these provisions protecting the information collected or used by an employer:

- during the recruitment phase?
- In the course of the employment for disciplinary reasons or others?

a) During the recruitment phase

The employer may consult the information available on social networks about a potential employee, subject to the respect for private life. Thus, it will usually be allowed to check the communications made by a candidate provided he uses lawful means to do so. There is no problem when the information is readily available (you can think of a Facebook "open" profile (anyone can see it) or "semi-open" (the content is available to "friends" of his friends ")). There is no problem either when the applicant authorizes to the employer to access the information (in particular in accepting him as a Facebook "friend"). In the case of a "closed" profile, the employer may also obtain the information indirectly, for example when a person with access to the private content of the social network of a candidate communicates it to him. However, the employer is not allowed to access the content of the "closed" profile of a candidate by using a subterfuge (one can think of creating a fake profile) or by coercion exerted on the candidate or another person.

The information collected by the employer cannot be used to exclude candidates on discriminatory grounds, since discrimination in hiring, is generally prohibited (art. 10, 16 and 20 Quebec Charter). In addition, the employer who wishes to constitute a dossier on a candidate with the information available on social networks must respect the provisions of the Act respecting the protection of personal information (or the Act respecting access to documents).

b) In the course of the employment

The employee has a duty to act faithfully and honestly and not to use any confidential information of his employer (art. 2088 C.C.Q.). If he fails in his duty, he could face disciplinary measures that can go to dismissal. These obligations apply to communications made on social networks. Thus, an employer may impose sanctions on an employee when he finds out, on the
internet, that the employee has made false or fraudulent statements or that he openly criticized him. On the other hand, the information collection must be lawful and respect the employee privacy. It will therefore be necessary to assess the legality of the action of the employer, whether the communication in question is of the public or private domain. When the communication is private, we must balance the rights and interests involved to see whether the invasion of privacy is justified in the circumstances. Finally, the employer who establishes a dossier on an employee must also comply with the provisions of the Act for the protection of personal information (or Act respecting access to documents).

[4] Are the employees allowed to use social networks during working hours? If so, in which way?

The legislation does not govern directly the use of social networks during working hours. However, when it causes a drop in productivity, the use of social networks at work may violate the employee's duty of loyalty and could qualify as a robbery or "cyberloitering at work".

Employers generally do not allow the use of new technologies in the workplace and elaborate (more and more) often a policy on the use of the internet. Such a policy, which is an extension of the employment contract, can range from the outright prohibition of the personal use of the internet to more flexible rules allowing, under certain conditions, the use of the internet for other purposes than professional duties. Thus, repeated or serious transgression of the internet policy may result in disciplinary sanctions. In the absence of a policy prohibiting the internet, it is customary to allow the employee to use, in a moderate and reasonable way, internet for personal purposes during work, including using social networks. Finally, the adoption of an internet policy also allows the employer to diminish the reasonable expectation of privacy of the employee who uses social networks at work and facilitate the justification for the monitoring. Indeed, it will be difficult for an employee to claim that he reasonably believed that the information on the computer was private if there is a clear policy that indicates that the use of that computer should be exclusively professional.
Can the employer monitor the use of social networks by his employees during working hours? Outside of the working hours?

a) During the working hours

The stealing of time and the loss of efficiency at work are the main problems resulting from the use of social networks during working hours. The right to privacy tempers the employer's surveillance authority in respect of the use by employees of social networks. It is therefore important to check first whether the communications that the employer wants to monitor are part of the private or public domain. When the information is in the public domain, the employer may intercept and use it without the possibility for the employee to invoke his right to respect for private life. The employer may, for example, penalize the employee who publishes information accessible to all on Facebook during his working hours.

When communication is rather a private matter, the criteria for monitoring, in the traditional sense, apply to social networks. The reasonable expectation of privacy varies greatly depending on whether the technological tool (computer, smartphone, tablet) used to access social networks is owned by the employee or the employer. If the technological tool is owned by the employee, the information is protected by the right to privacy. The employer cannot therefore use the content of the tool to directly verify the use made of the employee during working hours. On the other hand, he may, if he has reasonable grounds to believe that the employee failed in his obligations, indirectly monitor the use that he made of his personal tool by installing, for example, surveillance cameras on the workplace.

If the technological tool is owned by the employer, the expectation of privacy rely on several factors. It will depend, in fact, if the employee could reasonably expect that the information contained on this tool, including data for determining the use made of it, would be kept confidential. Therefore, the expectation of privacy will depend on whether the employer authorizes or not the use of the technological tool for personal purposes. Thus, the employee cannot oppose his right to privacy if the employer checks the browsing history on a computer exclusively reserved for professional use. However, the solution is not so clear when the personal use of a technological tool is permitted, even in a limited way. The existence of an
internet policy can be very helpful in assessing the reasonable expectation of privacy of the employee. When information is a private matter, it has to be determined if the infringement of that right is justified in the circumstances to establish whether the monitoring is lawful or not.

In any case, before undertaking surveillance, the employer will have to suspect a breach, by the employee, of his duties or the commission of an offence. Accordingly, the monitoring cannot be a "fishing expedition" and it cannot be justified a posteriori.

b) Outside the working hours

The employee is required to meet its duty to act faithfully and not to use confidential information of his employer even after hours of work. He faces sanctions if he violates its obligations using social networks. Thus, an employee may be sanctioned especially if he attacks the employer's reputation, psychologically harasses a colleague, or is found to have lied to obtain a leave or justify an absence. The employer's management rights allow him to exert some control over its employees, but the way used to do so must be lawful. He can use information lawfully obtained to impose a sanction to the employee, which may even include dismissal in case of definitive rupture of trust.

The question of the legality of the access means to get information arises when employee challenges the penalty imposed and the court has to establish the admissibility of such evidence. This question is usually not a problem when the communication of the information is public and easily accessible. Indeed, the employer has the right to consult the information that is freely available to check what the employees say about him on the internet. It is also legitimate when the information comes from an employee who has a legal access to the content on social networks of his colleague (e.g. because of its status as a Facebook "friend"), or if the employee authorizes access to his employer. The employer may also ask the court for permission to consult the private contents of his employee's profile, particularly in order to complete his evidence. But the employer may not use a subterfuge or an indirect means to collect private information from an employee on the internet.

Regardless of the method used, the intrusion into privacy must be justified on rational grounds and required to verify the conduct of the employee. Before conducting surveillance, the employer must suspect that the
employee has breached his obligations. If the intrusion into privacy is not justified, the information collected by the employer in violation of this right may be inadmissible in evidence.

**Bibliography**


