

Employment & Labour - Argentina

Social networking in the workplace: rights and obligations

Contributed by [Marval O'Farrell & Mairal](#)

August 17 2011

[Monitoring](#)

[Limits and considerations](#)

[Impact of prohibition on equipment use](#)

[Blocking access in the workplace](#)

[Referencing social networking sites in disciplinary action](#)

[Limiting access outside the office](#)

[Are social networking policies standard practice?](#)

[Recent legal developments](#)

[Comment](#)

Employers and employees have a number of rights and obligations regarding the use of social networking in the workplace. Some of the main issues that have arisen in Argentina in relation to such use are detailed below.

Monitoring

Employers must consider the circumstances under which they are permitted to monitor the use of social networks (eg, Facebook or Twitter) by their employees at work. The use of social networking tools in the workplace is not regulated by a specific law; instead, the parameters and rules of such use are usually set out by employers and by individual case law.

The use of social networking tools is of increasing concern for employers. Under appropriate circumstances, employers are permitted to apply the general guidelines for monitoring email accounts and electronic systems to social network use, as well as powers of control and organisation. However, such control must be executed without restricting employees' privacy rights, to avoid providing employees with valid grounds to file complaints against their employers.

The Labour Contract Law (20,744) governs the majority of labour relationships in Argentina, but does not contain a specific rule on the use of social networks. Considering the boundaries established by companies' common practice and case law, a number of rules must be observed in order to minimise the risk of disputes with employees. Under the law, employers are permitted to monitor the use of work tools, and thus the time spent using social networking tools or sites. However, they may not intrude on their employees' privacy by, for example, accessing an employee's personal social networking account without authorisation.

Limits and considerations

Given that employers may monitor social network use by employees while at work under certain circumstances, it is important to consider the limits and considerations that apply to such monitoring, in respect of rights of privacy, data protection, consultation or consent from employee representative bodies and individual employee consent, among other things.

Privacy rights

In order to reduce the risk of claims regarding this or related issues, the limits of an employer's control over employees' social network use should be established beforehand in its privacy policy. Employers are therefore encouraged to issue a document for their employees to sign, in which each employee acknowledges the power of the employer in controlling his or her use of social networking tools in the workplace. This practice will minimise the risk of future claims by employees over invasion of privacy, but any action will nonetheless require an analysis of each specific case.

The courts have previously determined a rule concerning the use of email accounts, which can be applied by analogy to the use of social networking tools:

Authors

[Javier E Patrón](#)



[Enrique M Stile](#)



"if a company does not have a clear policy about the use of this tool, and it fails to advertise [to] the employee that such use would have to be executed exclusively for his/her labor activity and also fails to communicate the company policy about the correct use of those tools, it might [generate] in the employee a false privacy expectation."(1)

The courts have further determined that:

"it remains beyond doubt that the access to an informatic system and to [the] Internet granted by the employer to the employee has the characteristics of a work tool, which has to be used only to fulfill labor tasks and not for personal matters."(2)

Over the last few years, the courts have developed an increasingly broad concept of work tools, which now include not only email accounts, but also information technology, computers, software and the Internet, among others. However, there have been no cases in Argentina that consider the use of social networking sites in particular.

The courts validated a dismissal for just cause of an employee who had been using the email account provided by his employer during his work for personal correspondence, violating the parameters established by the company with regard to appropriate use of work tools. Consequently, it was determined that the worker had not complied with his main obligation, which was to render services to the employer.(3) Such argument could be applied to an employee who devoted a substantial portion of his or her working hours to the use of personal social networks.

Therefore, the employer may control the use of social networks at work within the limits explained above - that is, by monitoring the time spent by the employee and sites visited, but not by accessing the employee's own accounts without authorisation. In addition, employers must advise their employees of the limits of the use of the tools and the employer's power to control the correct use thereof.

Most employees will sign a privacy policy when starting work with a new employer. However, a more detailed document that specifically relates to the use of social networks will provide the employer with a stronger defence.

Data protection

From the employee's perspective, it is noteworthy that all tools used exclusively for work activities (eg, email accounts, computer hardware and software) fall under the broad control of the employer (provided that due prior notice as mentioned above is given), and consequently belong to the company. Email accounts and information systems (eg, computer hardware and software) belong to the company, as established by Section 86 of the Labour Contract Law. The law additionally states that the employee is obliged to maintain the work tools provided by the employer in perfect condition.

On the other hand, from the employer's point of view, Section 1 of Law 24,766 establishes the right of every individual or company to protect its data under special circumstances. It states that individuals and companies are entitled to prevent the unauthorised disclosure to third parties or the trade of information that may be legitimately under their control, provided that the information would be considered by the individual or company as secret and of commercial value.

Confidentiality regarding employers' information is also an obligation of the employee under Section 88 of the Labour Contract Law, which survives termination of the labour relationship. The courts have determined that:

"the conduct evidenced by the employee by communicating to another company a price of the company he was working for at the time, through Messenger, constitutes a violation of loyalty and trust obligations of the employee towards the employer and grants the latter the right to dismiss the employee with just cause".(4)

Methods for preventing the misuse of social networking tools in respect of information that employees may disclose or trade should be also established and documented in advance, in order to minimise the risk of eventual claims or damage to the company's reputation following such misuse.

In addition, the Data Protection Law (25,326) provides certain limitations in relation to personal information, especially cross-border transfers. The protection of personal data is governed by Section I of the law, as restated by Regulatory Decree 1558/2001. Argentina is regarded by the European Commission as providing an adequate level of protection for personal data transferred from the European Union.(5) The law is applicable to both individuals and legal entities. Sensitive data is governed by a restrictive regime. According to the law, 'sensitive data' is defined as any personal data that reveals any of the following:

- racial or ethnic origin;
- political affiliation;
- religious, moral or philosophic convictions;

- union activity; or
- information related to health or sexual orientation.

No one can be forced to disclose sensitive data. Data related to criminal records may be collected solely by the relevant competent authorities, within the scope of the applicable legislation. The law also sets out principles for the handling of employees' personal information, which must be considered when an employer is monitoring employees' use of social networks.

Consultation or consent from employee representative bodies

There are no specific rules on consent from work councils or bodies under statute, collective agreements or otherwise.

Individual employee consent

Despite a lack of specific regulation on the subject, the issue of employee consent could be framed under Section 64 of the Labour Contract Law, which establishes that "the employer has sufficient power in order to organize the company, exploitation or establishment economically and technically".

As a consequence, employees must comply with the policy determined by their employer, provided that such policy is no less beneficial than the general regulations. The only limitation of this power is that it must be well designed and functional in relation to the company's goals.

Other considerations

As mentioned above, in order to minimise the risk of claims or disputes regarding the use of social networking tools in the workplace, and as a result of the lack of legal regulation on the matter, the few rules (or common standards) on such use are usually established by case law and by company practice. Such standards should be organised by the company under the following parameters:

- the regulation of use of social networks in the workplace;
- the signing of a privacy policy (and a confidentiality agreement, if necessary) by employees;
- the implementation of a password system in order to access information tools;
- the training of executives, management and general employees in the correct use of information tools; and
- the specification and proof (even in court) of any misuse of social networking tools by employees.

Companies that fulfil such requirements will have an improved line of defence in hypothetical claims.

Impact of prohibition on equipment use

Where employers prohibit use of social networking sites at work, they must consider the impact on the use of equipment - both equipment provided by employers and employees' own devices (eg, personal mobile phones).

Employers' equipment

Employers have the power to organise the manner in which their employees render services. Therefore, if the use of social networking tools is not essential for the company's activity, the employer can prohibit their use during the workday and on company computers or workstations. This limitation must be fully and clearly explained by the employer (in a written document) prior to the commencement of work, so that there is no chance of misinterpretation by the employee. In addition, employers may block access to such sites, so that if an employee attempts to visit such sites, no access will be granted.

Given that established practice is a source of acquired rights in labour terms in Argentina, in the event that a company previously granted access and then blocked it, claims from employees may not be totally ruled out. The company would have a reasonable defence, especially if such employees had granted written consent, although this might still be disregarded under the so-called 'no waiver of labour rights' principle (Section 12 of the Labour Contract Law).

Employees' devices

Under the rules on the control of social networks tools on employees' own devices (eg, mobile phones), employees are obliged to be at the full disposal of the employer at all times during the working day. Therefore, the personal use of social networking tools without the permission of the employer may represent a distraction or breach of the employee's obligations, and would be sufficient grounds for termination of the relationship with just cause. However, while the employer may require full availability during working hours, it may not interfere with an employee's own device.

Blocking access in the workplace

Employers are permitted to implement any system that they consider most effective in order to organise work, provided that employees' privacy is not invaded. As a result, an employer may determine the websites that an employee is allowed to visit and those that are excluded. By stating that the use of the Internet must be work related, any misuse is then prohibited. Such limitation may be implemented by the employer through periodic controls and through blocking certain sites. It need fulfil only the general requirements for such control to be valid (ie, providing prior communication to the employee stating the control, within the limitations mentioned above).

Referencing social networking sites in disciplinary action

Employers must consider the extent to which it is permissible to refer to social networking sites when taking disciplinary action against an employee or for decisions on recruitment and selection.

Disciplinary action

When taking disciplinary action against an employee, in order to minimise the risk of future claims, the conditions and policy of use of social networking tools should be determined in advance. The employee will then be unable to argue that he or she lacked knowledge of a certain policy established by the employer regarding the topic.

According to the courts, any disciplinary action must be proportional to the misconduct. In addition, Section 242 of the Labour Contract Law, regarding dismissal with just cause, states that:

"the appreciation (of the dismissal) would be made in a prudential manner by the judge, considering the nature of the relationship that arises from a labor contract, according to the statutes of this Law and of the particular case".

Therefore, any disciplinary action - whether warning, suspension without pay or dismissal - must be imposed under a common-sense criterion and bear in mind the bias of labour courts towards employees. Employers must be very careful when taking such actions and must gather proof of the actual breach and their right to sanction the employee.

While the employer cannot access an employee's social network account without authorisation, in certain circumstances (and with duly notarised documents), information provided voluntarily by other users may be accepted as evidence, on a case-by-case basis.

Decisions about recruitment and selection

No standard rules exist on the use of social networks in recruitment and selection, but companies often refer to social networks when making such decisions. Analysis of such use on a case-by-case basis must be undertaken to determine the scope of such references in respect of the candidate's dignity and to reduce the risk of discrimination claims. Additionally, employers must remember that information from social networks may be inaccurate.

Limiting access outside the office

Limitations by employers on the use of social networking tools outside the workplace can be enforced only where such use is connected to the work of the company or may provide information about the employer to third parties (eg, an employee who mentions that he or she works for certain employer or who makes any false or inaccurate reference about his or her employer, superiors or co-workers).

In such cases, as in those analysed above, the employer must communicate company policy on such tools to the employee. Such policy must be in writing and signed by the employee. Any decisions will be subject to specific analysis of each case.

Where the employee's social network use outside the workplace affects the image or prestige of the company, the company should be permitted to access such information, as it has a legitimate interest in the limitation. In other circumstances, such access could be considered an invasion of the employee's private life.

Furthermore, the status of the employee will be relevant - the impact of an employee's social network use will be greater for more senior employees, as their personal image, practice and statements are more likely to be associated with the employer's image, practices and statements. Nonetheless, a specific assessment of each case is still required prior to taking any action, as under general circumstances an employer is not entitled to control or influence employees' use of social networking tools outside the workplace.

Are social networking policies standard practice?

During the last few years, an increasing number of companies have been developing policies on the use of social networking tools. While most of these policies relate to email accounts, computers and the Internet in general, some have recently started to

address social networking tools.

In addition, employees are increasingly working remotely from outside the workplace (usually from home). Such employees may rely on the use of social networking tools while working, including MSN Messenger, Microsoft Outlook, Skype and even Facebook. As yet, no specific laws have been created that regulate this matter.

Recent legal developments

As mentioned above, although local employment conditions demonstrate increasing use of social networking tools in the workplace, this matter has not been considered by local labour law authorities (whether government authorities or workers' unions). It is still exclusively governed by company policies on the matter and the application of general regulations by analogy, whenever possible. The interpretation of such policies or the lack thereof is settled by case law on a case-by-case basis, under the parameters explained above.

Comment

Alongside topics relating to the misuse of social networking tools in the workplace during working hours, companies must consider the impact on their image and prestige and the confidentiality of information that may be disclosed by employees. In addition to communicating a privacy policy for such tools (especially concerning employees' email accounts), employers are encouraged to issue a warning regarding the protection of any information provided via email, in order to minimise the risk of claims by third parties. Only where such limitations have been duly notified in advance and there is evidence of misuse in the workplace during working hours may disciplinary action be applied, after an assessment of each specific case. The private use of social networking tools by employees is beyond the employer's power of control.

For further information on this topic please contact [Javier E Patrón](#) or [Enrique M Stile](#) at [Marval O'Farrell & Mairal](#) by telephone (+54 11 4310 0100), fax (+54 11 4310 0200) or email (jep@marval.com.ar or ems@marval.com.ar). The [Marval O'Farrell & Mairal](#) website can be accessed at www.marval.com.ar.

Endnotes

- (1) *Pereyra, Leandro Ramiro v Servicio de Almacén Fiscal Zona Franca y Mandatos SA*, Labour Court of Appeals, Room VII, March 27 2003.
- (2) *Zilberberg, Gustavo A v Total Austral SA*, Labour Court of Appeals, Room X, June 10 2005.
- (3) *VRI v Vestiditos SA*, Labour Court, Tribunal 24, May 27 2003.
- (4) *Vidal, Gustavo S v Microstar SA*, Labour Court of Appeals, Room VIII, December 10 2007.
- (5) EU Commission Decision C-2003-1731 of June 30 2003.

The materials contained on this website are for general information purposes only and are subject to the [disclaimer](#).

ILO is a premium online legal update service for major companies and law firms worldwide. In-house corporate counsel and other users of legal services, as well as law firm partners, qualify for a free subscription. Register at www.iloinfo.com.

Online Media Partners



© Copyright 1997-2010 Globe Business Publishing Ltd