Monitoring Employees' E-Mails in Spain

Report by Rosa J. Barcelo

IN SPAIN, EMPLOYER MONITORING of employees' workplace e-mail has been a hotly debated and unresolved topic. This report looks at the existing legal framework, including case law, as well as guidelines on how an employer can best approach the question.

IN FAVOUR OF THE RIGHT TO PRIVACY OF WORKPLACE E-MAIL

Articles 18 of the Spanish Constitution establishes a right to privacy of communications, including postal, telegraphic and telephone, unless a court order has authorized to the contrary. The Constitution does not limit the scope of application of this right. Thus, communications in the workplace would be covered by Article 18.

In addition, Article 18 of the 1995 Labour Act could also be relevant in concluding that employees' private communications must be respected, albeit within certain limits. This article, together with its interpretative case law, establishes the conditions under which it would be lawful for an employer to inspect an employee's "personal effects." In particular, the article establishes that the employer may inspect personal effects only under the following conditions:

(a) there is a reasonable belief that the employee is engaged in unlawful conduct; and

(b) the inspection is conducted in the presence of third parties.

This provision was meant to cover the inspection of employees' "personal effects" such as lockers. However, many commentators believe e-mail may be deemed a "personal effect" and fall under Article 18 of the Labour Act, meaning that an employer's monitoring of e-mail would be lawful only under the above circumstances.

If there is a right to privacy in the workplace, and the employer monitors e-mail in an unlawful manner, Article 197 of the Criminal Code could apply, triggering sanctions of up to five years imprisonment for violators of the privacy of communications.

AGAINST THE RIGHT TO PRIVACY OF WORKPLACE E-MAIL

Articles 5 and 20 of the Labour Act provide employers with the essential right to their employees' work product, giving companies two important powers. One is the employer's right to direct the labour activity, and the other is the employer's power to monitor or supervise employees' work-related obligations. However, the Act requires employers to exercise such control with due consideration to the dignity of the worker. To avoid undermining the scope of application of such rights, the Act could allow employers to monitor e-mail in order to control or supervise the worker's performance, so long as the "dignity of the worker" is not put at risk.

The only requirement when conducting such monitoring would be imposed by Article 5 of the Spanish Law (Ley Orgánica) 15/1999 of 13th December for protecting personal data (hereafter "Privacy Act"). This Act establishes the organization's obligation to inform the individual from whom it gathers private data about its collection. Spain's Data Protection Agency confirms that this issue is to be judged according to the Privacy Act which permits an employer to monitor e-mail if the employee has been duly informed.

CONTRADICTORY CASE LAW

Courts at all levels, right up to the Supreme and Constitutional Courts, are issuing decisions regarding employee monitoring. The case law has relied on a variety of legal arguments and obviously this has led to contradictory decisions.

In December 1998, the Constitutional Court issued a decision prohibiting a casino from installing microphones that would have recorded employees' conversations. The decision recognized the employer's right to monitor employee performance while recalling that the Labour Act limits such monitoring to that which respects "the dignity of the worker". The circumstances would influence the interpretation of the phrase in each case. Factors such as whether the monitoring is indiscriminate, whether it has been properly communicated to employees, and whether the activity of the company justifies such control, would play a key role in the interpretation

A recent trend among the Courts of Appeal, particularly that of Barcelona, is to maintain that the company has the right to control productivity (thus allowing employee

monitoring) so long as it is carried out only for such purposes and the employees have been informed. Under these circumstances, the monitoring complies with the Privacy Act. The most famous case of this type was filed by a former employee of Deutsche Bank who was dismissed for repeatedly using the company's e-mail for private purposes.

Political action to request government implementation of Senate motion

The issue of e-mail monitoring has led to confrontations between employers and unionised employees. The confrontation has moved into the political arena where both sides have used their political influence.

During the autumn of 2000, the Senate adopted a motion asking the government to allow employees to have their own private e-mail accounts at work, accounts which the employer could not read. Employers could still have access to all other e-mails, and employees would be allowed to send and receive e-mails from the unions.

This year, the unions asked the government to implement the Senate's request and adopt legislation establishing the conditions for monitoring e-mail use at work. To date, the government has made no moves in that direction.

Guidelines for companies

Without a clear legal framework, and with no legal developments in the pipeline, companies are forced to make their own choices. In particular, companies operating in Spain must endeavour to find a way forward to avoid any legal liability while leaving themselves some room to manoeuvre. The following may shed some light on how to achieve this balance.

1. The first step is to draft an e-mail policy allowing the company to monitor employees' e-mails under certain conditions. This entails assuming the existence of a right of privacy at work, but within certain limits. It appears reasonable to expect such a right to be limited by the employer's interest in overseeing worker performance, which leads one to believe that monitoring would be lawful under certain circumstances.

2. Thus, if the debate is focused on the conditions for monitoring, then as a bare minimum, the company should provide written and clear notice to each employee that their e-mail use will be monitored, and the notice should describe the purposes for such monitoring. Should employee consent be obtained? While the law does not seem to require consent, obtaining it gives full legitimacy to the company's practices. If a works council exists, it should be consulted on the e-mail policy.

3. The notice of monitoring must contain a clear description of the purpose and an explanation of why it is necessary. The language should explain clearly that e-mail (hardware and software alike) is a company tool provided uniquely for work purposes and therefore cannot be used for any other purpose. To highlight the lack of e-mail "privacy," the company should require employees to disclose any passwords to their managers. Permitting employees to have secret passwords could contribute to creating a reasonable expectation of privacy among employees.

4. The notice should also describe whether the monitoring will be performed only when there is reasonable suspicion of illegal activity or excessive use of e-mail, or if it will be performed indiscriminately. Broader monitoring could be justified when controlling e-mail (and possibly Internet use) as the only way to check employee performance. Limiting the grounds for monitoring to suspicion of criminal activity would mean virtually eliminating the employer's ability to monitor performance and to check employee e-mail during absences.

Another important decision for employers is the scope of the measures and the manner in which monitoring is done. Should employers limit the scope of monitoring to the company's e-mail, or extend it to employees' private e-mails (such as those on a Yahoo! e-mail account) sent and received during working hours? The need to monitor employee performance justifies monitoring all types of e-mail—while the e-mail account may belong to the individual, it is available through the company's computer system. If the employer feels the need for this broad a scope, it goes without saying that employees should always be informed of such monitoring through the e-mail policy. In addition, pop-up messages can be sent to employees every time they access the Internet or the e-mail network in the workplace, thus informing employees that they should have no expectation of privacy.

When examining monitoring methods, employers may want to consider employees' concerns that employers who monitor employee e-mail without a workers' representative or third party present, could be suspected of fabricating "evidence" of unlawful e-mail use to get rid of certain employees. Although companies are not obliged to have a third party present, individual companies may want to consider their particular circumstances before deciding on appropriate monitoring methods.

Finally, the company may also want to decide whether it wants to have a "zero tolerance" privacy policy; in other words, whether the company wishes to allow employees to use e-mail for other than purely work-related purposes. However, in this case, the employer should make it clear that this will not hinder its right to monitor such use.

Rosa J. Barcelo (rbarcelo@mofo.com) is an associate at the law firm Morrison & Foerster LLP in Brussels and lecturer in law at the University Notre Dame de la Paix, Namur (Belgium).

continued from page 3

gers with the US Drug Enforcement Administration (DEA), and then taking a percentage of assets seized from drug couriers. Will businesses be encouraged, or required, to automate their personal information handling practices in order to facilitate government review? Will they be encouraged or required to collect personal information they might not otherwise need for business purposes in the name of helping protect the security of the nation?

Access to information: Greater government interest in personal information held by the business community may be accompanied by greater government reluctance to disclose the non-personal data it controls. Details about the location of nuclear facilities and other major parts of our infrastructures are not as readily accessible as before September 11. Paradoxically, governments may demand businesses to be increasingly open about the personal information they hold while those same governments may become much more parsimonious with the information they hold.

Some may find these measures to diminish privacy and access acceptable now, but we must not ignore the very real dangers lurking in increased state control of personal data and increased state secrecy. The events of 11th September and the responses to those events are too immediate for us to assess whether our governments have responded wisely, too strongly, or with too little force. This is a truly an analysis that will require the passage of years, perhaps decades.