Social Networking: New Challenges in the Modern Workplace*

Ana Belén Muñoz Ruiz
Lecturer in Employment Law
Carlos III University of Madrid

Received: 31 July 2013 / Accepted: 1 October 2013

Abstract: The past few years have witnessed an exponential growth in the use of social networking. Employees often share photos, write messages to friends or leave virtual 'gifts', which are sometimes related to their employment. Indeed, employers sometimes use information found on these sites to make pre-employment decisions or take disciplinary action. In this paper we wish to focus our attention on Spanish case law and to contrast the criteria employed in this law with that of other relevant countries such as Germany, France or the United Kingdom. The overall purpose of this article is to rethink the scope of labour law and to examine how industrial relations are affected by employee's personal conduct.

Keywords: Privacy, secrecy of communications, social networking, workplace.

1. Introduction

The past few years have witnessed an exponential growth in the use of social networking. Employees often share photos, write messages to friends or leave virtual 'gifts', which are sometimes related to their employment (and which often defame their employers or play practical jokes on them).

While social networks may create difficulties for employers, they may also have an adverse impact upon employees. Indeed, employers sometimes use information found on these sites to make pre-employment decisions or take disciplinary action.

In this paper we wish to focus our attention on Spanish case law and to contrast the criteria employed in this law with that of other relevant countries such as Germany, France or the United Kingdom. Our main objective is to identify the important issues that help to resolve cases where employees have been sanctioned for posting negative comments about their employers.

Some large companies already have guidelines in place which govern the use of various means of communication. Typically, these codes of conduct regulate the personal use of computers and Internet and also include clauses that warn workers of possible employer control in these areas. It will be interesting to see if the courts consider these clauses to be valid or not.

Another of our goals is to analyze the data protection law to see whether or not it contains specific measures for individuals who post personal information on social networking sites. Moreover, we try to identify to what extent employers may use employees' personal data which has been stored on social networks (or transmitted over them). It is important to know whether such situations fall within the employees' right to freedom of expression.

One question that needs to be addressed is whether case law regarding e-mail and text messaging is equally applicable to the use of Facebook accounts. In Spain, both the Supreme Court and the Con-

*This paper is a reworking of the communication presented at The Labour Law Research Network Inaugural Conference hold in Barcelona in June 2013.

stitutional Court have handed down a ruling on this issue where an employee posts emails or uses the computer for personal matters at the workplace.

Finally, the overall purpose of this short paper is to rethink the scope of labour law and to examine how industrial relations are affected by employee's personal conduct. Up until the present, the main challenge in labour law has been the construction of fundamental rights in the workplace. Since the 1980's, in particular, the Spanish Constitutional Court has paid attention to the specific and non-specific fundamental rights of employees. Nowadays, however, the real issue is whether the personal behavior of employees has any bearing upon workplace relations.

2. How increased use of social networks has led to further labour law

While there are only a few cases regarding the use of social network in the workplace, we have managed to find a representative sample. In passing, it needs to be noted that there is no unified jurisprudence regarding the use of social networks and that the only consolidated criteria has to do with the monitoring of electronic devices in the workplace. The analysis of this matter will be structured in two parts. First, we will consider the problems arising from employee usage of company property for social networks. Secondly, we will address the remaining assumptions and describe the worker's personal sphere and the use of social networks outside the workplace and work time.

2.1. The usage of company-owned computers, phones and Internet for personal reasons

Both Spanish doctrine and courts have argued rigorously about the right of employees to use company-owned computers, phones and Internet for personal reasons. While the Supreme Court has ruled on relevant cases regarding employee privacy, there have been few cases concerning the right to secrecy of communications in the workplace[1]. In a recent ruling, the Spanish Constitutional Court (decision 241/2012, December 17, 2012) decided whether the employer had the right to monitor employee electronic communications.

In this particular case, two employees had installed a program named "Trillian" –in breach of company policy– on a work computer in order to criticize and insult their supervisor, colleagues and customers. This case has several interesting features; firstly, that the employees were expressly forbidden from installing the program; secondly, that the computer could be used by any employee and did not have a password; and thirdly, the way in which the company discovered the breach. In this last regard, it was an employee who discovered the conversations by chance. Two months later, the company called a meeting between two employees and four managers in which some of the conversations were read and the content of the rest were summarized. The employees subsequently admitted the facts and were verbally disciplined. However, one of the employees then sued for violation of privacy (article 18.1 of the Spanish Constitution) and secrecy of communications (article 18.3 of the Spanish Constitution).

In the STC 241/2012, the Constitutional Court ruled in favour of the company. The Court held that the employee had no reasonable expectation of privacy in her on-line communications and defended a more limited use of the proportionality principle in the resolution of conflict between fundamental rights. The dissenting opinion by Judge Valdés Dal-Ré emphasizes that "this is a case which, in my opinion, represents a step backwards in relation to the constitutional doctrine or means a perspective of labour relations which (…) is different from the consolidated model".

A) Key aspects of the new constitutional doctrine

Although the employee in this case laid claim to two fundamental rights, most of the Court's decision argumentation focuses on the secrecy of communications. This is confirmed in the opening

[1] Judgment of Constitutional Court, November 29, 1984 (114/1984), which supported as evidence in dismissal process the recording of a conversation with another person that provided the employing entity.

enumeration of article 18.3 of the Spanish Constitution which is concerned "particularly (of) postal, telegraphic and telephonic communications". It is also worth noting that the article protects both traditional and new means of communications.

Another significant aspect of the new constitutional doctrine is that it states that the company may monitor employee communications in the workplace. Following this reasoning, the Constitutional Court highlights the main criteria that establish the limits of employees' fundamental rights.

B) The balance between employee privacy and employer interests

The Spanish Constitutional Court rules that every employer may limit the personal usage of email and other forms of computer and online communications in the workplace. At the same time, however, the Court rulings seek a balance between employee privacy and employer interests. This last one serves to ensure that employers continue to observe management functions and to prohibit employees from using company-owned computers, phones and Internet for personal reasons.

Legal support for these rulings' may be found in article 20 of the Workers Statute in which the employee accepts the employment contract and thus consents to employer notification limiting the use of electronic devices. The employer thus obtains employee consent at the time of signing the employment contract (Bacigalupo, 2013).

The law is flexible regarding employer policy on electronic communication in the workplace. While the Spanish Constitutional Court enumerates laws, instructions and codes of conduct, it must be noted that the Court does not refer to the possibility of collective bargaining. Collective bargaining is therefore not excluded and could be used to negotiate this issue. Indeed there are relevant examples that demonstrate this point and the same argument may be seen in the dissenting opinion of Judge Valdés Dal-Ré when he mentions "the possible regulations decided by the employer or the collective bargaining regarding the usage of electronic communications".

The Court does not resolve whether the company is obliged to check that every employee has been informed of the policy. In this respect, mention must be made of the Supreme Court's decision of March 8, 2011. Here the company alleged that it had informed employees of the rules concerning the usage of electronic communication by giving them a manual. However, this claim was not proven and the employer's use of surveillance was considered illegal. On October 6, the Supreme Court considered a case where a letter was posted to employees –and signed by them– and in which they were instructed not to use electronic devices (computer, mobile phone, Internet) for personal interest. In contrast to the previous case, the Court found the letter to be legal.

C) Rules and elements in the protection of fundamental rights

The Constitutional Court made one of the most important contributions to debate when it observed that surveillance does not always affect fundamental rights and that some forms of surveillance are not illegal. In such cases, therefore, the principle of proportionality does not apply (the STC 241/2012 is a good example of this).

a) When there is no conflict between rights

There will be situations in which there is no conflict between employee privacy and employer interests. According to constitutional doctrine, a relevant aspect of these cases is whether there is a policy regarding employee usage of information technologies which clarifies whether employees are allowed to use devices for personal reasons.

The context of rules concerning in-company usage of information technology

In the aforementioned case (STC 241/2012) the company had deliberately prohibited employees from installing programs on their computers. The employees, however, used an instant messaging sys-

tem that they had installed on a work computer in breach of company policy. The Court thus reasoned that there was no expectation of privacy.

A similar argument may be observed in the doctrine of the Supreme Court. In a judgment handed down on September 26, 2007, the Supreme Court stated that the policies of the workplace are relevant in deciding whether there is an expectation of privacy[2]. Employers accordingly have a legitimate right to check how their computers are used by employees and surveillance is thus legal if the company previously establishes the rules of use and gives prior notice to employees on the issue. If the company has prohibited employees from using electronic devices for non-work related purposes, the monitoring will be legal[3].

One of the most important elements in this argument is that the computer had been specifically provided for public use among the employees (all employees were therefore able to access the company hard drive without needing a username or password). In such conditions, the court ruled, there can be no expectation of privacy. Under constitutional doctrine, privacy is defined as keeping one's personal information private or limiting other people's access to this information. This fundamental right has an objective content – "what, according to the prevailing social norms is usually considered as separate or alien to the legitimate interest of the other" –and a subjective content– "everything that a person decides to exclude from the knowledge of the other". Also relevant is whether the employee decides to limit the extent of protection given to privacy (Judgment of Supreme Court October 6, 2011). This is a theory defended by a sector of doctrine (Desdentado/Muñoz 2012: 180-182); when the company has prohibited personal usage, employees know they could be monitored and would accept this. Privacy is thus given less protection.

Returning to the original case under discussion, the Constitutional Court refused to accept that the right to privacy had been violated because it considered that the employees' actions reduced their own protection. In contrast, the dissenting opinion regarded this situation as being similar to that of a mail box containing sealed letters that belong to different people and which no one is authorized to open: that is, just as it is forbidden to open or read other people's mail when it is home delivered or distributed in the office through a system of personal but open 'pidgeon holes' (even with a perfectly feasible excuse), one is not allowed to open email files or messages, even when it is possible to access unprotected files on a shared computer. We might refute this example with that of a postcard: whoever sends a postcard, instead of a sealed letter, knows that secrets cannot be hidden from sight. Similarly, when an individual uses a computer under the control of another party –one which has banned personal use and which has power of control– then this individual knows that he/she does not have a guarantee of confidentiality[4].

In sum, the monitoring in this case did not violate the privacy or secrecy of communications because the company had carried out the activity after obtaining employee consent. This consent was presumed when the two employees knew of the company policy. Implied consent may be achieved when an employer gives prior notice to his employees that electronic communications are monitored.

Rejection of the general application of the principle of proportionality as a means of evaluating Fundamental Rights

According to a general formulation, the principle of proportionality may be applied to conflicts between fundamental rights. This is based on three types of test: first, if the application of the measure is able to achieve the objective (judgment of suitability); second, if it is necessary and that there is no other measure which is less aggressive (judgment of strict necessity); third, if it is balanced and obtains more advantages than disadvantages for the general interest (judgment of strict proportionality) (Mercader/García-Perrote, 2003: 257-264).

[2] RJ 2007\7514.

[3] The doctrine was established in the following judgments [March 8 2011 (RJ 2011\102184) and October 6 2011 (RJ 2011\7699)]. In the first case, the Supreme Court decided that the monitoring was not legal because the company had not set a policy regarding this issue. Neither the company had given notice employee about the monitoring. In the second case, the court declared the hidden monitoring legal because the company had prohibited employees from using electronic devices for non-work related purposes. According to the Supreme Court, if the prohibition is clear and strong, the employee should understand the possibility of control.

[4] Judgment of Supreme Court October 6, 2011.

It is also significant that the Constitutional Court does not state an opinion regarding the principle of proportionality. However, the Court of First Instance (Court of Seville, June 13, 2005[5] and High Court of Justice of Andalucía of 10 February, 2006[6]) held that the employee had she had no reasonable expectation of privacy based on the principle of proportionality despite the fact that she had laid claim to this principle[7].

Up until the present, the Constitutional Court has reasoned according to this principle particularly in cases regarding employee privacy (such as in, the well-known cases SSTC 186/2000, July 10 and 98/2000, April 10, which examined the conflict between privacy and hidden surveillance in the supermarket and the casino). Moreover, as we discussed in a previous paper, there has been a general application of the principle of proportionality in cases where there was no conflict between employer interests and the fundamental rights of employee (such as privacy or secrecy of communications). In addition, the general application of this principle could possibly produce different results in similar cases- a company that did not violate employee privacy in one case, could be found to have been violated it in another. Our proposal is thus based on first checking to see if there is a conflict between the rights and only then applying the principle of proportionality (Desdentado/Muñoz 2012: 20).

The new case (STC 241/2012) avoids applying the principle to every case and establishes the basis for a new approach. The Constitutional Court has assumed the doctrine of Supreme Court in the matter of privacy and has adapted it to the secrecy of communications. The analysis is the same: if the company has prohibited employees from engaging in personal use of computers in the workplace, that company is entitled to monitor for this use. Here, there is no conflict between fundamental rights of employee and the principle of proportionality does not apply. At the same time, it is not necessary to inform the employee about this[8].

Irrelevance of the means of communication

It must be noted that the means of communication used by the employee are irrelevant. While this case is about on-line conversation. It does not mean that there is less protection of privacy with regard to electronic devices.

The Constitutional Court based its position on the nature of the communications used and the context of the company policy. The Court did not say that the secrecy of communications were not protected or less-protected when the communications are electronic. This conclusion could be said to apply equally to conflict over privacy resulting from the monitoring of personal files located in the company's computers.

b) When there is a conflict between rights

There are cases of conflict between fundamental rights. One example is when the company does not set the rules of personal usage. Another may be when the company allows the usage of devices for personal reasons and then monitors the computers. The most conflictive case occurs when the secrecy of communications affects unions; here the proportionality principle needs to be applied.

If the company does not set rules, it is not entitled to engage in monitoring. When the company has not regulated the use of information technology, we argued that the employer loses the ability to control the usage, which would not make possible even special occasional checks. In addition, we pointed out that this conclusion seemed excessive and the issue could be raised if in some cases such as for example with regard to the company email, ensuring the confidentiality of communications is relative, as is shown by a criminal ruling[9]. First, a computer in the workplace is not the most appropriate channel

[5] The first case stated: "the measure met the proportionality test. First, it is suitable because searching the files is necessary to determine it. Second, it is necessary because there is not another less aggressive measure. Third, it is balanced because it produces more benefits than damages to the general interest. Moreover, it has not affected the expectation of privacy of employees".

[6] In the same way the High Court of Justice of Andalucía resolved this conflict.

[7] The employee alleged that it was not necessary to open the files. It was enough to check the installation of program. Thus, the company had violated her privacy and secrecy of communications.

[8] It must be noted that the Constitutional Court pointed out that the absence of information to the affected workers and the works council was a matter of ordinary legality and added that the prior notification of the filming would have hidden private effectiveness from the reach of surveillance (STC 186/2000).

[9] For example, the Judgment of High Court of the Madrid October 29, 2010, ARP\2011\259. This concerns a crime against

for transmitting secrets, especially when there is lack of set rules for personal use of computers; expectation based on the absence of prohibition does not mean the company is not exercising control. While the employee can expect that harmless use will not create disciplinary problems and that he will not be subjected to routine checks, it is not reasonable to think that the computer will not ever be monitored for emergency purposes (blockages by mass mailings, harassment via email, information filtering of companies, urgent need to address customer communications in cases of the absence of the worker ...). The expectation of confidentiality is not so great.

In the opinion of the Constitutional Court, it is relevant if the company has allowed employees to use electronic devices for personal reasons because in these cases there is an expectation of privacy. This is particularly relevant where there is a conflict between the fundamental right of employee (privacy/secrecy of communications) or the union (privacy/secrecy of communications and the privacy of Trade Union Freedom) and the employer interests (article 38 Constitution). The criteria of the Court is thus based on limiting employer interests but "the degrees of limitation to examine employers' measures of monitoring depends on the conditions of use and instructions given by the employer".

2.2. The usage of social networking outside of the workplace and working hours

The second part of this paper focuses on the usage of social networking outside of the workplace and working hours. Analysis of case law shows that events occur not only during the working hours or in the workplace but also outside working hours and the workplace. The study highlights the growth of this problematic situation that has no specific regulation in the Spanish case.

The following cases are typical of events that occur during working hours and in the workplace:

— An employee working as nurse and midwife was fired after taking a photo of a baby and then publishing it on a social network[10].
— A nurse was fired after disclosing clinical information in a blog that posted images and reports obtained from the radiological examinations carried out in the company[11].
— Some company sales personnel published photographs taken in the workplace in social networks where they could be seen dressed in the company uniform and lying on an office table, where documentation of the company could be seen, as well as an opened safe and bundles of banknotes[12].

Some typical events occurring out of working hours and the workplace are as follows:

— Criticism of the company on a social network or blog[13].
— Publication of a video which parodies a company boss in a well-known scene from a film, attributing insults and homophobic comments about the staff to him[14].

the consumer market and in the same, hidden control is supported for computer programmers who were fired for having picked and endorsed without authorization platform, e-learning courses and content of the company for which services were lent, with the intent to sell them on their own. Although not verifying the existence of rules of usage of computers, the Court appreciates exceptional element is satisfied in this case in that the computer was a fundamental and essential tool for employees and control developed by the employer has particular relevance in the case. The appreciation of this key element is the analysis carried out by the Court to presume that employees had to have had the knowledge that their activity (by computer) was to be kept under constant review by the directors of the company and for this reason employees should restrict the maximum computer usage for personal and private purposes, so it could almost be argued that personal capacity utilization was implicitly a waiver of his privacy that at most would be limited to those emails from the server particularly those who, by the way not agreed upon, and the files that were identified as belonging to individuals and which had a purely personal content.

[10] Judgment of High Court of the Galicia February 20, 2012, AS 657.

[11] Judgment of High Court of the Valencia February 8, 2011, JUR\2011\161437.

[12] Judgment of High Court of the Andalucía, Granada, November 10, 2011, JUR\2012\41677.

[13] Judgment of High Court of the Catalonia May 16, 2007 (AS 2400), July 17, 2009 (AS 1881), March 24, 2010 (AS 2012) and Judgment of High Court of the Madrid May 25, 2011 (JUR\2011\237900).

[14] Judgment of High Court of the Galicia February 23, 2012, JUR\2012\108833.

— Identity theft of staff in superior positions by creating a fake profiles and publication of insulting expressions about them[15].
— An employee who was in a situation of temporary disability published comments and photos of parties and consumption of alcohol[16].

According to our classification, in the first and second of these situations the employer is not entitled to monitor the employee network because the employee has not used the company-owned computer or Internet. However, analysis of case law shows that even in these cases it is possible to consider events in a work context. This may be the case when the employee uses the social network to disclose confidential information or to post offensive comments about the boss.

It is clear that employees´ usage of social networking outside of the workplace pertains to their personal life. The employer, however, may access this information if it is generally accessible on-line via a social networking site. Case law deals with events that may be discovered by anyone without a password; in such cases the courts state that the employer is entitled to this information.

Employers are thus allowed to collect or process data obtained from social networking sites whenever the purpose of the social network is linked to work and this information is relevant. In this paper we have identified some cases where the court ruled against the employer because the information obtained was insignificant and the employee's error was easily rectified. This was the case of the employee who took a photo of a baby and then published it on a social network (and who was subsequently fired from his job as nurse and midwife). In this case, the employer had informed the family involved and blown the events out of proportion.

It must be noted that it is not relevant that the company has established a policy about the usage of networking and informed its employees of this policy. The courts did not pay attention to this issue because they dealt with the personal sphere. In addition, most cases have shown that there was no company policy regarding this use. The employer is not allowed to prohibit employees from posting photos or comments on the social network

The courts have declared that the breach-alleged by the employer in the letter of termination has been demonstrated. The decision to terminate employment was based on the comments, photos and videos posted on the social networking. While it needs to be acknowledged that there is still no leading case on this issue, the cases examined demonstrate that disciplinary actions by employers are on the rise. The judicial criteria used to justify dismissals are described below.

First, with regard to the data published on the social networking, it is a relevant issue that the users are capable of easily identifying the name of the company or supervisors. If the users of the social network are not able to identify the name of the company or the supervisors, the employee conduct is then protected.

The second is when information posted on social networking causes serious damage to the company, employees or stakeholders. This damage is related to the company image or security; no one can be ignorant of the fact that negative comments posted on the social network regarding a company or employer could result in a loss of customers or benefits to the company. It is true that the employee has the right to freedom of expression but there are limits to this right.

Third, the courts have also considered the time taken by the employee in preparing the comments, videos or images and in transmitting them. This appears to be a relevant aspect because it demonstrates bad faith on the part of the employee.

In addition to the criteria listed above, it is important to consider the employee's position in the company. It is generally accepted that work relationships are defined by the level of trust among the parties involved. When, for example, the worker is a manager of a supermarket, his level of responsibility may require behavior which is of a higher standard than that of other employees who have less responsibility. If the worker violates trust placed in him by posting pictures on the social network, he may not only affect the image of the company but also his own safety.

[15] Judgment of Court number 1 of Cartagena (Murcia), July 6, 2011, AS 1167.
[16] Judgment of High Court of the Madrid January 23, 2012, JUR\2012\106651.

It should be emphasized that the use of social networking by employees is similar to other actions connected to the workplace. In our analysis of this issue, we have observed that it is almost the same thing to talk about freedom of expression and its limits. There is only one difference; an employee might make negative comments about a boss to a friend but it is another matter altogether when the employee publishes photos and comments on the social network and thus amplifies this action.

In light of these decisions, it appears that even if employees post comments from their own computer outside their working time, their employer is entitled to take disciplinary action against them. Obviously, the cases analyzed refer to information that was accessible by anyone. In any case, the employer would not be entitled to access social networks that have passwords and would not be entitled to simulate a profile in order to be invited by the worker to the social network.

It seems clear that the rules concerning disciplinary sanctions should be reformed. We propose that these rules should include the issue of social networking and in particular the possibility of requiring the employee to delete a blog or information held on the social network related to the company. We believe that this may avoid future disciplinary decisions based on the use of social networks that can cause damage to businesses. In Spain, the employers and employees would be responsible for negotiating such clauses in collective agreements. As with other countries such as France, in cases where the offense is not very serious, Spanish judges should consider declaring the dismissal to be unfair and sanction the worker by requiring them to erase all information relating to the company from their blog or social network (Martin, 2011)[17].

None of the cases analyzed dealt with the issue of hiring. It is generally accepted that social media provides an easy and inexpensive way for employers to gather information about job applicants to see if they will fit well into the workplace or will do a good job. In Spain, there are no regulations governing this issue. Germany, by way of contrast, is developing standards for information posted. In Germany a standard is being developed for information posted on social networks by job candidates so that companies are limited in the use they make of this information when it has no professional interest (Locklear, 2012). This solution is not applicable to the Spanish case without legislative reform. According to judicial criteria described above, the solution would be to permit the employer to monitor information which is available on social networks and which is freely accessible.

We have not identified cases addressing other situations such as employer pressure to obtain employee's passwords or the use of a third party to access the employee's social network. Obviously both situations should be rejected in order to protect employee privacy.

3. Conclusion

In Spain, the absence of legal criteria has meant that the industrial relations tribunals have played a dominant role in defining the scope of protection of privacy both within and outside of the workplace. While the subject of social networks and their work-related implications is still very new, a representative set of rulings are beginning to appear.

The Supreme Court's doctrine regarding the monitoring of computer has been of particular relevance. According to a solid criterion maintained since 2007, monitoring is legal if the employer has established a policy and has informed employees of this policy.

However, until recently the issue of monitoring of communications had not been decided and there were serious doubts about it. Most doctrine had rejected this monitoring because the constitutional protection of privacy was very strong. The new constitutional doctrine is extremely controversial be-

[17] In a Judgment of 16 October 2006, the Court of Paris held that a former employee of a multinational company must delete from her blog all the slanderous and defamatory words that she had posted about her former employer and pay damages. The former employee had created a blog where she claimed that when coming back from her maternity leave she had been unlawfully terminated by her employer. She claimed that she had been discriminated against because of her pregnancy. On her blog, she had posted internal mail from the company, communications with the labour authorities, her termination letter and insulting comments about her former colleagues and employer.

cause it extends the criteria of Supreme Court to monitoring of communications. It is clear, therefore, that the company is entitled to monitor employee usage of electronic devices.

The key difference in this approach is to distinguish two kinds of situations. In the first of these, there will be complaints about monitoring of employees where there is no conflict between employee privacy and employer interests. This is because the company has established a policy relating to the use of information technology in the company. Furthermore, it will mean that the proportionality principle will not be applied to solve such conflict. In the second of these, there will be situations where there is a conflict between rights and the application of proportionality principle will be necessary.

More problematic is the control of social networks outside the workplace and working hours. To address this question, we have advocated the application of some of the criteria already established to control the use of company owned computers, phone, Internet or e-mail. We would apply here the theory of protective barriers that workers themselves employ when posting videos, comments, pictures on social networks. When access to the social network is restricted, workers themselves do not need to surrender their own privacy.

References

Bacigalupo, E., Problemas penales del control de ordenadores del personal de una empresa, *Diario La Ley*, 2013, nº 8031.

Cardona Rubert, M.B., La utilización de las redes sociales en el ámbito de la empresa, *Revista de Derecho Social*, 2010, nº 52, pp. 67-77.

Desdentado Bonete, A., Contrato de trabajo y nuevas tecnologías. Una nota sobre algunas cuestiones de actualidad, prueba electrónica, garantías de la intimidad y uso sindical del correo electrónico, *Revista del Poder Judicial*, nº 88, 2009, pp. 241-265.

— and Muñoz Ruiz, A.B., *Control informático, videovigilancia y protección de datos en el trabajo*, Lex Nova, Valladolid, 2012.

Goñi Sein, J.L., Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos, *Justicia Laboral*, nº 39, 2009, pp. 11-58.

Levinson, A., Social media, privacy, and the employment relationship: the American experience, *Spanish Labour Law and Employment Relations Journal*, Vol. 2, nº 1, 2013, pp. 15-31.

Locklear, L. In the world of social media, when does "private" mean private? A critique of Germany's proposed amendments to its federal data protection act, *George Washington International Law Review, 2012*, Vol. 44 Issue 4, pp. 749-776.

Marín Alonso, I. *El poder de control empresarial sobre el uso del correo electrónico en la empresa. Su limitación en base al secreto de las comunicaciones*, Tirant lo Blanch, Valencia, 2005.

Martín, C., Social networking in the workplace: is the French approach different from that of other countries? *Employment & Industrial Relations Law*, 2011.

Mercader Uguina, J.R., *Derecho del Trabajo, nuevas tecnologías y sociedad de la información*, Lex Nova, Valladolid, 2002.

— Límites del control empresarial sobre el uso por el trabajador del ordenador facilitado por la empresa como instrumento de trabajo: TS 26-9-07 como "leading case", en AA.VV. (Coord. I. Sagardoy de Simón y Luis Gil Suárez), *Jurisprudencia y Grandes Cuestiones Laborales*, Madrid, Francis Lefebvre, 2010.

— and García-Perrote Escartín, I., Conflicto y ponderación de los derechos fundamentales de contenido laboral. Un estudio introductorio, en AA.VV. (Dir. A.V. Sempere Navarro), *El modelo social en la Constitución Española de 1978*, Ministerio de Trabajo y Asuntos Sociales, 2003, pp. 257-264.

Pérez de los Cobos, F., *Nuevas tecnologías y relación de trabajo*, Tirant lo Blanch, Valencia, 1990.

Sempere Navarro, A.V. and San Martín Mazzucconi, C., *Nuevas tecnologías y relaciones laborales*, Aranzadi, Cizur Menor, 2002.