Social Media: What Employers Need to Know

By Reinier Russell and Michèle Stutz

There has been a huge increase in the popularity of social media such as Facebook, Twitter, and LinkedIn. Social media has transcended languages, borders, and cultures; through social media a vast amount of information is exchanged daily and globally. For many people, it is very normal to post and read both personal and professional information. This information can be viewed not only by friends and relatives but also by colleagues, clients, and employers. Consequently, employers cannot ignore social media in a corporate environment. Social media can be a powerful tool a company can use to its advantage. On the other hand, inappropriate use of social media can influence the (online) reputation of the company in an unwanted way. But that is not all, social media also can play an important role in employment relationships. Employers are likely to be faced with questions such as: Is the company allowed to monitor what information (future) employees exchange and who they exchange it with? and How should the company deal with employees who are telling company secrets or are openly badmouthing the company or their colleagues?

Privacy legislation, which can vary from jurisdiction to jurisdiction, often plays an important role in employer–employee relationships. However, the key issues and pressure points are similar worldwide. More specifically, regarding employers, problems can arise throughout all stages of the employment relationship, that is, at the recruitment and selection stage, during employment, and after the termination of employment.

Reinier Russell *is the managing partner at Russell Advocaten in Amsterdam, The Netherlands, where he specializes in corporate, commercial and employment.* ***Michèle Stutz*** *is a partner at MME Partners in Zürich, Switzerland, where she specializes in litigation and employment law.*

RECRUITMENT AND SELECTION

Employers wish to gather information on future employees to get an overall picture of a person. But to what extent are employers allowed to review social media profiles and to what extent can and may that influence the employer's decisionmaking process? When hiring a sales professional, an employer will want to know who the prospective employee is networking with. On the other hand, social networking with competitors can have a negative effect. Information on a person's situation at home or on private activities can be more important than expected. Think, for instance, of difficult care situations at home or of "dangerous" hobbies.

But how does this relate to data privacy laws and antidiscrimination laws? In the United States, job candidates need to provide the employer with a written authorization prior to a background check, whereas job candidates in the United Kingdom must be given the opportunity to first check the accuracy of the online data collected about them.

In addition to privacy laws, antidiscrimination laws, and codes of conduct as implemented, for example, in France, user conditions of social networking sites themselves also can contain restrictions. User conditions (general terms and conditions) of social media or platforms may restrict the use of information for professional or recruitment purposes. In some jurisdictions, there is a difference among the types of social media. Employers in Germany, France, and Switzerland may use information collected from professional social networks only (such as LinkedIn), but they are not allowed to use information from general social networking sites, such as Facebook.

DURING EMPLOYMENT

An employee must observe the rules and regulations of the organization he or she works for, and the person must act as a good employee. Employees can thus be expected to act professionally and to behave like good colleagues, especially when it comes to

the use of social media. Information revealed on the Internet is hard to remove and spreads fast. This can have negative effects for both employer and employee. It is a completely different question, however, whether an employer is allowed to use information available through social media on the employee's private life. Can a Tweet (such as "Relaxing on the beach") by an employee on sick leave to his Twitter followers be used in a dismissal procedure? Is an employer allowed to monitor what an employee posts on Facebook about his manager or about the company? Is an employer allowed to check who an employee is linked with on LinkedIn? The answer to these questions depends on data privacy laws that vary from country to country.

MONITORING EMPLOYEE'S USAGE OF SOCIAL MEDIA

Whether or not employers are permitted to monitor the social network use of their employees and if so, what considerations and limitations apply, are additional questions to be answered by the different legislations. In most jurisdictions, employers are permitted to monitor social media use on work-provided devices on condition that the employee's privacy is respected. The European Court of Human Rights has ruled that in Europe employees enjoy their right to privacy and private life in their work environment as well and, therefore, in practice, limited private Internet use is allowed. Furthermore, the Court has determined that, for example, monitoring telephone conversations and emails should be announced beforehand.[1]

Of course, if the employer has a specific and good reason to suspect violations of the company policies, it will, in general, be allowed to investigate that specific situation. However, monitoring Internet use as a general policy is allowed only under certain conditions, or in some cases not at all.

In general, privacy rights of the employees must be balanced against the employer's legitimate interests to protect its business or information technology. Some jurisdictions have established guidelines about appropriate monitoring in the workplace (*e.g.*, United Kingdom and Switzerland). In others, it is important to have a consistent policy about monitoring that has to be made known to all employees beforehand, either via a works council or individually (Germany, the Netherlands, France). In Spain, monitoring is permitted only with the consent of the employee, and Switzerland does not allow preventive monitoring at all.

Is the employer allowed, besides monitoring the use of social media, to also monitor information posted on social media by the employee? Depending on the national data privacy laws, the employer may be allowed to use this information in dismissal proceedings. In the Netherlands, a picture posted on Hyves by a partying employee who officially was on sick leave with chicken pox was admitted by the court as evidence that she wrongfully had not reported fit for work.[2]

DISMISSALS DUE TO INAPPROPRIATE USAGE OF SOCIAL MEDIA

To what extent employees can be dismissed based on inappropriate use of or comments on social media, depends on the national legislation. When it comes to inappropriate use of social media, in the United States, the focus will be on whether or not it is related to "concerted activity." In Canada and in most European countries the reason given for dismissal will be checked. In Canada the criteria for inappropriate use of social media are: (1) breach of the company policy, for instance, regarding confidentiality, computer use, or antiharassment; and (2) damage to the company. Other considerations taken into account are whether it is a matter of frequent inappropriate use or one time inappropriate use only, and whether the employee has been warned.

A court in Australia considered that "excessive use of the Internet for personal purposes may constitute misconduct" and therefore may be a valid reason for the termination of the employment.[3] In two recent decisions rendered in France, the courts ruled that employees posting insulting comments about their employers on a social media Web site could be terminated for fault and also fined for the offense of public insult. It was held that comments posted on a social media site could not be considered private, because the postings were not set to be displayed only to friends.[4]

This is not only an issue in France but also in Switzerland, where employees must check the

relevant privacy settings before posting derogatory comments. In France, it was held that employees must be made aware about the possible sanctions and the consequences of inappropriate postings in advance. On the contrary, in the United Kingdom, an Employment Tribunal held that the employee's comments on Facebook were not in private even though the employee had set his privacy settings so that only his Facebook friends could see them.[5] The Dutch court had the same line of reasoning about an employee posting an insulting remark about his employer to his friends on Facebook. According to the Dutch court, the term "friends" is a rather relative notion on the Internet because these friends can forward the message very easily, as happened in this case. The employer's need to protect its reputation was weighted more important.[6] In the United States, the National Labor Relations Board issued a report about the protection of disparaging comments on social media about employers.[7]

CLEAR RULES REQUIRED

It is important for the employer to lay down rules on the use of social media and on the employees' online activities regarding revealing information about the company they work for, as well as the sanctions for noncompliance. In the best case, employees expressly consent to such rules, implemented either as policies or contractual provisions. Such rules not only facilitate proving whether or not an employee has broken company rules, but also are valuable in the event the employer intends to hold the employee responsible for damages the company or clients suffered due to information spread via social media. These rules may include, for example, if and to what extent employees are allowed to befriend business relations and whether employees will have to create separate accounts for business relations and for solely personal contacts. The employer should consider setting up employees' business accounts according to the company guidelines. An employer also can include whether, and if so, which social media sites can be accessed during work hours and to what extent they may be used. This often will depend on the position of the employee and the type of company. A sales manager of a software company will be allowed more social media activity than an accountant of a food wholesaler. In this regard, an employer also may take into consideration how often and to what extent emails and telephone calls are permitted for private purposes. This should not only apply to the use of company property but also to private devices such as smartphones, tablet computers, etc.

After Employment

After the termination of employment, the employer and employee are most likely to still be active on the Internet. At this stage, issues such as duty of confidentiality and noncompetition clauses are very important. As these clauses mostly are agreed to at the commencement of employment, the employer thus has to consider in advance the arrangements it wishes to make regarding these issues upon the termination of employment. It must be clear whether or not contacts with business relations and business-related social media and accounts will have to be terminated or closed. The employer is advised to make arrangements on whether LinkedIn contacts will have to be deleted or may be kept. Guidelines can be given in a Code of Conduct or Employee Handbook and more specific agreements and rules can be adopted in the individual employment contract, for example in a noncompetition clause, a business relations clause, or a confidentiality clause.

Controlling the online behavior and relations of employees during their employment can be a useful tool in controlling the behavior afterwards. It is important for the employer to stipulate that (without prior consent) no business relations will be accepted as Facebook friends, as these are private contacts that may not fall under a business relations clause. The employer also can arrange that it has a say in the management of a LinkedIn account and, for instance, has the passwords of business-related social media. If arrangements like this have not been agreed to in the employment contract, for instance in a special clause or included in the staff regulations, they can on occasion (most specifically) be agreed to in a termination agreement.

CONCLUSION

There is not just one uniform way to deal with social media. After all, every country, every company, and every human being is different from one another. A social media policy has to be tailored to fit the country, the company culture, the image of a company, the sensitivity level of information, and

safety aspects so that all employees know the company's rules and the company can enforce them. It is advisable for an employer to include such a policy as standard in the staff regulations.

NOTES

1. A.o. Copland v. the United Kingdom, no. 62617/00, § 41-42, ECHR 2007-I.
2. Breda District Court, April 4, 2012, ECLI:NL:RBBRE:2012:BW1629.
3. O'Connor v. Outdoor Creations Pty Ltd., 2011 [FWA] 3081, § 56, *http://www.fwc.gov.au/decisionssigned/html/2011fwa3081.htm*.
4. Sandrine F. v. Société Casa France, Court of Appeals Besançon [=Cour d'appel de Besançon], November 15, 2011, nr. 10/02642; *Société Webhelp v. Eric B.*, Criminal Court Paris [= Chambre correctionnelle du Tribunal de Grande Instance de Paris], January 17, 2012, *http://www.wk-rh.fr/actualites/upload/TCorr-Paris-17-1-2012-TIC-syndicats.pdf*.
5. Crisp v. Apple Retail (UK) Limited, Bury St Edmunds Employment Tribunal, September 15, 2011.
6. Arnhem District Court, March 19, 2012, ECLI:NL:RBARN:2012:BV9483.
7. "General Counsel Report Concerning Social Media Cases", January 25, 2012, pp. 3-5, *http://www.nlrb.gov/news-outreach/news-story/acting-general-counsel-issues-second-social-media-report*.