SOCIAL NETWORKING AND THE EMPLOYMENT RELATIONSHIP

by Stathis Mihos

1. Introduction

1.1. Aims & Definitions

The aim of this paper is to examine the legal aspects of the use of social networking in relation to the employment relationship

The term 'Social Networking' is taken to mean, as per the definition of D.M.Boyd and N.B.Ellison[1], web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, view and traverse their list of connections and those made by others within the system; to the above definition the ability to exchange data with other system users in the form of comments, files, messages etc should be added, as an essential part of the services.

An 'Employment Relationship' in this paper refers to any dependent employment relationship, valid or not, for a definite or indefinite period of time, full or part-time, in any place (including home or teleworkers), irrespective of duties or tasks or position assigned.

Although the Internet and most web services are inherently world reaching, references in this paper to specific legislation will be, unless otherwise stated, to Greek legislation.

1.2. A networked world

Less than a year ago, the 'Economist'[2] suggested that if Facebook were to be a country, the ubiquitous social networking site would be the world's third most populated country with more than 500 million active users and rising fast, behind leaders China (1.35 billion) and India (1.21 billion). Myspace would be the 5th largest country with 300 million users and Twitter the 8th with 124 million. In fact 'Facebook' is, at the time this paper was concluded, about to reach 700 million users, according to Socialbakers[3], a blog that tracks Facebook statistics.

1.3. The main conflict: Public vs Private

As with many questions relating to the use of technology in recent years, we attempt to find an analogy with the off-line world. In this context it might be fair to ask: 'If postings in cyberspace are equivalent to the behaviour in the public square, then are postings in Social Networks equivalent to behaviour in a private party?' Does this mean that a different set of rules apply to Social Networks, as opposed to the rules that apply to the Internet in general?

2. Use of Social Networks in an employment context

2.1. Employers and Social Networks: A love and hate relationship

For businesses, the use of Social Networks is a double-edged sword, as it can have both favourable and unfavourable consequences. On the one hand social networking is a great way to:

- Create brand awareness
- Manage online reputation
- Recruit talent
- Learn about technologies and competitors

- Intercept potential prospects

On the other hand, the use of Social Networks gives rise to a lot of worries for employers:

- Liability (given that accusations for libel, defamation, harassment or sexual harassment, discrimination etc. based on the behaviour of the employer or of the employees in the Social Networks are not uncommon)
- Security issues (i.e. the 2008 Koobface worm - the name is an anagram of the word 'Facebook'[4])
- Leaking of trade secrets
- Decrease in productivity (not an unfounded worry since it is estimated[5] that on Social Networking is spent worldwide a 22% of the total internet hours spent by all users)
- Copyright or trademark infringement
- Unauthorized use of client names or other info
- Creation of an unproductive workplace environment
- Corporate Espionage. The threat is real as hackers bypass security and access sensitive data using social engineering, thus having access to lists of employees, qualifications, functions and connections and committing crimes such as loss of corporate IP, hacking networks or blackmailing employees[6].

2.2. Social Networks misuse and the impact for the employees

A cornerstone of employment law is the employee's obligation of loyalty to the employer[7] (as foreseen by articles 288, 361, 652 of the Civil Code). In essence, the obligation of loyalty means that an employee should support and not harm the lawful interests of the employer.

From the general principle of the obligation of loyalty stem specific obligations, such as the ones:

- to respect employer's personality
- to maintain confidentiality
- not to compete with employer's business
- to get along with colleagues
- not to disparage employer's products

This does not mean however, that an employee may not act against the employer's rights in order to protect her own lawful interests or expose unlawful conduct (applicable also when employee's duties include postings in social networks about employers products).

It goes without saying that, absent exceptional circumstances, any misuse of the Social Networks by the employee, of the kind described in 2.1. above, may constitute violations of the employment contract's obligations for the employee and may be sanctioned, even leading to termination of the employment relationship.

They could also lead to penal sanctions: i.e. an employee that disseminates false or true (but confidential) information about the company could face criminal liability based on one or more of the following Penal Code provisions: Defamation (362 PC), Aggravated Defamation (363 PC), Defamation of a Corporation (SA) (364 PC), Fraud (386 PC), Fraudulent damage (389 PC), Secrecy of Letters (370 PC), Secrecy of data of particular types (i.e confidential professional or belonging to private enterprises data) (370B PC), Breach of professional confidentiality (371 PC).

It should also be reminded that a criminal act of an employee that is related to the employment relationship, may lead to unpaid termination of the employment relationship.

2.3. Examples of problems in using Social Networks in employment or quasi employment relationships

A significant (and growing!) number of incidents involving misuse of Social Networks and creating tensions between employers and employees has been recorded in recent years in many parts of the world. A selection illustrating the materialization of various fears that were previously mentioned follows:

Ireland[8]

In 2007 a customer brought to the attention of a retail outlet that an employee had posted on Bebo unflattering comments about a manager. The employer initiated disciplinary proceedings against the employee. A disciplinary meeting was held and the employee was dismissed for gross misconduct.

The claimant initiated unfair dismissal proceedings. The Employment Appeal Tribunal held that the dismissal was disproportionate to the offence and directed that the retail outlet pay the claimant €4,000 in compensation. *(Emma Kieran v A Wear Ltd, Employment Appeals Tribunal, Case Reference UD643/2007, MN508/2007*)

France[9]

Three employees of a French consulting company, posted comments in late 2008 from their personal home computers on Facebook about company managers, including its Human Resources Director.The conversation appeared on one of the three employees Facebook page, with comments by two other employees. The employer discharged all three employees for rebellion against the company's hierarchy, and denigration of the company's image.

The employee on whose Facebook page the comments appeared chose mediation while the other two filed a complaint before the labour court.

The employees argued that the Facebook page was private and the comments were humorous. The employer argued that the list of Facebook 'friends of friends' included the employee who owned the Facebook page and other company employees and the Facebook page was capable of being read by people outside the company during the time period in which it had been posted.

The Court accepted the employer's arguments and upheld the discharge of the two employees (*Barbera v. Société Alten SIR*; *Southiphong v. Alten Société SIR*, *Prud'hommes de Boulogne-Billancourt*, Nos. RG-F-/326/343, November 19, 2010)

Greece

In 2008 a higher education professor posted on Facebook derogatory comments as well as documents relating to the work and career of a colleague. Both professors were candidates for the same academic position.

The Court of First Instance of Thessaloniki (*16790/2009*)[10] found that the postings constituted an unlawful infringement on the claimant's personality and issued an injunction requiring the offender to refrain from using the claimant's personal data or using the Internet for the publication of the aforementioned documents.

In 2009 an airline employee was fired from her job because she was spending too much time visiting social networks such as Facebook at work, neglecting her duties and business clients calling. The employer had previously sent an email to all employees forbidding visits to social network sites.

The Labour Disputes Section of the Court of First Instance of Athens (*34/2011*)[11], in a decision widely published in the Press, found that the dismissal was not abusive, as the claimant's behaviour constituted a breach of her employment contract's obligations.

Canada[12]

In 2010 two employees posted on Facebook offensive comments about their supervisors and their employer. A supervisor who was an employee's Facebook 'friend' saw the comments and after being removed from the 'friends' list monitored the comments with the help of a former employee 'friend'. One of the employees alleged that his Facebook account could have been hacked as he had left it logged on at work. The employer terminated the employment of the two employees. The Union filed an unfair labour practice complaint alleging that there was no cause for termination and the employer was motivated by anti-union animus.

On 22.10.2010 the British Columbia Labour Relations Board decision in *Lougheed Imports Ltd (West Coast Mazda) v United Food and Commercial Workers International Union, Local 1518* dismissed the Union's application.

The decision established that employees have no reasonable expectation of privacy in comments made on social networking sites, and that when those comments are damaging to the employer's business or offensive, insulting and disrespectful to supervisors, the employer may have just cause for termination; however, employers should be cautious when deciding to monitor these sites.

United Kingdom[13]

In 2010 a government department employee, had made several posts on Twitter mentioning the fact that she had been hungover while at work, as well as making personal comments about people she had worked with. Two national newspapers reprinted these comments in articles about the views and behavior of public officials.

The employee complained to the Press Complaints Commission, that it was a breach of her privacy to reproduce the comments without permission

According to the commission, the employee made two main points: that it was reasonable to expect the message would only be seen by the 700 followers on her account; and that her account was clearly labeled as a personal view that did not reflect her employer's views (but not at the time the newspapers used the material)

The commission ruled to reject the complaint stating that anyone could have stumbled across the information and the retweet feature of Twitter meant there was a strong possibility it would be seen by people other than the employee's followers.

One notable point about the case is that the two newspapers stressed that Baskerville had openly used her own name rather than posting anonymously.

Unites States[14]

In 2009, a business owner stumbled upon an employee's MySpace profile saying this person was planning a two-hour lunch because her boss was out of the office.

In 2010 an employee exposed 'crucial details' on Twitter about a potential business deal with a prospective client, but the client never saw the post and the deal went through.

In 2009, an account manager of a firm posted on her Facebook profile that she had quit her job. One of the firm's largest clients, previously befriended by the employee, learned about her resignation this way and lodged a complaint.

The owner of a staffing agency in Las Vegas, said some of the independent contractors she hires seem to forget that she follows them on Twitter: *'One girl said she was out having a great time drinking and she called in sick the next morning.'*

Israel[15]

Although not, strictly speaking, an 'employment' relationship, this incident, by far the most spectacular, demonstrates the threat Social Networks' misuse poses to a quasi employer's operations: in March 2010 the Israeli military called off a raid on a West Bank town after a soldier posted on his Facebook profile that his combat unit was going to 'clean up' the area. The soldier was reported by his friends, court-martialed and sentenced to 10 days in prison, according to media reports.

3. Issues in the use of Social Networks before, during and after employment

3.1. 'Maybe we just don't like you'

The problems start even before an employee is hired, during the selection process. It has been the general belief that when making hiring decisions, employers can lawfully use information that the applicant voluntarily disclosed and is publicly available. The advent of Social Networks made it extremely easy for employers to use[16] information posted by the applicants themselves in order to find out whether an applicant has been involved in illegal activities, but also to discover incidents of poor work ethic, including hostile feelings about previous employer and discriminatory tendencies, to check the quality of the applicant's writing or communications skills and generally to evaluate the applicant's judgment in maintaining his or her public online persona.

However employers run the risk of being held criminally and/or administratively liable if found to have violated, in a hiring decision, anti-discrimination in the workplace laws (L.3304/2005) related to use of criteria such as race, age, disability, religion, sexual orientation etc.

Still, regulation is fast moving to claim this, so far uncharted, territory. In Finland, Data Protection Ombudsman Reijo Aarnio ruled that employers cannot use Internet search engines (i.e. Google) to obtain background information on job candidates[17]. In the UK the Employment Practices Code published by the UK Information Commissioner's Office says[18] that during a recruitment process, employers have to: '*Explain the nature of and sources from which information might be obtained*'. Even more drastic, a bill[19], to be passed by the German Parliament, would prohibit employers from using social networking sites such as Facebook (but not 'professional' online networks such as LinkedIn or Xing) when conducting background checks and screening current and potential employees.

3.2. 'To poke or not to poke at work?'

As already mentioned, employers have many reasons to be concerned about the use of Social Networks at work. During the employment, the most pressing issue regarding use of Social Networks in the workplace is whether or not to allow it and if not how to implement such ban. The simplest solution for an employer is to limit access at such networks from the workplace, to the extent possible. Indeed, according to a survey[20] social networks are among the most commonly blocked websites in businesses. Here's the top ten (percentages indicate proportion of business networks using blacklisting feature that reference a given site):

1. Facebook.com — 23%

2. MySpace.com — 13%
3. YouTube.com — 11.9%
4. Ad.Doubleclick.net — 5.7%
5. Twitter.com — 4.2%
6. Hotmail.com — 2.1%
7. Orkut.com — 2.1%
8. Ad.Yieldmanager.com — 1.8%
9. Meebo.com — 1.6%
10. eBay.com — 1.6%

For businesses that want to limit their employees' access to social networks, filtering is the legally safest option, as it is less invasive than monitoring. It remains, however, an open question whether blocking employees' access yields results, since use of social networking has become the norm, especially among younger workers. TUC (British Trades Union Congress) General Secretary Brendan Barber said[21] in 2007: '*Simply cracking down on use of new web tools like Facebook is not a sensible solution to [the] problem ... Better to invest a little time in working out sensible conduct guidelines, so that there don't need to be any nasty surprises for staff or employers*.'

3.3. 'Gone, but not forgotten…'

Problems relating to Social Networks do not end, for employers, when an employee leaves work. Supervisors and co-workers are increasingly asked to 'recommend' former employees on LinkedIn after separation from employment.

Technically, a positive recommendation on a person's LinkedIn page is not the same as an employment reference (Art. 678 Civil Code), unless given by an authorized company representative and has been requested by the employee.

However in practice it amounts to the same, so employers should consider adding to their policies a prohibition on managers from 'recommending' or commenting on the job performance of former employees via social media without prior specific authorization.

4. The concept of 'friendship' in Social Networks used in an employment context

4.1. Between friends & the '*household exemption'*

An interesting question is raised when discussing comments posted on Social Networks: are we taking things too far? Shouldn't we tolerate comments that take place in discussion between friends, much as we do when such discussions take place in the non virtual world?

To answer this question we should consider a few issues. But first of all it is not entirely true that we have (at least legally speaking) a higher degree of tolerance for acts that violate a law, even when they take place among friends (more on that later). But the latin proverb *'verba volant, scripta manent'* obviously applies in this case, too, giving the impression that just because certain acts in the non virtual world are not documented, they are not punishable.

In any case, I suggest that an analogy applies with the '*household exemption'* introduced by the Opinion 5/2009 of the Working Party of Article 29 of Directive 95/46/EC[22]. According to this Opinion, when users operate within a purely personal sphere, contacting people as part of the management of their personal, family or household affairs, the regulations governing data controllers do not apply. However, the '*household*

exemption' does not apply and the user might be considered to have taken on some of the responsibilities of a data controller, if a user:

- acts on behalf of a company or association
- uses the social network mainly as a platform to advance commercial, political or charitable goals
- acquires a high number of third party contacts, some of whom he may not actually know
- takes an informed decision to extend access beyond self-selected 'friends'
- provides access to profile to all members within the social network or the data is indexable by search engines

The number of third part contacts ('friends') is indeed a strong indication of the type of use. Dunbar's Law (Robin Dunbar, British anthropologist): limits[23] to 150 the number of individuals with whom any one person can maintain stable relationships. Facebook allows a maximum of 5,000 connections. BT's innovation head JP Rangaswami[24] thinks (but has not proved) that social software might help raise the Dunbar number.

Given the above, I am inclined to suggest that if the household exemption does not apply, then we are *not* in a closed environment of friends.

It should also be noted, as was mentioned earlier, that even the application of the household exemption does not exclude the possibility of a user being liable according to general provisions of national civil or criminal laws in question (e.g. defamation, liability in tort for violation of personality, penal liability).

4.2. When a 'friend' is not a friend

In most Social Networks, the user has a degree of control over the privacy settings. He or she can limit access to his or her information, thereby excluding people that can potentially harm the user. Employers or potential employers would often fall into this category. What then if they try to bypass the restrictions imposed by a user? Can one have access to information posted on social sites by *deceptively* 'friending' a person? (i.e. the employer befriending an employee by not revealing his or her real identity).

It is more than likely that such an action would be illegal, although it is not entirely clear which article of the Penal Code would be breached (Article 386 PC refers to fraud, but requires damage to property which would be hard to prove, 370C par.2 PC or 22 par. 4 L.2472/1997 forbid unauthorized access to data, but the concept of 'authorization' might constitute an issue when user does grant access and 415 PC, a misdemeanor, punishes the unauthorized change of name). In all cases, an employer that would use data that have not been collected fairly and lawfully, as article 4 of L.2472/1997 requires, risks being subject to the administrative, civil and possibly criminal sanctions that the Law foresees.

When, however, the *real* name is used, an ethical issue might arise but not necessarily a legal one (with the exception of Lawyers, who, collecting data in such a manner possibly violate article 38 of the Code of Ethics)[25].

5. Conclusions

Social Networks developed rather recently, as part of what is now commonly called Web 2.0. The Law, certainly moving in slower speed than technological developments, has not yet dealt specifically with the issues arising from Social Networks (mis)use, in general or, more specifically, in the employment relationship. This does not mean that their use is not regulated. As is to be expected, Courts apply general principles and legislation in matters involving Social Networks that are brought before them. However, the

employment relationship, by its nature sensitive and dynamic, flourishes and bears fruits when the rules that govern it are clear, precise and respected. To this end it is recommended that employers have in place a risk mitigation policy and program. This may sound commonplace, however a survey showed that only 17% of employers actually do have such a policy. (Deloitte 2009[26])

The employer may use the policy in addition to other company policies, to specifically address issues relating to Social Networks, such as to[27]:

- Prohibit the use of *company email address* to register with a social network
- Prohibit the use of company *logos or trademarks* in postings, pages etc.
- Request employees to *disclose* (to identify themselves as employees of the company, if needed, as in cases when they write reviews for company products) and *disclaim* (that the views express are those of the employee and do not reflect the views of the employer)
- Prohibit *tweeting* during company meetings.
- Give *guidelines* on friend requests by colleagues or managers and
- Generally *regulate*, to the extent that this does not contradict the Law, the Social Networks use by the employees.

A policy should not try to set out all forms of Social Networks, as it would run the risk of being outdated by the time it was adopted.

6. Future Research

This brief analysis of the matter has not been concerned, for lack of time and resources, with the important issue of trade union rights in using Social Networks. This may well be a sub-chapter in the greater issue of trade unions' use of the Internet, but given the rise in use of the Social Networks, I believe that further discussion is needed on whether and how archaic and quickly turning to obsolete methods of trade union communications can be adapted to the Internet age without disrupting the essential workplace order.

Endnotes

[1] Danah Boyd, Nicole Ellison, '*Social Network Sites: Definition, History, Scholarship*', Journal of Computer Mediated Communication, Vol. 13, issue 1, pp. 210-230, October 2008, available at http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html accessed 23.6.2011

[2] 'The Economist', 22.7.2010

[3] Socialbakers, '*Facebook is globally closing in to 700 million users!'* available at http://www.socialbakers.com/blog/171-facebook-is-globally-closing-in-to-700-million-users/ accessed 7.6.2011

[4] Lynn Greiner, '*Social Networking's Security Pitfalls: How You Can Go Oh So Wrong with Facebook, LinkedIn and MySpace'*, 9.2.2009, available at http://www.cio.com/article/480030/Social_Networking_s_Security_Pitfalls_How_You_Can_Go_Oh_So_Wrong_with_Facebook_LinkedIn_and_MySpace accessed 23.6.2011

[5] NielsenWire, '*Social Networks/Blogs Now Account for One in Every Four and a Half Minutes Online'*, 15.6.2010**,** available at http://blog.nielsen.com/nielsenwire/global/social-media-accounts-for-22-percent-of-time-online/ accessed 23.6.2011

[6] To deal with these problems it is recommended by ENISA (the European Network and Information Security Agency) that employers have awareness training, security policy for Social Networks and limited provision of information. See ENISA's Position Paper 1, '*Security Issues and Recommendations for Online Social Networks'*, October 2007, available at http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks/at_download/fullReport accessed 24.6.2011

[7] More on this at Stylianos Vlastos, '*Atomiko Ergatiko Dikaio' ('Individual Labour Law'*, in Greek), Ant.N.Sakkoulas Publishers, 1999
[8] As reported on Collier Broderick site, '*Dismissal Judged Unfair'*, available at http://www.collierbroderick.ie/Articles/Dismissal-Kiernan-v-Awear-Ltd , accessed 24.6.2011
[9] Available (in French) at http://legalis.net/spip.php?page=breves-article&id_article=3027 accessed 24.6.2011
[10] DIMEE ('Dikaio Meson Enimerosis kai Epikoinonias' - 'Media &Communication law', in Greek) 2009, p.400
[11] Available (in Greek) at http://www.dsanet.gr/Epikairothta/Nomologia/mprath34_2011.htm accessed 24.6.2011
[12] The decision is available at the Labour Relations Board - British Columbia site at http://www.lrb.bc.ca/decisions/B190$2010.pdf accessed 24.6.2011
[13] The rulings are available at the Press Complaints Commission site at http://www.pcc.org.uk/news/index.html?article=NjkzNQ and http://www.pcc.org.uk/news/index.html?article=NjkzNA (Regarding the complaints against 'The Independent on Sunday' and Daily Mail', respectively) accessed 24.6.2011
[14] Incidents reported by Sarah Needleman, '*Facebook, Twitter Updates Spell Trouble In Small Workplace'*, 10.3.2010, The Wall Street Journal (online), available at http://online.wsj.com/article/SB10001424052748703701004575113792648753382.html accessed 23.6.2011
[15] Reported by CNN World, '*Israeli military calls off raid after soldier posts details'*, 3.3.2010, available at http://articles.cnn.com/2010-03-03/world/israel.raid.facebook_1_idf-soldier-israel-defense-forces?_s=PM:WORLD accessed 23.6.2011
[16] In fact, in 2008 already 20 percent of companies admitted to checking out candidate's profiles on social-networking sites. PC World, Carrie-Ann Skinner, '*Employers Admit Checking Facebook Before Hiring'*, 14.9.2008, http://www.pcworld.com/businesscenter/article/151044/employers_admit_checking_facebook_before_hiring.html accessed 23.6.2011
[17] Nicole Kennedy, Matt Macko, '*Social Networking Privacy and Its Effects on Employment Opportunities'* in '*Convenient or Invasive? The Information Age'*, available at http://www.ethicapublishing.com/inconvenientorinvasive/2CH12.pdf accessed 23.6.2011
[18] European Digital Rights site, '*Germany Wants A New Law To Protect Employees' Privacy'*, EDRi-gram - Number 8.17, 8 September 2010 available at http://www.edri.org/edrigram/number8.17/law-facebook-germany-employees accessed 24.6.2011
[19] Morrison & Foerster Social Media Newsletter, Vol. 1, Issue 3, p.5, September 2010, available at http://www.mofo.com/files/Uploads/Images/100927-Socially-Aware.pdf accessed 24.6.2011
[20] OpenDNS '*2010 Report Web Content Filtering and Phishing'*. Source: Sample of OpenDNS business networks using whitelisting in 2010 (n = 31,623) available at http://www.opendns.com/pdf/opendns-report-2010.pdf accessed 18.6.2011
[21] Mail online, '*Let workers use Facebook during office hours, say union bosses'* available at http://www.dailymail.co.uk/sciencetech/article-478699/Let-workers-use-Facebook-office-hours--say-union-bosses.html, 30.8.2007 accessed 18.6.2011
[22] Adopted on 12 June 2009 available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf accessed 18.6.2011
[23] Research Intelligence, The University of Liverpool, Issue 17, August 2003, p.3, available at http://www.liv.ac.uk/researchintelligence/issue17/pdf/resint17.pdf accessed 18.6.2011
[24] '*Of followers and followees and friends*' available at http://confusedofcalcutta.com/2009/01/11/of-followers-and-followees-and-friends/ accessed 18.6.2011
25 "A lawyer has the obligation to avoid any communications with the opponent and any discussion related to the case, without his client's approval. I f the opponent has hired a lawyer for the case, his lawyer should be called in all discussions… A lawyer should not act in a malicious manner to cause the loss of rights by his opponent…". It is interesting to note that the New York State Bar Association and the New York City Bar Association have issued opinions on whether a lawyer may or may not "friend" an individual to obtain information. When the lawyer's real name is used, Rule of Professional Conduct 4.2, which prohibits a lawyer from communicating with a represented party about the subject of the representation absent prior

consent from the represented party's lawyer, is applicable (Paul Garrity and Kathryn Hines, '*Legal Ethics and The Social Network'*, 18.10.2010, available at http://www.socialmedialawupdate.com/2010/10/articles/ediscovery/legal-ethics-and-the-social-network/ accessed 23.6.2011)

[26] Elizabeth McNamee, Kim Magyar, '*Are You Building a House of Cards? Social Networking in the Office'*, ACC Docket, Vol. 28, issue 7, pp. 29-38, September 2010

[27] Useful suggestions can be found in Larry Silverman and Terri Imbarlina Patak's article '*How You Can Safely Use Social Media with Employees*', ACC Docket, Vol. 28, issue 3, pp. 19-30, April 2010