Social Networks in the workplace: employees' rights to online privacy

By

LOUIZA ANTONIADES(27394931)

Submitted in fulfilment of the requirements for the degree:

LLM
(Mercantile Law)

In the Faculty of Law,
University of Pretoria

November 2014

Supervisor: Mrs Papadopoulos

TABLE OF CONTENTS

SUMMARY

The aim of this application is to complete the LLM degree with a dissertation entitled "Social networks in the workplace: employees' rights to online privacy".

The study entails an analysis of the current regulatory environment in South Africa, together with relevant case law and legislation involving the rights of employees' in the workplace accessing social networking sites during working hours. The aims of this study are to analyse the current South African legislative position, and to determine the legal framework for the protection of employees' online privacy.

It can be seen from the basic information below, that one of the questions that arises is whether privacy can exist where there is in actual fact no physical space, and whether there is any legislation that can be applied in order to reach a conclusion.

It is clear that the dissertation is working from a hypothesis that an employee's right to online privacy is protected through various South African legislation as well as case law, provided that certain measures are taken. At present an employer is required to put in place an electronic communications policy in the workplace which should also comply with Schedule 8 of the Labour Relations Act 66 of 1995. The Employee must then be made aware of such a policy and consent must be given by the employee by signature thereof, which shall then bind the employee to the terms of the policy.

The dissertation further looks at the following questions that arise as to what rights the employers' have in respect of monitoring their employees' online activity and what the employees' rights to online privacy are with regard to social networks during the course of working hours. Legislation is referred to, for example the interplay between the PPI and RICA. The ECT Act is also discussed with reference being made to unauthorised access and interception with data, section 86(1) in particular prohibits the above without the necessary consent to do so.

These present the most pertinent questions that are to be answered in the dissertation. The dissertation will reach a conclusion as to the above with all relevant authorities, case law and legislation.

Annexure G

University of Pretoria

Declaration of originality

This document must be signed and submitted with every essay, report, project, assignment, mini-dissertation, dissertation and/or thesis

Full names of student: Louiza Antoniades

Student number: 27394931

Declaration

1. I understand what plagiarism is and am aware of the University's policy in this regard.
2. I declare that this mini-dissertation (eg essay, report, project, assignment, mini-dissertation, dissertation, thesis, etc) is my own original work. Where other people's work has been used (either from a printed source, Internet or any other source), this has been properly acknowledged and referenced in accordance with departmental requirements.
3. I have not used work previously produced by another student or any other person to hand in as my own.
4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.

Signature of student:

Signature of supervisor:

CHAPTER 1: INTRODUCTION

1.1 PRIVACY

In her analysis of the public disclosure tort in the United States legal system, Abril asserts that "[t]raditionally, privacy has been inextricably linked to personal space. In turn space often defines our notions of personhood and identity. Consider for example, the social stature ascribed to sitting in a corner office. Spatial concepts are interrelated with cultural norms prescribing social organization and human behaviour, interaction and expectations."[1] According to Neethling a person's right to privacy means that a person should have control over his or her affairs, reasonably free from unsolicited intrusions.[2]

Privacy is a personality interest and in turn a personality interest is a non-patrimonial interest that cannot exist separately from the individual.[3]

In South Africa the right to privacy is protected in terms of both the common law and the Constitution of the Republic of South Africa (hereinafter referred to as the Constitution).[4] Under the South African common law a person can rely on the law of delict for the protection of his or her right to privacy.[5] A delict is the wrongful, culpable conduct of a person that causes harm to another.[6] The Constitution guarantees a general right to privacy with specific protection against searches and seizures, and the privacy of communications.[7]

Neethling's widely accepted definition informs us that privacy is "an individual condition of life characterised by exclusion from the public and publicity. This exclusion embraces all those personal facts which the person concerned has

---

1 Abril (2007). Recasting Privacy Torts in a Speechless World. *Harvard Journal of Law and Technology* 3-4, also referred to in Papadopoulos S *Revisiting the Public Disclosure of Private Facts in a Cyberworld* 2009 Obiter vol 1, 38-39.

2 Neethling, Potgieter and Visser *Neethling's law of Personality 2ed (2005) 31 FN 334.*

3 Neethling *et al* (*2005)* 14; Roos, A. 2003. The law of data (privacy) protection: a comparative and theoretical study. Unpublished LLD Thesis, Pretoria: Unisa.

4 Papadopoulos & Snail *Ed Cyberlaw@SA III: The law of the internet in South Africa* (2012) 276.

5 Papadopoulos (2012) 276.

6 Neethling *et al* (2005) 1.

7 Roos (2003) (LLD Thesis UNISA) 540.

determined should be excluded from the knowledge of outsiders and in respect of which there is a will that they be kept private".[8] However, as explained by Neethling, in order to be able to define privacy, it is therefore necessary to understand that every personality interest has a pre-legal existence in factual reality, and if those principles are based on an inaccurate understanding of factual reality it may lead to uncertainty, ambiguity and that it may produce unfair results in law.[9]

1.2 ONLINE SOCIAL NETWORKS

As the decade drew to a close, a new development would change the face of internet and specifically the World Wide Web; this would be known as social networking.[10] Social networking sites such as Twitter and Facebook are now ubiquitous: companies, institutions, and individuals utilise these networks for a variety of purposes.[11] Online social networking websites facilitate hundreds of thousands of social interactions in a day and new technology has enabled unique social situations that create the potential for unprecedented invasions of privacy.[12]

Online social networking sites have been defined, by Boyd - as "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site".[13]

Online social networking usually refers to websites whose main purpose is to act as a link between users through the use of computer software in order to build online

---

8 Neethling *et al* (2005) 32.

9 Neethling et al (2005).

10 Mischke, C. 2011 'Social Networks, privacy and dismissal: Facebook, Twitter et al: the employer's reputational risk'. *Contemporary Labour Law,* Vol. 21 No. 2: 12.

11 *Idem.*

12 Abril (2007*)* Recasting Privacy Torts in a Speechless World. *Harvard Journal of Law and Technology*, 5.

13 Boyd, D.M & Ellison, N. 'Social network sites: Definition, history, and scholarship' (2007) 13 J *of Computer-Mediated Communication* article 11, available at *http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html* (accessed 28 October 2014)

social networks.[14] They provide various ways for users to communicate with one another, by using visible profiles and a display of an articulated list of friends who are also users of the system.[15] Anyone with a valid e-mail address can create a profile on an online social networking site.[16] Online social networking has revolutionised the way people communicate and share information with one another.[17] After one has joined an online networking site, the user is then prompted to identify others in the system or to invite others to join.[18] The friends' lists contain links to each friend's profile, which then allows viewers to navigate the network by navigating through the "friends" lists.[19] On most sites the list of friends is visible to anyone who is permitted to view the profile, although there are expectations.[20] No longer are users of the Internet passive consumers of information placed by others: they are now the creators of their own content.

Social networking sites (SNSs) such as Facebook and Twitter offer not only convenience and the ability to establish and maintain social links, but also the possibility of almost instantaneous communication with large groups of people from different backgrounds.[21] These networks are portable in that they can be accessed anywhere, not only by personal computers, but also by smart phones and tablet computers.[22]

A common restriction is to set a profile as visible to friends of the user only.[23] However, this in itself does not restrict the information posted to the list of friends on one particular user's profile as it may still be visible to the entire interlinked chain of the user's friends.[24] If there is an option for the user to select a privacy setting where only the user's friends have access to the information, and such option is not

14 Papadopoulos, S. 2009. Revisiting the Public Disclosure of Private Facts in a Cyberworld. *Obiter* vol 1, 32.

15 *Idem.*

16 *Idem*.

17 *Ibid* at 31.

18 Papadopoulos, S. 2009. Revisiting the Public Disclosure of Private Facts in a Cyberworld. *Obiter.* Vol 1: 32-33.

19 *Ibid* at 33.

20 Papadopoulos, S. 2009. Revisiting the Public Disclosure of Private Facts in a Cyberworld. *Obiter.* Vol 1: 33.

21 Mischke, C. 2011. 'Social Networks, privacy and dismissal: Facebook, Twitter et al: the employer's reputational risk' *Contemporary Labour Law,* Vol. 21 No. 2: 12.

22 *Idem.*

23 *Idem.*

24 *Idem*.

selected, a profile is then public, and the user's first name, picture and profile information will accompany all of the user's activities within the website.[25] This information will then be searchable by anyone regardless of any membership, making this information public.

1.2.1 Reasons why people use online social networking sites

There are three aspects of social interaction that a SNS enables, as identified by Grimmelman[26].

Firstly, the profile function allows the user to create an *identity*. It lets the user say who he or she is, and it allows the user to present him- or herself the way the user wants to in a specific context. It is important to recognise that the identity that a user portrays is aimed at the specific audience.[27]

Secondly, the contacts function allows the user to form or maintain one-to one connections or *relationships* with other users. This means that personal information is then shared with the contact. Sharing personal information with someone shows that one trusts that person; it creates a sense of intimacy.[28]

Lastly, the function of traversing lists of contacts allows the user to become part of a *community* or a 'social network'.[29]

The question is whether privacy can exist where there is in actual fact no physical space or inherently private subject matter, secrecy or seclusion and more pertinently whether the established jurisprudence can be applied within the phenomenon of social networking sites such as Facebook.[30]

---

25 *Idem.*

26 Grimmelman, J. '*Saving Facebook'* (2009) 94 IOWA *LR* 1134 at 1144.

27 *Idem.*

28 *Ibid* at 1154.

29 *Idem.*

30 *Ibid* at 31.

1.3 PRIVACY AND THE INTERNET

In the workplace most employers will have to give some thought to containing or managing the legal risks inherent in employee access to and the usage of electronic communications and the internet, by having an electronic communications policy which will in turn monitor the employee's access and usage of the internet with the consent of the employee.[31] Many internet users will find that their web activities are being monitored without their consent and this will prove to be problematic, as they may feel that this infringes on their right to privacy.

Within this context it is important to remember that the Constitution states that '[e]veryone has the right to privacy, which includes the right not to have…the privacy of their communications infringed'.[32] It is clear that the Constitutional safeguard of privacy by its nature protects a wide range of overlapping and inter-related rights.[33]

This is also true of the workplace where employees share office space and where computers, the internet, and telephones are used as means of communication to perform activities of varying nature in the employer's interest , but often also in an employee's own private interest.[34]

It can be said that the Internet, by the middle of the first decade of the 21st Century, had become a library without a librarian.[35] There was no editor to assist the users in distinguishing the good, the bad, and the lunatic fringe.[36] Users are to decide on their own as to what would be reasonably expected of them when accessing the internet.

---

31 Papadopoulos (2012) 276.

32 Section 14 of the Constitution.

33 McGregor, M. 2004. The right to privacy in the workplace: general case law and guidelines for using internet and e-mail. *SA Merc LJ*, 16: 638 FN 8.

34 *Ibid* 639.

35 Mischke, C. 2011. 'Social Networks, privacy and dismissal: Facebook, Twitter et al: the employer's reputational risk' *Contemporary Labour Law,* Vol. 21 No. 2: 11.

36 *Idem.*

1.3.1 Legal framework for the protection of privacy.

Privacy has been described as a broad value that represents concerns about autonomy, individuality, personal space, solitude and intimacy.[37]

In the workplace internet usage is often carefully monitored in order to reduce the risks that employers are exposed to.[38] Dating back to 1976, Neethling emphasised that individuals should be able to decide for themselves whether their personal information can be collected, intercepted and used, and that this right to self-determination should be afforded legal recognition.[39]

1.4 INFRINGEMENT OF PRIVACY

The protection of the right to privacy in the workplace has been a topic of a number of judgments, especially at a time where technology and devices are becoming an increasing threat to one's privacy.[40]

A distinction can be drawn between monitoring and surveillance.[41] Monitoring is when an employer merely observes the activities of an employee to observe conduct or measure performance.[42] Surveillance, on the other hand, is where the employer engages in the observation of the conduct or communication of employees without their consent or any knowledge of such.[43]

It must be noted that it is very difficult to clarify the right to privacy in the context of the employment relationship, as it is seen as very unique.[44] On the one hand, the employee has a right to privacy but at the same time is supposed to be honest and loyal to his employer, especially during working hours. On the other hand, the

37 SA Law Reform Commission (SALRC). 2005. Discussion Paper 109, Chapter1.

38 Papadopoulos (2012) *276.*

39 *Idem.*

40 Van Niekerk, A. 1994. The Right to Privacy in Employment*. Contemporary Labour Law,* 3: *97.*

41 Dekker, A. 2004. Vices or devices: employee monitoring at the workplace*. SA Mercantile Labour Journal,* 16: 624.

42 *Idem.*

43 *Idem.*

44 Dekker, A. 2004. *SA Merc LJ*, 16: 626.

employer is contractually entitled to know the content of the employee's calls and internet usage in so far as they relate to business.[45]

According to the South African Law Reform Commission, the courts seem to be developing the common law by instilling into it the spirit of the Constitution. Therefore any action in this sphere of the law is a hybrid action based on a mixture of common law and constitutional directives.[46] It has been expressed that caution must be exercised when attempting to assign common law principles to the interpretation and/or limitation of constitutional rights.[47] A distinction is therefore drawn between the two-stage constitutional enquiry into whether or not a right has been infringed and whether such an infringement can be justified, and a single enquiry under the common law, where it has been determined whether or not an unlawful infringement of a right has taken place.[48] This two-stage test has been developed by the South African Courts.[49]

An employer can however justify an intrusion of an employee's privacy by showing that the employee has consented to an intrusion, normally by means of prior consent in terms of the employment contract.[50] But the employee should be aware of the content and extent of such consent.[51] The American courts, however, seem to have adopted a view that an employee can have a reasonable expectation of privacy, and that such reasonableness is judged in the light of business necessity.[52] In *Katz v*

---

45 *Idem.*

46 Neethling *et al* (2005).

47 *Ibid* at 32.

48 SA Law Reform Commission (SALRC). 2005. Discussion Paper 109, Chapter 2, 6.

49 McGregor, M. 2004. The right to privacy in the workplace: general case law and guidelines for using internet and e-mail. *SA Merc LJ*, 16: 640. Further the Constitutional Court held in *Bernstein* v *Bester* that privacy is an 'amorphous and elusive concept'. Further in *Protea Technology Ltd & another v Wainer and others* (1997) 9 BCLR 1225 (W), it was held that even in the employment context, the employee may receive and make telephone calls that have nothing to do with the employer's business. In respect of such calls the employee has a legitimate expectation of privacy. But in respect of conversations relating to the employer's affairs, the employer is entitled to demand and obtain as full an account as the employee can furnish. These conversations are seen as private and protected by the Constitution. As soon as the employee abandons the private sphere for that of his employer's business, he loses the benefit of privacy.

50 Dekker, A. 2004. *SA Merc LJ, 16: 624.*

51 Van Niekerk, A. 1994. The Right to Privacy in Employment. *Contemporary Labour Law,* 3: 100.

52 Dekker, A. 2004. Vices or devices: employee monitoring at the workplace. *South African Mercantile Law Journal,* 16: 624.

United States,[53] the Supreme Court found that a reasonable expectation of privacy could exist only where an individual had a subjective expectation of privacy, and where society recognised the expectation to be reasonable.[54]

The South African Constitutional Court in *Bernstein v Bester*[55] followed an approach that is consistent with that of the above mentioned case, where it was acknowledged that 'as a person moves into communal relations and activities such as business and social interaction the scope of personal space shrinks accordingly'.[56]

In terms of the limitation clause in the Constitution, the infringement of the right to privacy can sometimes be justifiable in the context of the employment relationship.[57]

Therefore in order to establish an infringement of the constitutional right to privacy, South African law applies a two-part test that requires a person to have a subjective expectation of privacy that society has recognised as objectively reasonable.[58] The subjective expectation of privacy is more than whatever feels private, while objectively this has to be reasonable within the context to qualify for such protection.[59] The subjective component of this test determines that a person cannot complain about an invasion of privacy if he or she has explicitly or impliedly given consent to such.[60] The objective component is more important, but it is often quite difficult to assess the kinds of privacy expectation that society would regard as objectively reasonable.[61] It has been argued that in modern society the right to privacy seeks to protect the following three related concerns[62]:

---

53 *Katz v United States* 389 US 347 (1967) and *Abel v United States* 362 US 217 (1960) 241.

54 Dekker, A. 2004. *SA Merc LJ,* 16: 624.

55 *Bernstein v Bester* 1996 (2) SA 751 (CC).

56 Collier, D. 2002. Workplace Privacy in the Cyber Age. *Industrial Law Journal,* 23: 1743.

57 Dekker, A. 2004. Vices or devices: employee monitoring at the workplace. South African Mercantile Law Journal, 16: 625.

58 Papadopoulos & Snail *Ed Cyberlaw@SA III: The law of the internet in South Africa (2012) 278.*

59 Currie, I. & De Waal, J. 2005. *The Bill of Rights Handbook.* 5th Ed .318-319. Cape Town: Juta.

60 Roos, A. The law of data (privacy) protection: a comparative and theoretical study. Unpublished LLD thesis, Pretoria: Unisa (2003), 556; refer also to Neethling, J., Potgieter, J.M. & Visser, P.J. 2005. *Neethling's law of personality.* 2nd Ed. Durban: Lexis Nexis 32 in *FN* 332 and 334.

61 McGregor, M. 2004. The right to privacy in the workplace: general case law and guidelines for using internet and e-mail. South African Mercantile Law Journal, 16: 640.

62 De Waal, J., Currie, I. & Erasmus, G. *The Bill of Rights Handbook* 4 Ed (2001) 269.

Firstly, the right to privacy seeks to protect aspects of a person's life in respect of which every person is entitled to be left to oneself – a person's body, certain places and certain relationships.[63] Secondly, the right to privacy aims to protect the opportunities for an individual to develop his or her own personality.[64] Lastly, the right to privacy seeks to protect the ability of individuals to control the use of private information about themselves.[65] From the above it is therefore clear that all three concerns are to some extent applicable to the employee in the workplace.[66]

According to Roos she states that 'the individual himself or herself determines which information is private, coupled with the will or desire to keep the particular facts private. If the will to keep facts private is lacking, the individual's interest in privacy is also lacking'.[67]

According to Currie and De Waal, the subjective expectation of privacy is more than whatever feels private, while objectively this has to be reasonable within the context to qualify for protection.[68] The objective component on the other hand is more difficult to establish and requires one to establish the *boni mores* or the reasonable legal views of the community at large.[69]

1.4.1 Grounds of justification

The traditional grounds of justification are consent, private defence, necessity, impossibility, provocation, statutory or official authority and the power to discipline.[70] As will be seen in the chapters to follow, the most important ground of justification is consent given by the employee. Such consent can be given by the employee expressly or tacitly, and when done so validly, there can be no question of illegality. The harm experienced will be justified and therefore lawful provided the person

63 McGregor, M. 2004. *SA Merc LJ,* 16: 640.

64 *Idem.*

65 De Waal *et al* (2001) 270.

66 McGregor, M. 2004. *SA Merc LJ*, 16: 640.

67 Roos (2003) (LLD Thesis UNISA) 563-564.

68 Currie *et al* (2005) 318-319; refer also to Cheadle, M.H., Davis, D.M. & Haysom, N.R.L. (Eds). 2000. *South African constitutional law; the Bill of Rights.* Durban: Butterworths, 183-189.

69 *Idem.*

70 Roos (2003) (LLA Thesis UNISA) 574 & 589.

giving the consent is legally capable of expressing his or her will freely and lawfully and that he or she has consented to the specific conduct.[71] As will be discussed in the chapters to follow, the ground of justification most relevant to this discussion is that of consent.[72] Consent may be given expressly or tacitly, and when validly granted there can be no question of wrongfulness.[73]

1.5 CONCLUSION

The right to privacy is not an absolute right, it has to be balanced with other rights.[74] The employee's right to privacy has to be balanced with the employer's business necessity or operational requirements,[75] therefore it has to be exercised within certain parameters: 'The claim to respect for private life is automatically reduced to the extent that the individual himself brings his private life into contact with public life or into close connection with other protected interests'.[76] It has been argued that whilst employers' legitimate interests might mean some encroachment, there should be an 'inviolable zone of privacy' for employees upon which employers should not intrude.[77] It would therefore not make sense to say that employees lose their right to privacy when they enter the workplace.[78] In terms of the Constitution, if it is established that a legal subject's right to privacy has been infringed, the defendants' conduct may not be wrongful if they can show that the invasion of privacy was reasonable and justifiable.[79] The employees themselves need to make sure that they protect their online 'identities' as well the information that they are sending, receiving or posting online. What the employee does online needs to be done with care and

---

71 Papadopoulos, S. 2009. Revisiting the Public Disclosure of Private Facts in a Cyberworld. *Obiter.* Vol 1:36-37.

72 *Idem.*

73 Neethling *et al.* (2005) : 250-251. Also refer to SALC 2005. Chapter 2: 28-29.

74 McGregor, M. 2004.*SA Merc LJ,* 16: 639.

75 *Idem.*

76 South African Law Commission *Interim Report on Group and Human Rights* (1994) 36.

77 Bibby, A. 'Who's got mail? At Work, e-mail and the Web Become Public' (August 2001) 40 *The Magazine of the ILO World of Work 4.*

78 McGregor, M. 2004. *SA Merc LJ*, 16: 639.

79 Papadopoulos, S. 2009. Revisiting the Public Disclosure of Private Facts in a Cyberworld. *Obiter.* Vol 1: 37. Section 36 of the Constitution states that the rights of the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based in human dignity, equality and freedom, taking into account relevant factors, including – (a) the nature of the right; (b) the importance and purpose of the limitation; (c) the nature and extent of the limitation; (d) the relation between the limitation and its purpose; (e) less restrictive means to achieve the purpose.

caution. The chapter to follow indicates what precautionary measures should be taken in the workplace and what is reasonably expected of the employee in the workplace.

CHAPTER 2: ELECTRONIC COMMUNIACTIONS POLICY IN THE WORKPLACE

2.1 INTRODUCTION

The computer has become the defining technological device of the last quarter of the twentieth century.[80] Enriching the globe not only with a high computer network, including the internet, but also has expanded astonishingly to include millions of businesses and individual users.[81] For many, a personal computer linked to the internet is primarily a communications device, and only secondarily a data processor.[82]

Many companies today have replaced telephonic communications with electronic conversation. Much employee communication now takes place over private or public networks, through e-mail.[83] Employees often assume that e-mail, like a telephone conversation, is private and protected from interception by an employer, however, this is not always the case.[84]

The introduction of computers into the workplace has significantly changed the way in which employers conduct their business.[85] The rapid deployment and infusion of e-communication technologies in the workplace have affected the way in which employees are to perform their duties.[86]

According to Pistorius, technology has not only enhanced productivity but it also has also provided for an instant, "now" means of socialisation and interaction.[87] Our physical world has become so infused with e-communications technologies – electronic communication paraphernalia, such as multi-function mobile devices, palm

---

80 Modiba, M. 2003. Intercepting and Monitoring employees' e-mail communications and internet access. South African Mercantile Law Journal, 15: 363.

81 *Ibid* 363-364.

82 *Ibid* 364.

83 Modiba, M. 2003. *SA Merc LJ*, 15: 364.

84 *Ibid* 363.

85 Pistorius, T. 2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review*, Vol 12: 2.

86 *Idem.*

87 *Idem.*

tops and electronic organisers, which have altered our modern communication patterns as well as our social behaviour.[88] E-communication facilities link the office with the home and vice versa, therefore the border between office and home have become inter-related as the office is now wherever a notebook and a hotspot may be found.[89] This seamless inter-connection of public and private space raises several difficult legal issues as far as the privacy of e-communications is concerned.[90]

As electronic communications and the use of social media expand exponentially, employers across the globe are trying to deal with the following questions:
Is the employer entitled to have unlimited access to its employees' personal e-mail messages? Do employees have reasonable expectations of privacy in respect of personal e-mails and communications?[91]

Most employees do not give a second thought to the fact that they use the workplace's computer facilities also for their own personal use.[92] Employees are further under the impression that their online private communications are afforded privacy.[93] The right to privacy in the context of the employment relationship is difficult to define or elucidate. As noted in the *Moonsamy* case:

> *'The rights that a citizen is entitled to in his or her personal life cannot simply disappear in his or her professional life as a result of the employer's business necessity. At the same time the employer's business necessity may impact on the employee's personal rights in a manner not possible outside the workplace. Therefore there is a clear balancing of interests'.*[94]

A further case that can be looked at in this instance is the case of *Daniel Phillip Neethling v South African Fruit Terminals (unreported case) CCMA Durban, Case No. KN-4881-04* where the CCMA had to deal with the question of an employer obtaining electronic information, marked personal, from the employee's work

88 *Idem.*

89 *Idem.*

90 *Idem.*

91 Modiba, M. 2003. *SA Merc LJ*, 15: 364.

92 Pistorius, T. 2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review.* Vol 12: 3.

93 *Idem.*

94 *Moonsamy v The Mailhouse* (1999) 20 *ILJ* 464 (CCMA) at 471G.

computer, in the absence of an ECP permitting the employer to do so. [95] The Commissioner, ruling in favour of the employee, held that "employees were entitled to use their computers for personal purposes" and that "the documents complained of were taken from correspondence clearly marked personal in his computer".[96] The respondent had no policy that entitled it to investigate the personal correspondence of the staff, and therefore, "the evidence the respondent obtained from invading the applicant's privacy must be disregarded".[97]

2.2 ELECTRONIC COMMUNICATIONS POLICY (ECP) IN THE WORKPLACE

Modiba explains that the scope of the right to privacy extends only to those aspects of life or conduct to which a legitimate expectation of privacy can be harboured.[98]

According to McGregor, the right to privacy, like all other rights, is not an absolute right, as it has to be balanced with other rights.[99]

In *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO,* the court held that '*when people are in their offices, in their cars or on their mobile phones, they still retain a right to be left alone by the state unless certain conditions are satisfied* '.[100]

Therefore, for the purposes of legal certainty, it is essential that an employer put in place an electronic communications policy which must be strictly monitored and consistently applied.[101] This would in turn then give the employee legal certainty as to what he is entitled to do with regards to his online activities, and would also avoid any infringements of the employee's right to privacy. Modiba suggests that the employer obtain prior written consent for the interception of communications within

95 *Phillip Neethling v South African Fruit Terminals (unreported case)* CCMA Durban, Case No. KN-4881-04.

96 Idem.

97 *Idem.*

98 Modiba, M. 2003. *SA Merc LJ*, 15: 366.

99 McGregor, M. 2004.*SA Merc LJ,* 16:639.

100 Papadopoulos (2012) 279.

101 Papadopoulos (2012) 279.

the workplace by insisting that the employee sign a document confirming such consent.[102]

As a starting point, McGregor explains, that in drafting a policy on the use of e-mail and the internet in the workplace, the purpose and scope of such a policy should be determined to meet the needs of the various departments of the employer's business.[103] This should be done in light of the employees' reasonable expectations and the subjective expectation of society to have the employees' privacy respected by the employer.[104]

To assist the employer with putting such a policy in place, the policy should also comply with Schedule 8 of the Labour Relations Act 66 of 1995 (LRA), which contains a *Code of Good Practice on Dismissal* wherein it states the factors that must be taken into consideration for the contravention of such a policy.[105] These include:

-The employee's awareness of the rule or practice;

-The reasonableness of such a rule or practice;

-The consistent application of the rule or practice.[106]

2.2.1 Employee's awareness of the policy

The LRA's Code of Good Practice places emphasis on the fact that such rules or practices must be made clear and unambiguous in order to avoid any uncertainty and inconsistency.[107] This has led to much accepted approach that a policy implemented in the workplace must either be expressly contained in an employment contract or incorporated into it by reference.[108] A failure to include an Electronic Communications Policy (ECP) has, however, not been a bar to dismissal in all Commission for Conciliation Mediation and Arbitration (CCMA) cases.[109]

---

102 Modiba, M. 2003. *SA Merc LJ*, 15 : 366

103 McGregor, M. 2004. *SA Merc LJ,* 16:647.

104 *Idem*.

105 Papadopoulos (2012) 280.

106 Schedule 8 of the Labour Relations Act 66 of 1995.

107 *Idem.*

108 Papadopoulos (2012) 280.

109 *Idem.*

2.2.2 The reasonableness of such policy

The question of the employee's right to privacy in the workplace will inevitably be raised in order to determine whether such a rule in an ECP is reasonable or not.[110] In *Protea Technology v Wainer,* the court made the observation that *'[t]he scope of a person's privacy only extends to those issues where the person has a legitimate expectation of privacy […] an employee can make and receive calls that are private as long as they have nothing to do with the employer's business […] but where it concerns the employer's affairs the employer is entitled and may demand a full account'.*[111] This rule would obviously also apply to e-mail and internet use.[112]

Where an ECP is in place at the workplace and an employee has signed such a policy in his or her employment contract, then he or she does not have the right to claim privacy for work-related activities,[113] as they have been made aware of such a policy and have consented to it.

2.2.3 The consistent application of a rule or practice

It is important for employers to be aware that despite the existence of an ECP, it is vital that the ECP be enforced and applied on a consistent basis for it to be effective.[114]

2.3 CONCLUSION

Viewed from the Employer's perspective, it may be argued that privacy is not an absolute right.[115] As discussed above, employees' right to privacy should be balanced with the employer's business necessities or operational requirements.[116] It

110 *Ibid 281.*

111 Papadopoulos (2012) 281.

112 *Idem.*

113 Papadopoulos (2012) 281.

114 *Ibid 282.*

115 Pistorius, T.2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review*. Vol 12: 4.

116 *Idem.*

should, however, be kept in mind that the employer provides and owns the computer facilities the employee uses.[117]

It is in this context that Le Roux[118] notes:

> *'The employer is also permitted to set more general standards relating to conduct in the workplace and to the use of equipment and tools. The Employer can, for example, prescribe when personal computers may be used, for what purposes they may be used, and how they may be used. The same applies to access to the internet. If an employee fails to comply with these rules it will, in principle, be open to the employer to discipline an employee for such a failure. In the correct circumstances this may also justify the disciplinary sanction of dismissal'.*[119]

The Labour Relations Act[120] and Code of Good Practice[121] place an obligation on the employer to adopt rules or codes of conduct for the workplace that will create certainty as well as consistency.[122] This will also help the employee to understand his or her rights in the workplace with regards to online social networking during working hours. The employee must, as seen from the above chapters, take caution in what is said on social networks. He/she must make sure that their privacy settings are set as well as take care as to what is said, as not everything will be protected by legislation. This will be discussed in the following chapters.

---

117 *Idem.*

118 Le Roux PAK 'Employment Practices in the Age of the Internet' (Unpublished paper delivered at the E-commerce and Current Commercial Law Workshop on 29 August 2003 at Sandton Johannesburg).

119 Pistorius, T. 2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review*. Vol 12: 4.

120 Act 66 of 1995.

121 Schedule 8 of Act 66 of 1995.

122 Pistorius, T. 2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review*. Vol 12: 4.

CHAPTER 3: LEGISLATION ON INTERCEPTION AND MONITORING

3.1 INTRODUCTION

The question arises as to what extent an employer may monitor whether or not employees are using electronic communication technologies responsibly.[123] Several pieces of legislation will be discussed in this chapter and their effects on employees' right to online privacy in the workplace.

3.2 INTERCEPTION AND MONITORING IN THE WORKPLACE

South African Labour Law plays an important role with regards to what rights the employers have over their employees and their social media content, for example the employee's Facebook profile. The type of information typically contained in a profile includes the user's photo along with the user's name, country, gender, sexual orientation, marital status and date of birth.[124] The profile often includes a list of friends, a list of groups to which the user is affiliated, blogs, news bulletins, interests, personal photos, favourite music and videos,[125] in fact , according to Abril, these profiles constitute the user's digital identity in cyberspace.[126]

The question arises to what extent an employer may monitor whether or not employees are using electronic communication technologies responsibly.[127] The answer lies within the interpretation of the *Regulation of Interception of Communications and Provision of Communication-Related Information Act* 70 of 2002.[128]

---

123 Pistorius, T. 2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review*. Vol 12: 5.

124 Papadopoulos, S. 2009. Revisiting the Public Disclosure of Private Facts in a Cyberworld. *Obiter.* Vol 1: 32.

125 *Idem.*

126 Abril 2007 *Harvard Journal of Law and Technology* 14.

127 Pistorius, T. 2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review*. Vol 12: 5.

128 Pistorius, T. 2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review*. Vol 12: 5.

3.3 THE REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT 70 OF 2002 (RICA)

RICA is wider than that of the previous IMP Act (Interception and Monitoring Prohibition Act), as the Act is also applicable to the private sphere such as the workplace.[129] It prohibits the intentional interception or authorisation of an interception of any communication in the course of its occurrence or transmission.[130]

Section 2 of RICA states that:

> *'[n]o person shall-*
> *Intentionally intercept or attempt to intercept or authorise, or procure any other person to intercept or to attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission.'*[131]

This according to Cohen[132] means in simple terms that it is unlawful and therefore prohibited to:

a) Intentionally and without the knowledge or permission of the dispatcher to intercept a communication which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications line; or
b) Intentionally monitor any conversations or communications by means of a monitoring device so as to gather confidential information concerning any person, body or organisation.[133]

One must note that the attempt is as unlawful as the actual act of actually intercepting and monitoring a data communication.[134]

---

129 *Ibid* at 6.

130 *Idem.*

131 Papadopoulos (2012) 282.

132 Cohen, T. 2001. But for the necessity of knocking and requesting right of entry. *Surveillance Law & Privacy Rights in South Africa,* 1: 2-4.

133 Cohen, T. 2001. But for the necessity of knocking and requesting right of entry. *Surveillance Law & Privacy Rights in South Africa,* 1: 2-4.

134 Papadopoulos (2012) 282.

The term "communication" is defined to include both 'direct' and "indirect" communication.[135] The term "indirect communication" is of greater importance and the definition can be found in section 1 which reads as follows:

'… the transfer of information, including a message or any part of a message, whether –

(a) In the form of –

(i) speech, music or other sounds; data, text, visual images, whether animated or not; signals; or radio frequency spectrum; or

(b) In any other form or in any combination of forms; that is transmitted in whole or in part by means of a postal service or a telecommunication system.'

Indirect communication includes telephone calls (land line and cellular); intranet, internet, facsimile facilities, private and personal e-mail messages, the downloading of information from an internet site or sending or receiving of an e-mail message, or the message itself.[136]

The definition of "intercept" is found in section 1. It reads as follows:

> *'the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient of that communication, and includes the (a) monitoring of any such communication by means of a monitoring device; (b) viewing, examination or inspection of the contents of any indirect communication; and (c) diversion of any indirect communication from its intended destination to any documentation.'*[137]

The meaning of intercept is important.[138] According to Dekker it includes the acquisition of the contents of any communication through the monitoring of a

---

135 Pistorius, T. 2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review*. Vol 12: 6.

136 *Ibid* at 7.

137 Pistorius, T. 2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review*. Vol 12: 7.

138 Pistorius, T. 2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review*. Vol 12: 8.

communication, the viewing of the contents and the diversion of an indirect communication from its intended destination.[139]

No person may intentionally intercept an e-mail message in occurrence or transmission by using interception or monitoring devices.[140] All activity that monitors the traffic on a telecommunication system is covered by section 2 of RICA. [141] The meaning of monitoring is to record communications, including the mere fact that a communication was sent or a site visited.[142] Indirect communications further include a message or a part of a message in the form of data, text, visual images in the subject line, text or symbols in filling in recipient's address and any other form or combination of forms.[143]

3.3.1 Interception and monitoring by consent

Sections 3 to 11 of RICA set out the circumstances where there will be no contravention of section 2.[144] Section 4(1) provides for consensual monitoring and states that any person, other than a law enforcement officer, may intercept a communication if that person is a party to that communication.[145] Section 5(1) of RICA states that any person may authorise or give anyone else "written" permission to monitor or intercept any data communication unless it is for the purposes of unlawful conduct.[146] Another important factor to note in the interpretation of section 5(1) is that this consent to monitoring may be given by one of the parties to the communication.[147]

---

139 Dekker, A. 2004. *SA Merc LJ*, 16: 622-637.

140 Pistorius, T. 2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review*. Vol 12: 8.

141 *Idem.*

142 *Idem.*

143 *Idem.*

144 Pistorius, T. 2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review*. Vol 12: 9.

145 *Idem.*

146 Papadopoulos (2012) *282.*

147 Pistorius, T. 2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review*. Vol 12: 10.

Modiba suggests that if the employer wants prior written consent to intercept and monitor communication devices at the workplace he should insist that the employee sign such a documentation confirming such consent.[148] Alternatively, an employer could also inform the employee by means of a pop-up screen that the employee should agree to the terms and conditions of the employer's ECP.[149] This will either be in the pop-up notice or in a link where the policy can be accessed.[150] Pistorius is of the opinion that electronic consent could also be obtained from an employee through express written electronic consent. [151]

3.3.2 Interception and monitoring of indirect communications at the workplace

Despite the fact that Section 5 authorises the data interception of employees and "direct and indirect communication" by consent of the parties engaged in the data communication, Section 2 is also subject to certain exceptions that are contained in Section 6 of RICA where it states that:[152]

1) 'Any person may, in the course of the carrying on of any business, intercept any indirect communication –

a) by means of which a transaction is entered into in the course of that business;

b) which otherwise relates to that business; or

c) which otherwise takes places in the course of the carrying on of that business, in the course of its transmission over a telecommunication system.'

Section 6(2) of RICA then sets certain requirements that must be met before there is interception of indirect communications in terms of Section 6(1) will be permitted. Section 6(2) reads as follows:

'A person may only intercept an indirect communication in terms of subsection (1):

a) if such interception is effected by, or with the express or implied permission of the system controller,

148 Modiba, M. 2003. *SA Merc LJ*, 15: 366.

149 Papadopoulos (2012) 282.

150 Papadopoulos (2012) 282-283.

151 Pistorius, T. 2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review*. Vol 12: 10.

152 Papadopoulos (2012) 283.

b) for the purposes of-

i) Monitoring or keeping record of indirect communications-

(aa) in order to establish the existence of facts,

(bb) for purposes of investigating or detecting the unauthorised use of the telecommunications system, or

(cc) where that is undertaken in order to secure, or as an inherent part of the effective operation of the system.

ii) Monitoring indirect communications made to confidential telephony counselling or support service which is free of charge, other than that the cost, if any, of making a telephone call, and operated in such a way that users thereof may remain anonymous if they choose to.'

Section 6(2)(c) and (d) add further requirements in that such interception must take place either partly or wholly on the telecommunication system of that business and that the person who is being intercepted must have either freely consented by his own will or tacitly by his actions.[153] To satisfy such provisions, the employer must therefore inform the employees in the ECP that the employer may read the employee's communications and it should also describe the circumstances under which it will do so[154], giving the employee knowledge of what he or she is consenting to.

According to Pistorius Section 6 is a tremendously intricate provision, this is because at first blush, it seems that the protection which is so offered by section 6 would apply only to clients of a business.[155] Pistorius goes further to state that one may also argue that any private communication by employees would not fall within the ambit of section 6(1) in that these indirect communications, in the course of being transmitted, would not facilitate the entering into a transaction in the course of business, it would not otherwise relate to the business, or would not otherwise take place in the course of the carrying on of that business.[156]

---

153 Papadopoulos (2012) 283.

154 *Idem.*

155 Pistorius, T. 2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review*. Vol 12: 11.

156 Pistorius, T. 2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review*. Vol 12: 11.

3.4 THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002 (ECT ACT)

It is believed that the Electronic Communications and Transactions Act 25 of 2002 was enacted to remove barriers that previously hampered the validity of electronic consent.[157]

3.4.1 The requirement of a written notice of intended interception and monitoring

The requirement of a written consent or the giving of a written consent may also be communicated electronically.[158] Section 12 of the ECT Act provides for the following: *'A requirement in law that a document or information must be in writing is met if the document or information is:*

a) In the form of a data message; and

b) *Accessible in a manner usable for subsequent reference.'*[159]

This section is intended to define the basic standard to be met by a data message in order to satisfy a requirement that information be retained or presented "in writing" or that it be contained in a "document' or other paper-based instrument. [160]

The information in a data message must be accessible so as to be usable for subsequent reference.[161] Here, according to Pistorius, "usable" includes human and/or computer use and "accessible" is meant to imply that information in the form of computer data should be readable and interpretable, and that the software that might be necessary to render such information readable should be retained.[162]

---

157 *Ibid* 14.

158 Pistorius, T. 2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review*. Vol 12: 17.

159 *Idem.*

160 Pistorius, T. 2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review*. Vol 12: 17.

161 *Idem.*

162 *Idem.*

Section 12 makes reference to the phrase "in law".[163] The precise ambit of this "law" and its scope of application create uncertainty.[164] Following the UNICITRAL Model Law,[165] such a term is likely to be interpreted to refer not only to statutory, regulatory and common law, but also to judicial precedent, procedural and subordinate law.[166]

3.4.2 Electronic expression of consent in terms of interception and monitoring

Section 24 of the ECT Act states:

'As between the originator and the addressee of a data message an expression of intent or other statement is not without legal force and effect merely on the grounds that-

a) *It is in the form of a data message ; or*
b) *It is not evidenced by an electronic signature but by other means from which such person's intent or other statement can be inferred.'*

Section 22 of the ECT Act provides for the general rule that contracts can be concluded in an electronic form.[167] Section 24, unlike with section 22, does not impose the use of electronic means of communication but validates such use.[168]
Unauthorised access to data and interception or interference with data is covered in chapter XIII offences, and in particular Section86 (1)[169] prohibits a person from intentionally accessing or intercepting any data without the authority or necessary consent to do so.[170]

---

163 *Idem.*

164 *Idem.*

165 See UNCITRAL Model Law on Electronic Commerce 1996 with additional art 5*bis* as adopted in 1998; see also Hill, R and Walden, I. 1996. The draft UNCITRAL Model Law for Electronic Commerce: Issues and Solutions .*The Computer Lawyer* March. www.batnet.com/oikoumene/tacr.html

166 Meiring, R *"Electronic Transactions"* in Buys, R and Cronje, F. (Eds). 2004. *Cyberlaw@SA II: the law of the internet in South Africa.* 2nd ed. Pretoria: Van Schaik.

167 Pistorius, T. *Monitoring, interception and big boss in the workplace: Is the devil in the details?* In Potchefstroom Electronic Law Review, (2009). Vol 12, 18.

168 *Idem.*

169 The Electronic Communications and Transactions Act 25 of 2002.

170 Papadopoulos (2012) 299.

3.4.3 Interplay between the ECT Act and the Regulation of Interception Act

The requirement of prior written consent in terms of section 5(1) of RICA will not pose any problem.[171] In terms of sections 12, section 13(5) and section 24(2) of the ECT Act, written consent may also be given in electronic form.[172] According to Pistorius, the requirement of "prior consent' will be met with ease if the giving of such consent is conditional for obtaining access to the work station or telecommunication equipment.[173]

3.4.4 Reasonable steps to inform

There must be compliance with the requirements of section 6(2) of RICA, namely, that the systems controller has made all reasonable efforts in order to inform all persons, in advance, who intend to use the telecommunications and electronic systems concerned of the fact that interceptions may take place, this will also be facilitated by the ECT Act.[174]

The ECT Act facilitates this process by affording the employer the opportunity to incorporate their e-mail or internet policy[175] on the welcoming page when employees log on. This notice may be displayed every time an employee logs on to the employer's computer facilities.[176]

3.5 LABOUR RELATIONS ACT

South African Labour legislation plays an important role with regards to an employee's right to privacy in the workplace. The Labour Relations Act 66 of 1995 protects job applicants as well as employees to claim that instruction to divulge

---

171 Pistorius, T. 2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review.* Vol 12: 20.

172 *Idem.*

173 *Idem.*

174 Pistorius, T. 2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review*. Vol 12: 20.

175 McGregor, M. 2004. *SA Merc LJ,* 16:647.

176 Pistorius, T.2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review*. Vol 12: 20.

private information does not have a bearing on the employment relationship and is not a lawful instruction.[177] Employees may not be unfairly discriminated against based on their personal lives and what is displayed on their social networks.

The LRA must be read together with Schedule 8 of the *Code of Good Practice* in order to determine whether an employee has been unfairly dismissed.
The LRA's *Code of Good Practice* states the following:

1) *'This code of good practice deals with some of the key aspects of dismissals for reasons related to conduct and capacity. It is intentionally general. Each case is unique, and departures from the norms established by this Code may be justified in proper circumstances.*
2) *[…]*
3) *The key principle in this Code is that employers and employees should treat one another with mutual respect. A premium is placed on both employment justice and the efficient operation of business. While employees should be protected from arbitrary action, employers are entitled to satisfactory conduct and work performance from their employees.'*[178]

With regards to fair reasons for dismissal, one can refer to the *Code of Good Practice* in the LRA. Which reads as follows:

1) *'A dismissal is unfair if it is not effected for a fair reason and in accordance with a fair procedure, even if it complies with any notice period in a contract of employment or in legislation governing employment. Whether or not a dismissal is for a fair reason is determined by the facts of the case, and the appropriateness of dismissal as a penalty. Whether or not the procedure is fair is determined by referring to the guidelines set out below.*
2) *This Act recognises three grounds on which a termination of employment might be legitimate. These are: the conduct of the employee, the capacity of the employee, and the operational requirements of the employer's business.*

---

177 SA Labour Law protects Facebook passwords. *http://www.itweb.co.za/index.php?option=com_content&view=article&id=54212:sa-labour-law-protects-facebook-passwords* (accessed 29th May 2014)

178 Schedule 8 of the Labour Relations Act 66 of 1995.

3) *This Act provides that dismissal is automatically unfair if the reason for the dismissal is one that amounts to an infringement of the fundamental rights of employees and trade unions, or if the reason is one of those listed in section 187.'*[179]

Employers in South Africa may not unfairly discriminate against employees on a number of grounds as listed in section 6 of the Employment Equity Act 55 of 1998.[180] Section 6 reads as follows:

1) '*No person may unfairly discriminate, directly or indirectly, against any employee, in any employment policy or practice, on one or more grounds, including race, gender, sex, pregnancy, marital status, family responsibility, ethnic or social origin, colour, sexual orientation, age, disability, religion, HIV status, conscience, belief, political opinion, culture, language and birth.*'

3.6 THE CONSTITUTION OF THE REPUBLIC OF SOUTH AFRICA 108 0F 1996

In South African law the right to privacy is protected in terms of both the Constitution[181] and our common law.[182] Under the South African common law a person can rely on the law of delict for the protection of his or her right to privacy.[183]

The Constitution guarantees a general right to privacy, with specific protection against searches and seizures, and the privacy of communications.[184] This list, however, is not exhaustive.

The instances of privacy listed in section 14 relate to the "informational" aspects of the right to privacy.[185] The informational right to privacy has been interpreted by the

179 *Idem.*

180 *Idem.*

181 S14 of The Constitution.

182 Papadopoulos, S. 2009. Revisiting the Public Disclosure of Private Facts in a Cyberworld. *Obiter,* vol 1: 34.

183 *Idem.*

184 Roos (2003) (LLD Thesis UNISA).

185 Van der Merwe, D., Roos, A., Pistorius, T. & Eiselen, S. 2008. *Information and Communications Technology Law:* Lexis Nexis 353.
The courts have, however, also extended the constitutional right to privacy to "substantive" privacy rights. These are rights which enable persons to make decisions about their family, home and sex life.

Constitutional Court as coming into play whenever a person has the ability to decide what he or she wishes to disclose to the public.[186] A person has a strong expectation of privacy in relation to his or her home, family life and intimate relationships, however, where communal relationships and activities such a business and social interactions are concerned, his or her expectation of privacy is then diminished.[187]

Section 14(d) guarantees the right to privacy as a fundamental right not to have the privacy of one's communications infringed.[188] According to Modiba, one should question whether the constitutional right to privacy guarantees absolute privacy to an employee in the workplace, so that an employer cannot, under any circumstances, read the contents of private personal e-mail communications sent or received by an employee.[189]

It is clear that where an employer monitors information about e-mail and other forms of Internet access that would not necessarily be a breach of privacy.[190] The integrity of the message is maintained and the substantive communication taking place is unaffected by the monitoring taking place by the employer.[191] However, intercepting and reading the contents of the messages or internet usage should be done with care and discretion.[192] The employer should respect the rights of his or her employees in respect of contents of e-mail messages and other forms of Internet communications unless there is sound reason for the employer to suspect that some abuse is taking place, or where issues, concerns, grievances, or disciplinary matters have already arisen.[193]

Section 16 states that -

1) 'Everyone has the right to freedom of expression, which includes-

---

186 *Idem.* See *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others: In re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* 2001 (1) SA 545 (CC) 557. The court added that the expectation that such a decision will be respected must be reasonable.

187 *Idem.* According to the Constitutional Court, the protection of privacy lies in continuum (*Bernstein v Bester NO* 1996 (2) SA 751 (CC) 788).

188 Modiba, M. 2003. *SA Merc LJ*, 15: 365.

189 *Idem*.

190 *Idem*.

191 *Idem.*

192 Carl Mischke. 1999 9(5). *Disciplinary Action and the Internet. Contemporary Labour Law* .48.

193 *Idem*.

a) *Freedom of the press and other social media;*
b) *Freedom to receive or impart information or ideas;*
c) *Freedom of artistic creativity; and*
d) *Academic freedom and freedom of scientific research.'*

Therefore the Constitution provides for the protection of one's dignity as well as one's privacy in respect of their personal lives. This is not to say that an employee is completely protected by the Constitution should the employee himself or herself do something to bring the employer's business or name into disrepute. One has the freedom to express themselves but within reasonable expectations within their working environment.

3.7 THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 (PPI ACT)

This legislation aims to ensure that the processing of personal information of individuals take place according to internationally accepted data protection principles and that there is adequate enforcement to ensure compliance.[194] According to the PPI it requires the employer to obtain the employee's consent before collecting stored information.[195]

The purpose of this Act is to:

'a) give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at-

(i) balancing the right to privacy against other rights, particularly the right of access to information; and

(ii) protecting important interests, including the free flow of information within the Republic and across international borders.'[196]

According Sections 7-24 of the PPI Act, personal information may only be processed where the data subject has given consent; where it is necessary for the performance

194 Papadopoulos (2012) 299.

195 Section 23 of the Protection of Personal Information Act 4 of 2013.

196 Section 2 of the Protection of Personal Information Act 4 of 2013.

of a contract or agreement to which the data subject is party, or for actions to be carried out at the request of the data subject; where it is necessary in order to comply with a legal obligation; where processing is necessary for the proper performance of public law duties; or where it is necessary for upholding the legitimate interests of the responsible party or of a third party to whom the information is supplied.[197] The processing then has to take place in accordance with eight information protection principles contained in Chapter III of the PPI Act.[198]

Chapter III of the PPI Act requires adherence to the principles of:
-Accountability
-Processing limitation
-Purpose specification
-Further processing limitation
-Information quality
-Openness
-Security safeguards[199]
-Data subject participation

These principles are drawn from the OECD guidelines and the EU Data Protection Directive 95/46/EC, but have been adapted to conform to local conditions.[200]

Section 26 of the PPI states that-
'A responsible party may, subject to section 27, not process personal information concerning:
a) the religious or philosophical belief, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject.'

197 Papadopoulos (2012) 301.
198 *Idem.*
199 *Idem.*
200 *Idem.*

According to section 25 of the PPI with regards to the manner of access, this section must be read together with section18 and section 53 of the Promotion of Access to Information Act 2 of 2000.

Section 18 reads as follows-

1) '*A request for access must be made in the prescribed form to the information officer of the public body concerned at his or her address or fax number or electronic mail.*
2) *The form for a request of access prescribed for the purposes of subsection (1) must at least require the requester concerned-*

a) *to provide sufficient particulars to enable an official of the public body concerned to identify-*
   i) *the record or records requested; and*
   ii) *the requester;*
b) *to indicate which applicable form of access referred to in section 29(2) is required;*
c) *to state whether the record concerned is preferred in a particular language;*
d) *to specify a postal address or fax number of the requester in the Republic;*
e) *if, in addition to a written reply, the requester wishes to be informed of the decision on the request in any other manner, to state that manner and the necessary particulars to be so informed; and*
f) *if the request is made on behalf of a person, to submit proof of the capacity in which the requester is making the request, to the reasonable satisfaction of the information officer…*'[201]

Section 53 of the Promotion of Access to Information Act reads the same as the above section.

Both these sections are to be read in conjunction with section 25 of the PPI Act with regards to the manner of access to such information.

[201] The Promotion of Access to Information Act 2 of 2000.

3.7.1 Enforcement, offences and penalties

The PPI Act also provides for civil remedies against a responsible party.[202] According to Section 99 of the PPI Act the data subject, or at the request of the data subject, the Regulator, may institute a civil action for damages in a court having jurisdiction against a responsible party[203] for breach of any provision of the Act.

3.8 CONCLUSION

As can be seen from the above, South African legislation provides protection to employees in the workplace and does indeed protect their privacy to an extent.

It is therefore clear that from Section 6 of RICA, the interception of data messages will only be justifiable in certain specific instances that mostly relate to business and that any deviation from the general rule prohibiting interception would be a violation of privacy attracting criminal as well as civil sanctions in terms of Section 86(1), (2) and (3) of the ECT Act and would result in a fine or imprisonment of up to 12 months.[204] RICA's requirements of written consent, taking reasonable steps to inform and obtaining express or implied consent may all be met with ease.[205] The ECT Act's provisions enable employers to integrate such requirements with that of workstation use.[206]

---

202 Papadopoulos (2012) 308.

203 Section 1 "responsible party" means a public or private body or any other person which, alone or in conjunction with others, determines the purpose and means for processing personal information.

204 Papadopoulos (2012) 283.

205 Pistorius, T. 2009. Monitoring, interception and big boss in the workplace: Is the devil in the details? *Potchefstroom Electronic Law Review.* Vol 12: 21.

206 *Idem.*

CHAPTER 4: RELEVANT CASE LAW

4.1 INTRODUCTION

It can be seen in South African law that there is a link between space, secrecy, seclusion, subject matter and privacy which is clearly demonstrated in various decisions of our Constitutional Court.[207]

As seen above in *Bernstein v Bester*[208], the court held that "Privacy is acknowledged in the truly personal realm, but as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks". In *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd : In Re: Hyundai Motor Distributors (Pty) Ltd v Smit NO*[209], *Langa DP held that* " Thus, when people are in their offices, in their cars or on mobile telephones, they still retain the right to be left alone by the State unless certain conditions are satisfied."[210]

These decisions clearly place the right to privacy as lying along a continuum in which the more a person interacts with the world, the more the right to privacy becomes diluted.[211]

4.2 RELEVANT CASE LAW:

The case law referred to below both discuss the unfair dismissal of an employee as a result of intercepting and monitoring the employee's personal communication devices, without the necessary consent required from the employee. The case law is relevant to the above discussion in that both cases make reference to legislation and relevant authorities that provide the necessary legal framework for the protection of

---

207 Papadopoulos, S. 2009. Revisiting the Public Disclosure of Private Facts in a Cyberworld. *Obiter*. Vol 1: 37.

208 *Bernstein v Bester* 1996 2 SA 751 (CC) 789.

209 *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd; In Re: Hyundai Motor Distributors (Pty) Ltd v Smit NO* 2001 1 SA 545 (CC) 557.

210 Papadopoulos, S. 2009. Revisiting the Public Disclosure of Private Facts in a Cyberworld. *Obiter*. Vol 1: 37.

211 Papadopoulos, S. 2009. Revisiting the Public Disclosure of Private Facts in a Cyberworld. *Obiter*. Vol 1: 34.

employees' online privacy, however, this is done within reason. The following case law will now be discussed:

4.2.1 *MOONSAMY V THE MAILHOUSE (1999) 20 ILJ 464 (CCMA)*

The right to privacy in the workplace was interpreted and applied in an extensive amount of detail[212] in this following case, which will now be discussed. The arbitrator held that the issue was one of balancing the competing interests of the employer and the employee.[213]

The facts of the case are as follows:

The employee alleged that he was the victim of an unfair dismissal.[214] The question was whether the employer was entitled to use evidence which it obtained by way of an interception, listening and recording device (a 'tap' or 'bug') that was connected to the employee's telephone in his office at the premises of the employer.[215] This evidence was led at the employee's disciplinary hearing, and relying on that and other evidence, the chairperson of that hearing decided that the dismissal of the employee was the appropriate sanction.[216] The employee approached the CCMA for relief, and argued that the telephonic evidence was obtained illegally and in contravention of the Constitution.[217]

The arbitrator structured his reasoning on five premises based on the factors set out in section 36 of the Constitution to be considered when fundamental rights are limited.[218]

The first concerned the actual nature of the right.[219] It was held to be 'extremely difficult to clarify, at least with any degree of precision, the nature of the right to

212 McGregor, M. 2004. *SA Merc LJ,* 16:641

213 *Idem.*

214 *Moonsamy v The Mailhouse (1999) 20 ILJ 464 (CCMA) at 466G-H.*

215 *Idem.*

216 *Idem.*

217 *Idem.*

218 McGregor, M. 2004. *SA Merc LJ,* 16:641.

privacy of an employee on the premises of the employer during working hours'.[220] The arbitrator relied on the American case law (*Katz v US 389 US 347 1967)* to the effect that a person is entitled to a 'reasonable expectation' of privacy.[221] This reasonable expectation could only exist when the individual had a subjective expectation of privacy and secondly, that society must recognise the expectation as reasonable.[222] Within the context of the employment relationship, the second requirement is largely determined by the 'operational realities of the workplace'.[223] In another American case (*O'Connor v Ortega 480 US 709 1987*), the same court found that the operational realities of the workplace may make some employee expectations of privacy unreasonable, which might be found to be reasonable in other non-employment contexts.[224] Office practices and procedures, and legitimate employer regulations, might reduce the employees' expectations of privacy in their offices, desks, and filing cabinets.[225] Given the great variety of work environments, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis.[226]

The commissioner in Moonsamy noted that the present case went further than rummaging in an employee's desk or filing cabinet.[227] This was a telephone interception with the express purpose of monitoring all of the employee's conversations.[228] Whilst it may be argued that the telephone conversation took place on the employer's telephone, on the employer's premises, and was related to the employer's business, telephone conversations by their nature demand a higher degree of privacy than the employer's office or desk.[229] It may be argued that if a telephone call was related to the employer's business, the employer was entitled to be privy to that conversation.[230] However, if the employer was allowed to make that

---

219 McGregor, M. 2004. *SA Merc LJ,* 16:641.

220 *Moonsamy v The Mailhouse (1999) 20 ILJ 464 (CCMA) at 469I.*

221 McGregor, M. 2004. *SA Merc LJ,* 16:641.

222 *Moonsamy v The Mailhouse (1999) 20 ILJ 464 (CCMA) at 469J-470.*

223 *Idem.*

224 *Moonsamy v The Mailhouse (1999) 20 ILJ 464 (CCMA) at 469J-470A.*

225 *Ibid* at 470A.

226 *Ibid* at 470A-B.

227 McGregor, M. 2004. *SA Merc LJ,* 16:641.

228 *Moonsamy v The Mailhouse (1999) 20 ILJ 464 (CCMA) at 470B.*

229 *Moonsamy v The Mailhouse (1999) 20 ILJ 464 (CCMA) at 470B-C.*

230 *Ibid* at 470C.

initial decision regarding the nature of the call (personal versus business), the right to privacy would then serve to be meaningless.[231] The right would then amount to having a tribunal decide, after the interception of the call, the call did not in actual fact relate to the business of the employer and was therefore confidential.[232]

The second point related to the importance of the purpose of the limitation.[233] The employer argued that the right to privacy was a qualified one and that the employer had a contractual right to know the content of the employee's calls insofar as they related to its business.[234] The employer considered its actions necessary for its financial self-preservation as the employee was conducting business that was damaging to the employer.[235]

It was explained that the employee's right to privacy regarding the work-related matters had to be qualified on the basis of the fiduciary relationship between employee and employer that entitled the employer to loyalty and honesty.[236] The employer argued that it considered its actions necessary for its financial self-preservation, as the employee conducted business that was damaging to the employer, but the court held that a person's work or occupation was pivotal to his life, personal and professional.[237] The rights to which a citizen is entitled to in his personal life could not just disappear in his professional life as a result of his employer's business necessity.[238]

The third point related to the nature and extent of the limitation.[239] Telephone conversations are by their nature a very private affair and therefore the interception of these is a serious infringement of the right to privacy, even in the workplace.[240] An employer might have the right to ask an employee to disclose the number of

231 *Ibid* at 470D.

232 *Idem.*

233 McGregor, M. 2004. *SA Merc LJ,* 16:642.

234 *Moonsamy v The Mailhouse (1999) 20 ILJ 464 (CCMA) at 470I.*

235 *Idem.*

236 *Moonsamy v The Mailhouse (1999) 20 ILJ 464 (CCMA) at 470 I-J.*

237 McGregor, M. 2004. *SA Merc LJ,* 16:642.

238 *Idem.*

239 *Idem.*

240 *Moonsamy v The Mailhouse (1999) 20 ILJ 464 (CCMA) at 471J-472A.*

personal as opposed to business calls he or she makes during working hours, but the right to disclosure ends there, unless the employer can show, when seeking prior authorisation, that there are compelling reasons within the context of business necessity, that the content of those conversations are disclosed.[241]

The fourth point related to the limitation and its purpose.[242] The interception of the employee's telephone conversations was intended to provide evidence against him.[243] This was certainly not the only method in which to accumulate evidence of wrongdoing against the employee, and also meant that in the process of gathering evidence, the employer was privy to the content of all the employee's telephone conversations, which is a serious invasion indeed.[244] In addition, there were clearly other methods of obtaining evidence, and the fact that the employer has evidence other than the transcripts of the telephone conversations is proof of this.[245] If the employer could show that the telephone interception was the only method available of securing evidence against the employee, in circumstances where the employee was clearly causing harm to the employer, then perhaps the use of telephone tapping could be justified.[246]

The fifth and final point was that less restrictive means had to be used to achieve the purpose.[247] If an employer actually could have used other more conventional methods of obtaining incriminating evidence against an employee, it should have been done so.[248] If there were none, the employer had to seek prior authorisation to tap the telephone.[249] Prior consent could be obtained by way of employee consent as a condition of the employment contract, or by authorisation by the Labour Court.[250]

---

241 *Idem.*

242 McGregor, M. 2004. *SA Merc LJ,* 16:642.

243 *Moonsamy v The Mailhouse (1999) 20 ILJ 464 (CCMA) at 472B.*

244 *Ibid* at 472B-C.

245 *Ibid* at 472C.

246 *Moonsamy v The Mailhouse (1999) 20 ILJ 464 (CCMA) at 472D.*

247 McGregor, M. 2004. *SA Merc LJ,* 16:642.

248 *Idem.*

249 McGregor, M. 2004. *SA Merc LJ,* 16:643.

250 Section 158 of the Labour Relations Act 66 of 1995.

The commissioner found that the employer's actions in intercepting the employee's telephone calls, without prior authorization or the consent of the employee, contravened section 14(d), read with section 36 of the Constitution. Therefore the evidence that was obtained by the employer as a result of the interception of the employee's telephone conversations were inadmissible.[251]

4.2.2 *SMITH and PARTNERS IN SEXUAL HEALTH (NON – PROFIT)*[252]

The applicant, Smith, was employed by the respondent non-profit organization as an administration assistant.[253] The respondent operated an Internet-based e-mail account (Gmail) which was used to communicate with donors, sponsors and users, it was the applicant's duty to check the Gmail account regularly and to forward the e-mails to the other users.[254] Smith also had her own Gmail account.[255] While Smith was on leave the respondent's manager, De Lora (respondent's CEO), used the office computer to log onto the respondent's Gmail account and found that she had access to e-mails between Smith and former employees and others outside the organization relating to confidential information about internal matters, De Lora then proceeded to print out several of them and logged out.[256] De Lora testified that she was looking for a document that was stored on the computer at Smith's workstation.[257] De Lora printed a number of the e-mails and exited the account.[258] When she later re-accessed Gmail and attempted without success to find the same e-mails again she realized that she was now looking at respondent's Gmail account and further, that what she had been looking at earlier was Smith's private Gmail account.[259]

In an e-mail from Smith to one Mr T, a former employee of the respondent, on 16 July 2010, Smith complained that De Lora was planning to incorporate weekend

---

251 *Moonsamy v The Mailhouse (1999) 20 ILJ 464 (CCMA) at 474C-D.*

252 *Smith and Partners in Sexual Health (non-profit), (2011) 32 ILJ 1470 (CCMA)*

253 *Smith and Partners in Sexual Health (non-profit), (2011) 32 ILJ 1470 (CCMA) at 1470F.*

254 *Smith and Partners in Sexual Health (non-profit), (2011) 32 ILJ 1470 (CCMA) at 1470F.*

255 *Smith and Partners in Sexual Health (non-profit), (2011) 32 ILJ 1470 (CCMA) at 1470F.*

256 *Smith and Partners in Sexual Health (non-profit), (2011) 32 ILJ 1470 (CCMA) at 1470G.*

257 *Ibid at 1473, par 13E.*

258 *Ibid at 1473, par 13F.*

259 *Ibid at 1473, par 13F-G.*

attendance at board meetings into her job description in order to render it part of normal working hours and thus it would no longer attract overtime. [260] Smith stated that she was 'so upset'.[261] In the same strand of e-mails, Smith shares with Mr T: 'Just so upset pay is not changing she only looks after her buddies, can't believe… overtime anyway not just me but everyone.'[262]

Relying on these e-mails, Smith was charged at a disciplinary hearing with material breach of contract, insubordination and insulting behaviour, and bringing the respondent's name into disrepute.[263] At the hearing Smith challenged the impartiality of the chairman and argued that the e-mails had been obtained in breach of both the Constitution and of RICA.[264] The chairman concluded that the e-mails were admissible as evidence against Smith, he further concluded that the e-mails breached clauses of Smith's contract of employment.[265] She was then dismissed and referred the dispute to the CCMA.[266]

At arbitration the commissioner considered first, whether the e-mail evidence was obtained unlawfully, and if it was, the admissibility of that evidence.[267] Section 2 of RICA provides that 'Subject *to this Act, no person may intentionally intercept or attempt to intercept… any communication in the course of its occurrence or transmission'.*[268] Section 4(1) of the same Act provides: '*Any person, other than a law enforcement officer, may intercept any communication if he or she is a party to the communication, unless such communication is intercepted by such person for purposes of committing an offence.'* [269] Section 5(1) of the same Act provides: '*Any person, other than a law enforcement officer, may intercept any communication if one of the parties to the communication has given prior consent in writing to such*

260 *Ibid at 1473, par 14H.*
261 *Ibid at 1473, par 14H.*
262 *Ibid at 1473, par 15I.*
263 *Ibid at 1470H.*
264 *Ibid at 1470H-I.*
265 *Idem.*
266 *Ibid at 1471J.*
267 *Ibid at 1471A.*
268 *Idem.*
269 *Ibid at 1476, par41I.*

interception, unless such communication is intercepted by such person for purposes of committing an offence.[270]

The commissioner noted, from the date stamps on the print-outs, that only one of the e-mails produced at arbitration had been printed out on the day that De Lora accidentally accessed Smith's private Gmail account.[271] This meant that the account must have been intentionally accessed later.[272] The respondent had no right to access Smith's private e-mails as it had to exit its own sphere of ownership and enter the Internet domain technically owned by Google in order to do so.[273] The fact that Smith clearly exited her account in a manner which left it open to access by another person did not, by default, place it in the public domain, unlike Facebook, where privacy could not reasonably be expected, Smith's e-mails had specified recipients and was intended for their eyes only.[274]

The commissioner considered the consequence of that finding and found that any evidence which depends on the breach of a constitutional right may only be admitted if its admission is justified by section 36(1) of the Constitution.[275] This includes the applicant's right to privacy as contained in section 14(d) of the Constitution.[276] Respondent acquired the content of Smith's communications by electronic means although she was not the sender, the recipient or intended recipient of those communications.[277] As such, respondent was not party to the communications.[278] Smith had not given consent to such interception.[279] The Commissioner stated that the Respondent had no right to rely on the presence of the e-mail data on its own hard drives or servers, as might have been the case had Smith downloaded her private e-mails into a pc-based e-mail box.[280]

---

270 *Smith and Partners in Sexual Health (non-profit), (2011) 32 ILJ 1470 (CCMA) at 1476-1477, par 42J-43.*

271 *Ibid at 1471B.*

272 *Idem.*

273 *Ibid at 1471C.*

274 *Ibid) at 1471C-D.*

275 *Ibid at 1471E.*

276 *Idem.*

277 *Ibid at 1477, par 48H.*

278 *Smith and Partners in Sexual Health (non-profit), (2011) 32 ILJ 1470 (CCMA) at 1477, par 48H.*

279 *Idem.*

280 *Smith and Partners in Sexual Health (non-profit), (2011) 32 ILJ 1470 (CCMA) at 1477, par 49I.*

After reviewing the evidence as a whole the commissioner could not find that the limitation of Smith's right to privacy was justified and ruled that, with the exception of the one accidently discovered e-mail, the e-mail evidence was inadmissible.[281] On the content of that single e-mail dismissal was not warranted and was substantively and procedurally unfair.[282] Smith also received compensation as according to Section 194 of the Labour Relations Act which provides that compensation must be '*just and equitable in all circumstances but may not be more than the equivalent of 12 months' remuneration'.*[283]

4.3 CONCLUSION

As seen from the above cases, one can make the inference that where an employee is using the employer's electronic communications (whether e-mail or telephone or even social media) during working hours for their own personal use, this would not constitute as breaching the employment contract nor would it be bringing the employer's name into disrepute. It would be different if the employee was using the employer's electronic communications during working hours and the communications were detrimental to the employer's business entity. The mere fact that an employee makes use of communications at work for their private life should therefore be respected and their privacy not infringed, all within reasonable expectations. Especially as can be seen in the *Smith* case above where the employee had made use of her own private e-mail account and not that of the employer's general e-mail. The employer was not given any consent to access the employee's personal e-mail account and therefore that evidence used against the employee was inadmissible and obtained without any consent given by the employee. The same can be said with regards to social networking sites, access to such a site by an employer without the consent of the employee is an infringement of the employee's privacy, if access gained to those sites was done without consent given by the employee. An employer may also not use an employee's social networking site to gather information about such employee that would be used to discriminate against the employee in his working environment. However, if there are statements that are made on such social

281 *Smith and Partners in Sexual Health (non-profit), (2011) 32 ILJ 1470 (CCMA) at 1471E.*

282 *Smith and Partners in Sexual Health (non-profit), (2011) 32 ILJ 1470 (CCMA) at 1471E-F.*

283 *Smith and Partners in Sexual Health (non-profit), (2011) 32 ILJ 1470 (CCMA) at 1480, par 66E.*

networking sites that would bring the employer's name into disrepute then there will be no infringement of the employee's privacy.

CHAPTER 5: CONCLUSION

5.1 PRIVATE OR PUBLIC SPACES?

It has been argued that cyberspace has a unique structure and that it is made up of the "internet's 'public roads' or backbone transit infrastructure" which is regulated according to telecommunications law,[284] and secondly of a "mosaic of private allotments-namely, neighbouring proprietary websites".[285] Benoliel argues firstly that there has been an over-emphasis on information or database privacy and secondly that private and public localities could coexist on the internet just as they do in the physical world.[286] He suggests that the courts could be "required to differentiate and identify public locales and then fence them out from private ones".[287] This, he proposes, could be achieved through the creation of legal fictions for online locales.[288]

Undeniably online social networking sites could be identified as a locale where private acts occurs, where personal information is recorded and therefore one would have to agree with Abril's argument that the customs and usages of this space, and not the objective facts of space, could define the territory in which one could legally claim a right to privacy.[289] To distinguish between private and public spaces on the internet the emphasis should be on whether or not the online networking profile is protected by a password and set at private, where custom and usage could indicate that a person demonstrates a will to keep such information private,[290] and that the mere visibility of a cyber-identity should not automatically imply consent to an invasion of privacy.[291]

---

284 Papadopoulos, S. 2009. Revisiting the Public Disclosure of Private Facts in a Cyberworld. *Obiter*. Vol 1: 39.

285 Benoliel 2005 23 *Cardozo Arts and Entertainments Law Journal 3.* http://www.cfp2004.org/spapers/benoliel-caseOfTerritorialPrivacy.pdf (accessed 26 July 2014).

286 Benoliel 2005 23 *Cardozo Arts and Entertainments Law Journal 6, 9 and 16.* http://www.cfp2004.org/spapers/benoliel-caseOfTerritorialPrivacy.pdf (accessed 26 July 2014).

287 Papadopoulos, S.2009. Revisiting the Public Disclosure of Private Facts in a Cyberworld. *Obiter.* Vol 1: 39.

288 Benoliel 2005 23 *Cardozo Arts and Entertainments Law Journal 16.* http://www.cfp2004.org/spapers/benoliel-caseOfTerritorialPrivacy.pdf (accessed 26 July 2014).

289 Abril. 2007. *Harvard Journal of Law and Technology* 34.

290 Abril 2007 *Harvard Journal of Law and Technology* 35.

291 Abril 2007 *Harvard Journal of Law and Technology* 34.

5.2 CONCLUSION

"The much quoted 'right to be left alone' should be seen as a negative right to occupy a private space free from government intrusion, but as a right to get on with your life, express your intimate relationships without penalisation".[292] The question remains however, how can we give effect to the words of our constitutional court and ensure that privacy exists where traditional jurisprudence dictates that there is no physical space and no inherently private subject matter, secrecy or seclusion?[293]

South African law readily protects the privacy of telephone communications as well as e-mails sent between parties communicating with each other, and it found a way to apply traditional privacy jurisprudence to these modes of communication.[294]This can be seen from the legislation as well as case law mentioned in the previous chapters.

As can be seen from the previous chapters, South African law plays an important role with regards to determining an employee's right to online privacy in the working environment. South African law does protect employee's provided that the employee does not in his personal life or on his or her social networking sites make any defamatory remarks about the employer's business and that the employee does not bring the employer's business into disrepute. The employees making use of social networking sites should also realise that although they are communicating in cyberspace, their actions have real world consequences.[295] Employees need to take care in what they are posting onto social media, as that "space" is not viewed as having complete privacy. The internet is a very public place and therefore one cannot expect guaranteed privacy regardless of their privacy settings on their social media accounts. The employer is, however, not entitled to have access to the employee's social media account but should it be known that there are derogatory or defamatory remarks made about the employer's business, then the employee shall

---

292 *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 12 BCLR 1517 (CC) par 116.

293 Papadopoulos, S. 2009. Revisiting the Public Disclosure of Private Facts in a Cyberworld. *Obiter*. Vol 1: 42.

294 Papadopoulos, S. 2009. Revisiting the Public Disclosure of Private Facts in a Cyberworld. *Obiter*. Vol 1: 42.

295 Roos, A. 2012. Privacy in the Facebook Era: A South African Legal Perspective. *The South African Law Journa*l. 129: 401.

be held responsible regardless of their privacy settings. The more access we have to the internet the less restrictive our privacy becomes.

There is, however, a reasonable expectation that is to be had with regards to what information is being transmitted electronically or via telephone communications. An employer does not just have the right to access any of its employee's private communications without prior consent which has to be given freely by the employee. No interception or monitoring of the employee's online activities can be done without consent from the employee, either by way of the employee signing an ECP or by being part of the employment contract. It is therefore important for the employer to have an ECP in place in order to protect the employer as well as to provide certainty to the employee as to what is expected from the employee. At present an employer is required to put in place an ECP in the workplace which should also comply with Schedule 8 of the Labour Relations Act 66 of 1995. The Employee must then be made aware of such a policy and consent must be given by the employee by signature thereof, which shall then bind the employee to the terms of the policy.

As argued by Roos, the right to privacy as recognised in South African law is already capable of protecting the privacy of the uses of social networking sites, provided that the law recognises that people who use these social networking sites such as Facebook do not give up all expectations of privacy.[296] The mere fact that they reveal personal information on what may be considered a public or quasi-public forum does not mean that they intended to make that information available to all and sundry.[297] Roos further states that information revealed to 'friends only' should be treated as information that has been published to a limited number of persons, and any distribution of that information by third parties to a wider audience should be considered an invasion of the right to privacy that should have legal consequences.[298] The law should also give recognition to the fact that searches on social networking sites by third parties (such as employers) for purposes unrelated to

296 Roos, A. 2012. Privacy in the Facebook Era: A South African Legal Perspective. *The South African Law Journa*l. 129: 401.

297 *Idem.*

298 *Idem.*

the purpose for which personal information was initially supplied, are wrongful and could give rise to a claim based on the infringement of the right to privacy.[299]

It can therefore be concluded that the rights and privacy of an employee need to be balanced against that of the employer. In order to have such a balance an ECP needs to be put in place, one that is fair to both employer and employee. Without such a balance, the employee's right to online privacy could be infringed.

[299] Roos, A. 2012. Privacy in the Facebook Era: A South African Legal Perspective. *The South African Law Journa*l. 129: 401.

BIBLIOGRAPHY

BOOKS AND REPORTS

Buys, R. & Cronje, F. (Eds). 2004. *Cyberlaw@SA II: the law of the Internet in South Africa.* 2nd ed. Pretoria: Van Schaik.

Cheadle, M.H., Davis, D.M. & Haysom, N.R.L. (Eds). 2000. *South African constitutional law: the Bill of Rights.* Durban: Butterworths.

Currie, I. & De Waal, J. 2005. *The Bill of Rights handbook.* 5th ed. Cape Town: Juta.

De Waal, J., Currie, I., & Erasmus,G. 2001. *The Bill if Rights handbook* 4th ed.

Le Roux, PAK. *'Employment Practices in the Age of the internet'* (Unpublished paper delivered at the E-commerce and Current Commercial Law Workplace on 29 August 2003 at Sandton Johannesburg).

Neethling, J., Potgieter,JM. & Visser,P.J. 2005. *Neethling's law of personality. 2nd ed. Durban*: Lexis Nexis.

Papadopoulos & Snail *ed Cyberlaw@SA III: The Law of the internet in South Africa (2012)*: Van Schaiks.

Roos, A. 2003. The law of data (privacy) protection: a comparative and theoretical study. Unpublished LLD thesis, Pretoria, UNISA.

SA Law Reform Commission (SALC). 2005. Discussion paper 109.

South African Law Commission.1994. *Interim Report on Group and Human Rights.*

UNCITRAL Model Law on Electronic Commerce. 1996 with additional *art 5bis* as adopted in 1998.

Van der Merwe, D., Roos, A., Pistorius,T. & Eiselan, S. 2008. *Information and Communications Technology Law*: Lexis Nexis.

JOURNAL AND INTERNET ARTICLES

Abril 2007. Recasting Privacy Torts in a speechless World*. Harvard Journal of Law and Technology.*

Benoliel. 2005. 23 *Cardozo Arts and Entertainment Law Journal*

Biddy, A. 'Who's got mail? At work, e-mail and the Web Become Public' (August 2001) 40 *The Magazine of the ILO World of Work.*

Boyd, D.M & Ellison, N. 'Social network sites: Definition, history, and scholarship' (2007) 13 J of *Computer-Mediated Communication* article 11, available at *http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html*. (accessed 28 October 2014).

Cohen T. 2001. But for the necessity of knocking and requesting right of entry. *Surveillance Law and Privacy Rights in South Africa,* 1:2-17.

Collier, D. 2002. Workplace privacy in the cyber age. *Industrial Law Journal,* 23: 1743-1759.

Dekker, A. 2004. Vices or devices: employee monitoring at the workplace. *South African Mercantile Law Journal,* 16: 624.

Grimmelman, J. 'Saving Facebook' (2009) 94 IOWA *LR* 1134 at 1144.

Hill, R. and Walden, I. 1996. The draft UNCITRAL Model Law of Electronic Commerce: Issues and Solutions. *The computer Lawyer* March. www.batnet.com/oikoumene/tacr.html (accessed 26 October 2014).
http://www.cfp2004.org/spapers/benoliel-caseOfterritorialPrivacy.pdf. (accessed 26 July 2014).

McGregor,M. 2004. The right to privacy in the workplace: general case law and guidelines for using internet and email. *SA Mercantile Law Journal*, 16: 639-650.

Mischke, C. 1999 9(5). Disciplinary Action and the Internet. *Contemporary Labour Law.*

Mischke, C. 2011. Social Networks, privacy and dismissal: Facebook, Twitter et al: the employer's reputational risk. *Contemporary Labour Law.* Vol 21, no 2 :11-17.

Modiba, M.2003. Intercepting and monitoring employees' e-mail communications and internet access. *South African Mercantile Law Journal*, 15: 366.

Neethling (2005) *South African Law Journal* : 18-19.

Papadopoulos, S. 2009. "Revisiting the Public Disclosure of Private Facts in a Cyberworld" *Obiter,* 1: 30-43.

Pistorius, T. (2009) Monitoring, interception and big boss in the workplace: Is the devil in the details*? Potchefstroom Electronic Law Review*, 12(II): 1-26.

Roos, A. 2012. Privacy in the Facebook Era: A South African Legal Perspective. *South African Law Journal,* 129:375-402.

SA Labour Law protects Facebook passwords
http://www.itweb.co.za/index.php?option=com_content&view=article&id=54212:sa-labour-law-protects-facebook-passwords. (Accessed 29th May 2014).

Van Niekerk, A. (1994). The right to privacy in employment. *Contemporary Labour Law*, 3: 97-100.

LEGISLATION

Constitution of the Republic of South Africa 108 of 1996.

Electronic Communications and Transactions Act 25 of 2002.

Employment Equity Act 55 of 1998.

Labour Relations ACT 66 of 1995.

Promotion of Access to Information Act 2 of 2000.

Protection of Personal Information Act 4 of 2013.

Regulation of Interception of Communications and Provisions of Communication-Related Information Act 70 of 2002.

CASE LAW

Abel v United States 362 US 217 (1960) 241.

Bernstein v Bester 1996 2 SA 751 (CC).

Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd; In Re: Hyundai Motor Distributors (Pty) Ltd v Smit NO 2001 1 SA 545 (CC).

Katz v United States 389 US 347 (1967).

Moonsamy v The Mailhouse (1999) 20 *ILJ* 464 (CCMA) at 471G.
National Coalition for Gay and Lesbian Equality v Minister of Justice 1999 12 BCLR 1517 (CC)

O' Connor v Ortega 480 US 709 1987.

Phillip Neethling v South African Fruit Terminals (unreported case) CCMA Durban, Case No. KN-4881-04.

Protea Technology Ltd & another v Wainer and others (1997) 9 BCLR 1225 (W).

Smith and Partners in Sexual Health (non-profit), (2011) 32 *ILJ* 1470 (CCMA).