

**LEGAL PRINCIPLES REGULATING THE PROCESSING OF PERSONAL
INFORMATION IN THE WORKPLACE**

by

UNATHI PEARL NXOKWENI
(Student number 43803873)

Submitted in accordance with the requirements
for the degree of

Masters of Laws (LLM)

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR


PROFESSOR ANNELIESE ROOS

2018

DECLARATION

Student number:43803873

I **UNATHI PEARL NXOKWENI** hereby declare that **LEGAL PRINCIPLES REGULATING THE PROCESSING OF PERSONAL INFORMATION IN THE WORKPLACE** is my own work and that all the sources I have used or quoted have been indicated and acknowledged by means of complete references.



Signature

October 2018

Date

PREFACE

Firstly, I would like to thank God and my Ancestors for giving me the strength and courage to complete this dissertation.

To my son Kamogelo Tseke, this is yours my lovely son. I pray that this dissertation motivates you to work harder than your mom, I love you.

To my supervisor Prof A Roos. Thank you for your constructive criticism, guidance, and supervision. Thank you for your effort of taking your time to read my work. You are indeed a good supervisor.

To Prof F Abioye thank you for being patient and understanding. Thank you for helping me with my research, for proofreading my work. God bless you Fumni.

To my family, relatives and colleagues thank you for your continual support and love.

SUMMARY

This study focuses on the right to privacy in the workplace, specifically employees' expectations of electronic privacy where personal information is processed. The main aim of this dissertation is to establish whether, given advances in technology, South African laws offers adequate protection for employees when their electronic information is being processed.

The study analyses South African law as it relates to the privacy of employees during the processing of their personal Information in the workplace. This is examined within the parameters of the constitutional and legislative framework with due regard to the common-law right to privacy. The legal issues are examined from a South African context and is compared with data protection laws and regulations of the United Kingdom. It also offers recommendations based on experience gained in the United Kingdom.

List of Abbreviations

Art	Article
CC	Constitutional Court
CCMA	Commission for Conciliation Mediation and Arbitration
CEO	Chief Executive Officer
Dir	Directive
DPA	Data Protection Act (UK)
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
ECT	Electronic Communication and Transaction Act (SA)
EEA	European Economic Area
EU	European Union
Fn	Footnote
GDPR	General Data Protection Regulation
ILJ	Industrial Law Journal
LRA	Labour Relations Act (SA)
OECD	Organisation for Economic Cooperation and Development
PAIA	Promotion of Access to Information Act (SA)
PER	Potchefstroom Electronic Law Journal
POPI	Protection of Personal Information Act (SA)
RICA	Regulations of Interception of Communications and Provisions of Communication-Related Information Act 70 of 2002 (SA)
RIPA	Regulation of Investigatory Powers Act of 2000
S	Section
SALJ	South African Law Journal
SALRC	South African Law Reform Commission
TSAR	Tydskrif vir die Suid-Afrikaanse Reg
UK	United Kingdom
WP29	Article 29 Data Protection Working Party
WWW	World Wide Web

KEYWORDS

Personal information, right to privacy, workplace, processing, monitoring. data, employer, employee.

TABLE OF CONTENTS

DECLARATION	II
PREFACE	III
SUMMARY	IV
LIST OF ABBREVIATIONS	V
KEYWORDS	VI
Chapter 1 Introduction	
1.1 BACKGROUND	1
1.2 RESEARCH QUESTION AND PURPOSE STUDY	2
1.3 METHODOLOGY	3
1.4 PRILIMINARY DEFINITION OF KEY TERMS	4
1.5 STUCTURE OF THE DISSERTATION	6
Chapter 2 Right to privacy	
2.1 INTRODUCTION	7
2.1.1 Meaning of privacy	8
2.1.2 Privacy in the employment context	9
2.2 PRIVACY UNDER COMMON LAW	10
2.2.1 Background	10
2.2.2 General principles for liability	12
2.2.2.1 <i>Act</i>	13
2.2.2.2 <i>Wrongfulness</i>	14
2.2.2.3 <i>Intention</i>	16
2.2.3 Grounds of justification	16
2.2.4 Remedies	18
2.2.5 Conclusion	19
2.3 CONSTITUTIONAL PROTECTION OF PRIVACY	19
2.3.1 Provision in the Constitution	19

2.3.2	Elements for constitutional invasion of the right to privacy	22
2.3.3	Constitutional Remedies	23
2.3.3.1	Constitutional damages	23
2.3.3.2	Interdicts	23
2.3.4	Limitation of the right to privacy	24
2.4	INTERNATIONAL RECOGNITION OF THE RIGHT TO PRIVACY	25
2.5	CONCLUSION	26

Chapter 3 Data privacy legislation in South Africa

3.1	INTRODUCTION	27
3.2	LABOUR RELATIONS ACT	28
3.2.1	Introduction	29
3.2.2	The need for an electronic communication policy	30
3.3	PROMOTION OF ACCESS TO INFORMATION ACT 2 OF 2000	32
3.4	THE REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATION RELATED INFORMATION ACT 70 OF 2000	33
3.4.1	Prohibition on interception and monitoring	34
3.4.2.	Interception of communication allowed by RICA	35
3.4.2.1	Interception of a communication by a party to the communication	35
3.4.2.2	Interception of a communication with the consent of the party to communication	36
3.4.2.3	Interception of an indirect communication pertaining to carrying on of a business	37
3.5	PROTECTION OF PERSONAL INFORMATION ACT	38
3.5.1	Introduction	38

3.5.2	Provisions of POPI that are relevant to this discussion	39
3.5.3	Action based on POPI	43
3.6	CONCLUSION	43
Chapter 4 United Kingdom perspective		
4.1	INTRODUCTION	44
4.2	PROTECTION OF PRIVACY UNDER COMMON LAW	45
4.2.1	Privacy protection before European Convention of Human Rights (ECHR)	45
4.2.1.1	<i>Breach of confidence and misuse of private information</i>	45
4.2.1.2	<i>Breach of contract</i>	46
4.3	PROTECTION OF PRIVACY UNDER HUMAN RIGHTS ACT	46
4.4	PROTECTION OF PRIVACY UNDER LEGISLATION	50
4.4.1	Data Protection Act of 1998	50
4.4.2	Data protection principles	51
4.4.2.1	<i>Personal data must be processed fairly and lawfully</i>	51
4.4.2.2	<i>Personal data must be held only for one or more specified and lawful purposes, and not processed in any manner incompatible with that purposes</i>	53
4.4.2.3	<i>Personal data must not be used or disclosed in a manner incompatible with the purpose for which it is held</i>	54
4.4.2.4	<i>Personal data must be adequate, relevant and not excessive in relations to the purpose for which it is held</i>	54
4.4.2.5	<i>Personal data must be accurate and where necessary kept up to date</i>	55
4.4.2.6	<i>Data may not to be kept longer than necessary for the purposes for which they were collected</i>	55
4.4.2.7	<i>Personal data must be processed in accordance with the rights of the data subjects under the Act</i>	57
4.4.2.8	<i>Appropriate technical and organisational measures must be</i>	

<i>taken against unauthorise or unlawful processing of personal data and against accidental loss, destruction of, or damage to, personal data</i>	57
4.4.2.9 <i>Personal data may not be transferred to a country or territory outside the European economic area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information</i>	58
4.4.3 Exemption to the prohibition in terms of Schedule 4	58
4.5 RIGHTS OF THE DATA SUBJECT	59
4.5.1 Right of access to personal data	59
4.5.2 Right to prevent data processing likely to cause damage or distress	59
4.5.3 Right to compensation for failure to comply with certain requirements	60
4.5.4 Right in relation to inaccurate data	61
4.6 INTERCEPTION OF ELECTRONIC COMMUNICATION	61
4.7 GENERAL DATA PROTECTION REGULATION	65
4.7.1 Three main reforms under the GDPR	66
4.7.1.1 Compulsory appointment of the data protection officer from companies whose business includes processing data	67
4.7.1.2 The obligation to protect data as early as the design stage and of the processing system	67
4.7.1.3 The obligation to document all of the personal data processing activities the company perform	68
4.8 CONCLUSION	68
Chapter 5 Conclusion and recommendation	
5.1 SUMMARY	70
5.2 CONCLUSION	72
5.3 RECOMMENDATIONS	73
5.3.1 Privacy by design	73

5.3.2	Data protection impact assessments	74
5.3.3	Data portability	74
5.3.4	General recommendations	74
	BIBLIOGRAPHY	76

Chapter 1

Introduction

1.1 BACKGROUND

The introduction of electronic communication in the workplace has changed how employers conduct their business and, in turn, the way in which employees are expected to perform their duties.¹ Increased electronic communication in the workplace has infused the physical employment environment with electronic communication technology.² The increase in this form of communication threatens the employee's right to privacy in today's workplace characterised by reliance on information communication technology, and in particular, the use of emails and the internet to conduct business.

An employee typically sends and receives thousands of emails, and certain of these contain information of a personal nature about the employee. These emails are stored on the employer's server.³ Line managers and colleagues are also likely to send and receive emails with personal information about the employee concerned. Through the interception of online communications, personal information can be collected, processed, and, at times used in a wrongful manner.

Employers also process personal information of employees during basic management activities, such as hiring, payroll processing, performance evaluation, and decisions on promotion.

¹ Collier 2002 *ILJ* 1743.

² Pistorius 2009 *PER* 1.

³ Lorber 2004 *ILJ* 180.

1.2 RESEARCH QUESTION AND AIM OF THE STUDY

This research examines the degree of protection afforded the personal information of employees in the workplace, and whether the employee's right to privacy can effectively be balanced against the employer's aim of establishing a productive and safe environment when personal information is processed.

Employees do not have a significant influence in the processing of their personal information once it is in the hands of their employer. They also generally have limited knowledge of who is able to access their personal information. From the perspective of the individual, the enactment of the Protection of Personal Information Act 4 of 2013 (the POPI Act) is to be welcomed. In terms of this Act, employers are required to amend systems, processes, and policies regarding the handling of personal information to bring them in line with the legislation. Once fully operational, the POPI Act will ensure a significant level of protection for individuals and organisations in South Africa as regards how their personal information is handled. Other than has been the case to date, employees will be able to hold employers accountable for actions involving their personal information.

The efficacy of the POPI Act in the employment environment has not yet been established as the Act is not yet fully operational. However, it is hoped that the Act will be subjected to public scrutiny in the near future.⁴

⁴ Only the sections dealing with the establishment of the Regulator have come into force (see GG 37544 of 11 April 2014). It is anticipated that the Act will come into full effect once the Regulator is operational (Information Regulator Media Statement 2 Dec 2016 available at <http://www.justice.gov.za/inforeg/docs/ms-20161202-inforeg.pdf> (date of use: 18 July 2018).

1.3 METHODOLOGY

This research makes use of the literature review as its methodology. This involves a review and analysis of the literature that has contributed significantly to the development of privacy protection in South Africa and the United Kingdom (the UK). It includes legislation, case law, common law, treaties and other international instruments, textbooks, journal articles, and electronic material sourced from various internet sites. The findings are used to offer workable suggestions for the improvement of the current position in South Africa.

The UK has been selected for comparative study as it offers a rich source for comparison. It has data protection legislation – the Data Protection Act⁵ – the UK’s implementation of European Directive 95/46/EC which aims to create uniform European standards for the collection, storage, and processing of personal information.⁶ Although the UK has recently adopted a new Data Protection Act,⁷ the focus of our discussion is on the 1998 Act and case law decided under that.⁸ South Africa’s Protection of Personal Information Act⁹ is based on the EU Directive and South Africa can still learn from the interpretation given to its provisions as implemented in the UK Data Protection Act of 1998.

The UK also has secondary legislation which contains provisions governing privacy in the employment relationship and the interception of communications, namely, the Regulation of Investigatory Powers Act.¹⁰ Furthermore, the UK has other sources that assist in improving and complying with the Data Protection Act when it comes to the processing of personal information in the workplace. Notable here is the Employment Practice Code¹¹

⁵ Data Protection Act, 1998.

⁶ Carey *Data Protection* 6.

⁷ Data Protection Act of 2018.

⁸ The new Act is the UK’s implementation of the European Parliament’s new Regulation (EU) 2016/679 on data protection, also known as the General Data Protection Regulation (the GDPR).

⁹ Act 4 of 2013.

¹⁰ Regulation of Investigatory Powers Act, 2000. It also regulates the powers of public bodies to carry out surveillance and investigation.

¹¹ Available at https://ico.org.uk/media/for-organisations/documents/1064/the_employmentpractices-code.pdf (date of use: 19-07-2016).

issued by the Information Commissioner under section 51 of the Data Protection Act.¹² The purpose of the code of practice is to translate the legislative provisions into actual practice in the information sector involved. The UK courts have heard a number of cases that directly or indirectly involve the processing of personal information influencing the data protection regime, for example, *Halford v United Kingdom* that is discussed below.¹³ We can learn from the UK when implementing our domestic data protection law as the UK law addresses most data protection and privacy issues in the workplace.

It is acknowledged that data protection legislation has recently been adopted in several African states, but none of them has the rich background and development found in UK law and therefore they were not considered helpful for purposes of comparison.¹⁴

1.4 PRELIMINARY DEFINITION OF KEY TERMS

This section provides preliminary definitions of certain key terms frequently used in the dissertation.

Processing: ‘Any operation or activity, or any set of operations, whether by automatic means or not, which concern personal information. This may include the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, use, dissemination by means of transmission, distribution or making available in any other form, or merging, linking, as well as restriction, degradation, erasure or destruction of information’.¹⁵

¹² Act of 1998.

¹³ *Halford v United Kingdom* (20605/92) [1997] IRLR 471, (1997) 24 EHRR 523.

¹⁴ See Makulilo *African Data Privacy Laws* in general. The African Union has also adopted a Convention on Cyber Security and Personal Data Protection (EX.CL/846(XXV)). The convention covers a very wide range of online activities, including electronic commerce, data protection, and cybercrime, with a special focus on racism, xenophobia, child pornography, and national cyber security. The convention will only come into force once 15 of the 54 member states have ratified it.

¹⁵ Act 4 of 2013 s 1.

Data controller: Any person who by electronic means, requests, collects, collates, processes, or stores personal information from or in respect of a data subject.¹⁶

Data subject: Any natural person from or in respect of whom personal information has been requested, collected, collated, processed, or stored.¹⁷

Employee: The Employment Equity Act defines an employee as any person, other than an independent contractor, who works for another person or the state, and who receives, or is entitled to receive, any remuneration, and who in any manner assists in carrying on or conducting the business of the employer.¹⁸

Personal Information: Information relating to an identified, living, natural person and, where applicable, an identified, existing juristic person. The following types of information are examples of personal information: information relating to race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, wellbeing, disability, religion, conscience, belief, culture, language, and birth. It further includes information relating to the education, the medical, financial, criminal, or employment history of a person, and any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other particular assignment to the person. Other examples include the biometric information of a person, the personal opinions, views, or preference of a person, correspondence sent by the person that is implicitly or explicitly of a private or confidential nature, or further correspondence that would reveal the contents of the original correspondence. Also included are the views or opinions of another individual about the person, and the name of the person if it appears with other personal information relating

¹⁶ Ibid.

¹⁷ Ibid.

¹⁸ Act 55 of 1998 s 1.

to him or her, or if the disclosure of the name itself would reveal information about the person.¹⁹

1.5 STRUCTURE OF THE DISSERTATION

Chapter One provides the background to the topic and sets out the research question.

Chapter Two examines the protection and development of the right to privacy in South Africa. The chapter commences with a brief discussion of the right to privacy. It thereafter analyses the right to privacy under common law and the Constitution of the Republic of South Africa, 1996, (the Constitution), and briefly considers the international recognition of the right to privacy.

Chapter Three is the core of the dissertation, and focuses on the protection of privacy in the workplace given the advances in technology. This chapter examines South African legislation applicable to the privacy of electronic communications and personal information in the workplace.

Chapter Four examines the scope and extent of the right to privacy, with respect to the processing of personal data in the workplace environment in the United Kingdom. The chapter considers and analyses the legal framework and relevant sources – legislation, textbooks, journal articles, and cases – that have contributed to the development of the protection of privacy in the workplace environment.

Chapter Five presents the conclusions and recommendations emerging from the dissertation.

¹⁹ Act 4 of 2013 s 1.

Chapter 2

Right to Privacy

2.1 INTRODUCTION

This chapter focuses on the nature and the scope of the right to privacy in South Africa in terms of the common law and the Constitution. It also considers the extent of the right to privacy within the employment relationship. The right to privacy is one of the most important rights recognised worldwide. In many instances, it is protected as a fundamental right. The right to privacy is not a new legal concept in South Africa; before the Constitution came into force, the right to privacy was protected by common law as a personality right under the law of delict. Privacy is a personality interest, and in turn, a personality interest is a non-patrimonial interest that cannot exist independently of an individual.²⁰

Neethling points out that the importance of the recognition of the right to privacy as a fundamental right lies in the fact that the legislature and the executive of the state may not adopt any law or take any action, which infringes or unreasonably limits the right.²¹

The right to privacy, like the other rights in the Bill of Rights, applies to both the state and individuals.²²

For the purpose of this dissertation, the focus is on 'informational privacy'. Informational privacy is the particular aspect of the general right to privacy that has come to be of

²⁰ Neethling, Pogieter, & Visser *Neethling's Law of Personality* 14 and Roos *Data (privacy) Protection* 545.

²¹ Neethling, Pogieter, & Visser *Neethling's Law of Personality* 17 and Van der Merwe et al *Information Communications* 418.

²² Constitution of the Republic of South Africa, 1996, s 8.

considerable practical importance²³ in that it restricts the collection, use, and disclosure of private information. It also encompasses a related interest in having access to personal information collected by others, in order to establish its content and check its accuracy.²⁴ Informational privacy is relevant in the workplace as personal information is regularly processed in the workplace during basic management activities, including, but not limited to, hiring, payroll processing, performance evaluation, and decisions on promotion.²⁵

2.1.1 Meaning of privacy

Privacy is regarded as a valuable aspect of an individual's personality.²⁶ Two American lawyers, Brandeis and Warren, have described it as an individual's right to be left alone.²⁷ The idea of the right to privacy has been extended from the simple right to be left alone, to a far wider concept, which includes a person's right to control his or her personal information and affairs.²⁸

It is generally accepted that privacy is difficult to define in that it is vague, amorphous, and elusive, and often means different things to different people.²⁹ This notwithstanding, Neethling defines privacy as an individual condition of life characterised by seclusion from the public and publicity.³⁰ This condition embraces all those personal facts which the person concerned has him- or herself determined must be excluded from the knowledge of outsiders, and which he or she wishes to be kept private.³¹ Neethling points out that the crucial question is how to determine what facts regarding a person are private in nature. He argues that it is up to each person to determine this for him- or herself – in other words, he or she must make the facts private.³² In line with this principle, he submits

²³ Currie & de Waal *Bill of Rights* 323.

²⁴ Currie & de Waal *Bill of Rights* 323.

²⁵ Schwartz & Reidenberg *Data Privacy* 252.

²⁶ South African Law Reform Commission Discussion Paper (Project 124 2005) *Privacy and Data Protection* 49.

²⁷ Warren & Brandeis 1890 *Harvard LR*193.

²⁸ Roos 2012 *SALJ* 378.

²⁹ Neethling 2005 *SALJ* 18.

³⁰ This definition was also accepted in *National Media Ltd v Jooste* 1996 (3) SA 262 (A).

³¹ Neethling, Pogieter & Visser *Neethling's Law of Personality* 270.

³² Neethling, Pogieter & Visser *Neethling's Law of Personality* 270.

that a person must have the will, wish, or desire that the fact be kept private. He qualifies this by stating that society must agree with the person that the information may be kept private. In other words, the *boni mores* play a role, and a person cannot keep information private if it is unreasonable to do so, or if society has a legitimate interest in being aware of the facts.

2.1.2 Privacy in the employment context

The right to privacy in the context of the employment relationship is unique and very difficult to pin down. The employee has a right to privacy, but he or she is expected to be honest and loyal, especially during working hours, and to stand in a relationship of trust with the employer.³³ Employees, however, remain people; they retain their status as moral agents and, clearly, an employee does not forfeit all his or her privacy when entering the workplace.³⁴ The Commission for Conciliation, Mediation and Arbitration³⁵ held in *Moonsamy v The Mailhouse* that the rights to which the citizen is entitled 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 might legitimately affect the employee's personal rights in a manner not possible outside of the workplace. In other words, there is a clear need to balance interests.³⁶ Neethling also points out that all persons have a fundamental need for some degree of privacy.³⁷ Lack of privacy or infringement of privacy, may negatively affect a person, whether mentally or otherwise.³⁸ Therefore, individuals have an interest in the protection of their privacy.³⁹

Collier⁴⁰ suggests that the protection of privacy includes the protection of personal data in an employment-law context. The employee will always be entitled to some level of privacy,

³³ Dekker 2004 *Merc LJ* 622.

³⁴ Mischke 2003 *Cont LL* (8) 73.

³⁵ Hereafter the CCMA.

³⁶ *Moonsamy v The Mailhouse* (1999) 20 *ILJ* 464 (CCMA) 471G.

³⁷ Neethling 2005 *SALJ* 19.

³⁸ Neethling, Pogieter & Visser *Neethling's Law of Personality* 29.

³⁹ Neethling, Pogieter & Visser *Neethling's Law of Personality* 29.

⁴⁰ Collier 2002 *ILJ* 1744.

meaning that the employer cannot compel an employee to relinquish all his or her rights to privacy. Consequently, there is a need for the employer to differentiate clearly between what is considered private data on the one hand, and business related data, on the other. Collier further points out that employers are required to protect their employees' personal data from disclosure to others, by putting in place a range of programs and systems that provide varying degrees of privacy and security of communications.⁴¹ These include encryption, anonymous remailers, proxy servers, and digital cash.⁴²

Viewed from the employer's perspective, it can be argued that as the employer provides and controls the computer facilities the employee uses, the employer has the right to control its employees' working life. The employer also has the right to protect his or her business interests and the integrity of his or her computing equipment against viruses, cyber loafing, etcetera.

2.2 PRIVACY UNDER COMMON LAW

2.2.1 Background

In South Africa, privacy is protected under common law as a personality interest by the law of delict.⁴³ Infringement of a personality right is regarded as an *iniuria*, and a plaintiff may institute the *actio iniuriarum* against anyone causing the *iniuria*. The *actio iniuriarum* protects injury to the *corpus* (bodily integrity), *fama* (good name or reputation), and *dignitas* (all personality interests apart from the *corpus* or *fama*, such as dignity, privacy, and identity).

The idea of the right to privacy as a separate personality right was not initially recognised by South African courts. For this reason, judgments limited the concept of *dignitas* to dignity, and the courts were reluctant to recognise the existence of an independent right

⁴¹ South African Law Reform Commission (SALRC) Privacy and Data Protection project 124 discussion paper 109 October 2005.

⁴² SALRC Privacy and Data Protection discussion paper 109 October 2005.

⁴³ Neethling, Pogieter & Visser *Neethling's Law of Personality* 3.

to privacy.⁴⁴ Limitation of the concept of *dignitas* to dignity, resulted in insult or *contumelia* being set as a requirement for *iniuria*.⁴⁵ This changed when, in *O’Keeffe v Argus Printing and Publishing Co Ltd*,⁴⁶ the court firmly rejected the argument that the right to privacy should be equated with the right to dignity. Accordingly, this case has come to be regarded as the *locus classicus* for the recognition of an independent right to privacy in South African law.⁴⁷ In this case, the plaintiff, O’Keeffe, brought an *actio iniuriarum* for the unauthorised use of her photograph and name in an advertisement for a company distributing rifles, pistols, revolvers, and ammunition on the basis that the advertisement violated her *dignitas*. The defendant argued that *iniuria* demands that there must be an insult. Watermeyer AJ rejected the idea that *contumelia* or insult is the essence of an *iniuria*.⁴⁸ The court held that the unauthorised publication of a person’s photograph and name for advertising purposes is capable of “constituting an aggression upon that person’s *dignitas*”.⁴⁹ In considering whether there had been an invasion of the plaintiff’s privacy, Watermeyer AJ interpreted *dignitas* to include all the legally protected personality interests, save for bodily integrity (*corpus*) and reputation (*fama*). He further stated that such *dignitas* includes not only the single right to personality, but also all rights relating to dignity.⁵⁰ This case signaled the start of the recognition of the right to privacy in South African law.

Another case in which privacy was clearly distinguished from the other personality rights, is *S v A*.⁵¹ In this criminal case, two private detectives placed a listening device under the complainant’s dressing table at the request of her estranged spouse. The court found the detectives liable for invading the complainant’s privacy. In reaching this decision, the court held that the right to privacy is included in the concept of *dignitas*, and further that the

⁴⁴ *S v A* 1971 (2) SA 293 (T) 297. Botha AJ recognised a right to privacy as an independent personality right, but clouded this recognition by restricting *dignitas* to dignity or honour, thereby also negating the existence of an independent right to privacy.

⁴⁵ Neethling, Pogieter & Visser *Neethling’s Law of Personality* 242.

⁴⁶ *O’Keeffe v Argus Printing and Publishing Co Ltd and Others* 1954 (3) SA 244 (C).

⁴⁷ Neethling, Pogieter & Visser *Neethling’s Law of Personality* 271.

⁴⁸ *O’Keeffe v Argus Printing and Publishing Co Ltd and Others* 1954 (3) SA 244 (C) 246.

⁴⁹ *Ibid.*

⁵⁰ *O’Keeffe v Argus Printing and Publishing Co Ltd and Others* 1954 (3) SA 244 (C) 248.

⁵¹ *S v A* 1971 (2) SA 293 (T) 297.

infringement of a person's privacy, *prima facie* constitutes an impairment of his or her *dignitas*.⁵²

In the case of *Kidson v SA Association Newspapers Ltd*⁵³ the court was called upon to consider the protection of privacy in relation to the photographs of nurses taken by a journalist during their leisure time without their permission. The caption to the photograph read: "97 lonely nurses want boyfriends". Kuper J determined that the publication on the alleged desire to meet persons of the opposite sex because the nurses were lonely when off duty, was an insult to the young married plaintiff, and had infringed her privacy.

From these cases it can be concluded that the right to privacy is firmly established in common law as an independent right to personality, and the infringement of dignity and insult play no role in deciding whether there has been a violation of privacy.

2.2.2 General principles for liability

In order to establish common-law liability for the infringement of a personality interest such as the right to privacy, the plaintiff must establish that:

- (i) there has been an impairment of privacy, in other words an infringing act (either an intrusion or a disclosure);
- (ii) wrongfulness; and
- (iii) intention.

Under the *actio iniuriarum*, conduct that infringes a personality interest gives rise to two presumptions: a presumption that the publication was made wrongfully; and a presumption that it was made with intent. The defendant must rebut these presumptions.⁵⁴ The presumption of wrongfulness can be rebutted by proving that a ground of justification,

⁵² *S v A* 1971 (2) SA 293 (T) 297.

⁵³ *Kidson v SA Association Newspapers Ltd* 1957 (3) SA 461 (W).

⁵⁴ *Jansen van Vuuren v Kruger* 1993 (4) SA 842 (A) 849; *Herselman v Botha* 1994 (1) SA 28 (A) 35; *SAUK v O'Malley* 1977 (3) SA 394 (A) 401–402; *Naylor v Jansen*; *Jansen v Naylor* 2006 (3) SA 546 (SCA) 551 [7]. Loubser et al *Law of Delict* 335.

such as private defence, necessity, provocation, consent to injury, and exercise of a statutory right or official authority, exists.⁵⁵ The presumption of intent can be rebutted by proving that the publication was made mistakenly.⁵⁶

2.2.2.1 Act

For purposes of the law of delict, the conduct must, first, be that of a human. A juristic person acts through its organs (directors, managers, and officials) and may, therefore, be delictually liable for such actions. It is said that “an act performed by or at the command or with the permission of a director, official or servant of the legal corporation in the exercise of his duties or functions in advancing or attempting to advance the interest of the legal corporation, is deemed to have been performed by such corporation”.⁵⁷

The act must be voluntary. This entails that the conduct must have been susceptible to human control, thus it need not be voluntary or desired.⁵⁸

It is apparent that the act which is relevant in the area of informational privacy or data protection is any conduct that can be classified as the processing of personal data.⁵⁹ The fact that these types of conduct – such as the processing of data – are often performed automatically by means of a computer, does not result in the conduct not meeting the definition of the act as a voluntary human act, because the computer is merely an instrument in the hands of humans.⁶⁰

In an employment context, an example of an act of disclosure would be where an employee emails documents marked private and confidential, to an employer, and the employer discloses this information to another party without the employee’s consent.⁶¹

⁵⁵ Neethling, Pogieter, & Visser *Neethling’s Law of Personality* 56.

⁵⁶ Neethling, Pogieter, & Visser *Neethling’s Law of Personality* 163.

⁵⁷ Neethling, Pogieter & Visser *Law of Delict* 27.

⁵⁸ Neethling, Pogieter & Visser *Law of Delict* 28.

⁵⁹ Roos *Data (privacy) Protection* 552.

⁶⁰ Neethling, Pogieter & Visser *Law of Delict* 27.

⁶¹ Van der Merwe et al *Information Communications* 419.

In a CCMA case, *Smith and partners in sexual health (non-profit)*, Ms Smith was employed as an administrative assistant. One of her duties was to check the company's Gmail account and forward emails to the company's new email address. The company's CEO (Ms de Lora) wanted to log onto the company's Gmail account to check whether any emails had come in while Smith was on leave. Smith had forgotten to sign out of her personal Gmail account, and the CEO ended up looking at Smith's personal account. De Lora dismissed Smith because she found emails in her personal account in which the employee complained about her job, complained about De Lora, and told people outside of the organisation about its daily activities.

Smith took her employer to the CCMA for unfair dismissal. She argued that her employer had unlawfully intercepted her private internet-based emails on Gmail, and that her employer's action infringed her right to privacy. It was held that Smith had been unfairly dismissed and that De Lora (as CEO) had no right to read the employee's emails on her personal account.

2.2.2.2 *Wrongfulness*

The determination of wrongfulness entails a dual investigation. Firstly, it must be determined that a legally recognised interest has in fact been infringed. Secondly, prejudice must have occurred in an unreasonable manner.⁶²

The processing of data can infringe a personality interest in two ways: where personal information that is true is processed, the person's privacy is infringed. Examples would be if the employer were to disclose true private facts about his or her employee without a valid reason for doing so; or if an employer informs colleagues or employees about another employee's HIV status.⁶³ The second way is where false or misleading personal information is processed, in which case the person's identity is infringed.⁶⁴ This is illustrated in *S v Naidoo*⁶⁵ where the employer provided misleading information to a judge

⁶² Neethling, Pogieter & Visser *Law of Personality* 27.

⁶³ Loubser et al *Law of Delict* 318.

⁶⁴ Neethling, Pogieter & Visser *Neethling's Law of Personality* 270.

⁶⁵ *S v Naidoo* 1998 (1) BCLR 46 (D).

to obtain an order to tap a telephone in terms of the Interception and Monitoring Prohibition Act.⁶⁶ As the judge granted an order based of the false information he had been given about the employee, the order was unlawful and the monitoring was accordingly declared an unlawful violation of the accused's (employee) right to privacy. It was pointed out that the employer may monitor the employee's electronic communication, if it is connected to a business activity.

The general norm or criterion used to determine whether the particular infringement of interest is wrongful, is the objective *boni mores* test based on reasonableness.⁶⁷ The basic question is whether, according to the legal convictions of the community and in the light of all the circumstances of the case, the defendant infringed an interest of the plaintiff in a reasonable or unreasonable manner. In *Bernstein v Bester*⁶⁸ the court held that an expectation of privacy in relation to an individual's body, home and family life, and intimate relationships is reasonable.⁶⁹ However, as a person moves into communal relations and activities such as business and social interaction, the scope of the personal space decreases proportionately.

In *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd*⁷⁰ the court held that even when people are in their offices, in their cars, or on mobile telephones, they retain a right to privacy, since the Constitutional Court recognises that the right to privacy in section 14 of the Constitution includes 'informational privacy'.

2.2.2.3 *Intention*

The general rule is that intent, or *animus inuriandi*, is required by the common law before liability can be established. This means that the perpetrator must have directed his or her will to violating the privacy of the prejudiced party, in the knowledge that the violation would be wrongful. In the absence of any of these elements, there is no intent.⁷¹

⁶⁶ Monitoring Prohibition Act 77 of 1995.

⁶⁷ Neethling, Pogieter & Visser *Law of Delict* 34.

⁶⁸ *Bernstein v Bester* NO 1996 (2) SA 751 (CC).

⁶⁹ *Bernstein v Bester* NO 1996 (2) SA 751 (CC) 788.

⁷⁰ *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd* 2001 (1) SA 545 (CC) 557.

⁷¹ Neethling, Pogieter & Visser *Neethling's Law of Personality* 57.

In *NM v Smith (Freedom of Expression Institute intervening as Amicus Curiae)*,⁷² Justice O'Regan, delivering a majority judgment, considered whether the court should extend the common-law requirement for liability under the *actio iniuriarum*, to include negligent infringement of privacy.⁷³

Neethling is also of the view that the collection and use of personal information (especially by electronic databases) create so enormous a threat to the privacy of the individual, that it would be fair to hold the data industry accountable, even without having to prove intent in each case. However, as an alternative to restrict liability, he proposes that liability for negligence could also be considered.⁷⁴

2.2.3 Grounds of justification

However, wrongfulness can be excluded by the presentation of a ground of justification. Grounds that are often present in the field of data processing in the employment context are the following:

Consent: If the employee has validly consented to the processing of personal data, there can be no question of wrongfulness.⁷⁵ The consent must be valid, for example, it may be argued that consent for the processing of data is invalid if it is set as a condition of employment, or for the continuation of a contract of employment.⁷⁶

Public interest: Certain public officials and judicial officers are authorised by law to perform certain acts that are justified and therefore not wrongful.⁷⁷ The processing of personal information to protect public interest vests exclusively within the jurisdiction of the state and its organs.⁷⁸

⁷² *NM v Smith* 2007 (5) SA 250 (CC).

⁷³ Van der Walt & Midgley *Delict* 322.

⁷⁴ Neethling 2012 *THRHR* 241-255.

⁷⁵ Neethling, Pogieter, & Visser *Neethling's Law of Personality* 274.

⁷⁶ Neethling, Pogieter & Visser *Neethling's Law of Personality* 274.

⁷⁷ Van der Walt & Midgley *Delict* 136.

⁷⁸ Neethling, Pogieter & Visser *Neethling's Law of Personality* 277

An employer does not act wrongful if he or she performs an act while exercising a statutory authority.⁷⁹ Harmful conduct authorised by statute, is thus reasonable and consequently lawful. For the person to rely on this ground of justification certain requirements must be complied with: firstly, the statute must authorise the infringement of the particular interest concerned; and secondly, the conduct must not exceed the bounds of the authority conferred by the statute.⁸⁰ Lastly, the protection of public interest must take place in a reasonable manner, which means that the information must be reasonably necessary and related to the statutory purpose.⁸¹ For example, although it is wrongful for an employer to publish private facts about an employee, the wrongfulness will fall away if the employee concerned is a public figure and publication of facts about his or her private life is in the public interest.⁸²

Mistake: If the defendant did not intend to invade the plaintiff's privacy, or was unaware of the wrongfulness of his or her act, this would rebut the presumption of *animus injuriandi*. In *Maisel v Van Naeren*⁸³ it was held that to prove a *bona fide* mistake, the defendant must show that, subjectively, both a mistake of a fact and a mistake of law exist.

2.2.4 Remedies

The generally accepted remedies for the invasion of a personality interest such as privacy or identity are, under common law, an interdict and a claim under the *actio iniuriarum* for non-patrimonial loss. If patrimonial loss occurs because of the *iniuria*, that may be claimed under the *actio legis Aquiliae*.

Interdict: An interdict may be obtained to prevent the intentional, wrongful processing of personal information, or to stop the further wrongful processing of personal information.⁸⁴

Requirements for an interdict

⁷⁹ Neethling, Pogieter & Visser *Law of Delict* 95.

⁸⁰ Neethling, Pogieter & Visser *Law of Delict* 96.

⁸¹ Roos *Data (privacy) Protection* 34.

⁸² Skosana *Privacy and Identity* 58.

⁸³ *Maisel v Van Naeren* 1960 (4) SA 836 (C) 840.

⁸⁴ *Finacial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 SA (A) 451.

In order to obtain an interdict the applicant must show that he or she has a clear right, has suffered actual injury, and that no other satisfactory remedy is available.⁸⁵

Actio iniuriarum: A claim based on the *actio iniuriarum* may be instituted for non-patrimonial loss sustained due to the wrongful and intentional processing of personal information.⁸⁶ A claim based on non-patrimonial loss for injury caused to an employee's personality as the result of the wrongful intentional processing of personal data may be claimed with the *actio iniuriarum*.⁸⁷

Actio legis Aquiliae: Patrimonial loss sustained as the result of the wrongful, intentional or negligent processing of personal information⁸⁸ may be claimed with the *actio legis Aquiliae*.

2.2.5 Conclusion

Although South African common law has a well-developed level of protection for the right to privacy and identity in the law of delict, this protection is not adequate when personal information is processed; the common-law principles do not give the individual active control over personal information that is being processed.⁸⁹ Roos points out that the traditional delictual principles are useful in determining whether or not the processing of personal information has taken place lawfully. However, these principles do not ensure that the data subject knows that his or her personal information has been collected, nor does it ensure that the data subject has access to that information, or that he or she is able to rectify incorrect information.⁹⁰ Furthermore, common-law principles do not make provision for issues arising from the cross-border flow of personal information.⁹¹ As these principles are inadequate in ensuring the protection of the privacy of personal information

⁸⁵ *Seglogelo v Seglogelo* 1914 AD 211 [227].

⁸⁶ Neethling, Pogieter, & Visser *Law of Delict* 250.

⁸⁷ Naude *Data Protection* 9

⁸⁸ Neethling, Pogieter, & Visser *Law of Delict* 251.

⁸⁹ Van der Merwe et al *Information Communications* 422.

⁹⁰ Roos 2007 *SALJ* 423.

⁹¹ Neethling 2012 *THRHR* 244.

in the current information technology era, the legislature must remedy the deficiencies legislatively. This aspect is discussed below.

2.3 CONSTITUTIONAL PROTECTION OF PRIVACY

2.3.1 Introduction

Several sections in the Constitution are relevant to the topic under discussion.

Section 2 of the Constitution provides that:

This Constitution is the supreme law of the Republic; law or conduct inconsistent with it is invalid, and the obligations imposed by it must be fulfilled.

This section is of utmost importance in that it confers powers on the Constitutional Court to declare any law invalid if it is found to be inconsistent with the provisions of the Bill of Rights in Chapter 2 of the Constitution.

Section 8 of the Constitution provides that:

- (1) The Bill of Rights applies to all law, and binds the legislature, the executive, the judiciary and all organs of state.
- (2) A provision of the Bill of Rights binds a natural or a juristic person if, and to the extent that, it is applicable, taking into account the nature of the right and the nature of any duty imposed by the right.
- (3) When applying a provision of the Bill of Rights to a natural or juristic person in terms subsection (2), a court -
 - (a) in order to give effect to the Bill, must apply, or if necessary develop, the common law to the extent that the legislation does not give effect to that right; and
 - (b) may develop the rules of the common law to limit the right, provided that the limitation is in accordance with section 36(1).
- (4) A juristic person is entitled to the rights in the Bill of Rights to the extent required by the nature of the rights and the nature of that juristic person.

These provisions are important in that they illustrate that all laws and bodies in South Africa, including employers, are subject to the Constitution with constitutional supremacy as our point of departure.

Section 14 provides that:

Everyone has the right to privacy, which includes the right not to have:

- (a) Their person or home searched;
- (b) Their property searched;
- (c) Their possessions seized; or
- (d) The privacy of their communications infringed.

The provisions of this section protect the right to privacy. According to Currie and De Waal,⁹² section 14 of the Constitution has two parts: “the first part guarantees a general right to privacy, the second protects against specific infringements of privacy, namely search and seizures and infringement of the privacy of communications”.⁹³ The general right to privacy protects against unauthorised processing of personal information.⁹⁴

Section 14 protects the privacy of personal information to the extent that it limits the ability to gain, publish, disclose, or use information about others. Like the common law, it does not address the privacy challenges or threats posed by the developments in technology.⁹⁵ In other words, it does not ensure that the data subject is aware that his or her personal information has been collected,⁹⁶ and does not give him or her active control over personal information that is being processed.⁹⁷

The Bill of Rights binds the state, but also binds natural and juristic persons. In other words, it has both vertical and horizontal application.⁹⁸ It is of particular interest to look at juristic persons as this dissertation relates to a relationship that is often between a juristic person and a natural person – ie, a relationship between an employer and an employee. (An employer may, of course, also be a natural person.)

⁹² Currie & de Waal *Bill of Rights* 317.

⁹³ Currie & de Waal *Bill of Rights* 317.

⁹⁴ Van der Merwe et al *Information communications* 41.6

⁹⁵ Currie & de Waal *Bill of Rights* 317.

⁹⁶ Roos 2007 *SALJ* 423.

⁹⁷ Neethling, Pogietter & Visser *Neethling's Law of Personality* 278.

⁹⁸ SALRC Privacy and Data Protection discussion paper 109 October 2005.

Juristic persons are also entitled to the fundamental rights in the Bill of Rights – including the right to privacy – to the extent that these rights can be applicable to them.⁹⁹ Both the vertical and horizontal application of fundamental rights can be direct or indirect.¹⁰⁰ Direct vertical application requires the state to respect the fundamental rights in the Bill of Rights, unless such an infringement is reasonable and justifiable in terms of the limitation clause in section 36 of the Constitution. Direct horizontal application requires the court to give effect to applicable fundamental rights by applying and developing the common law. Indirect application of the Bill of Rights requires that all legal rules, principles, or norms be subject to the basic values in the Bill of Rights, and be in accordance with the spirit, object, and purport of the Bill of Rights.¹⁰¹

The provisions of section 14 of the Constitution, according to Currie and De Waal, prohibit the unauthorised processing of employees' personal information.¹⁰²

2.3.2 Elements for constitutional liability

A breach of section 14 of the Constitution is regarded as an unlawful invasion of privacy, and the onus vests in the person or body breaching it to establish that the breach is justifiable in terms of section 36.¹⁰³

The Constitutional Court has pointed out that whereas common law establishes unlawful infringement of privacy in a single enquiry, under the Constitution a two-fold inquiry is required.¹⁰⁴ In the case of an alleged constitutional invasion of privacy, the following two questions need to be considered:

⁹⁹ Pienaar 1998 *PER* 1.

¹⁰⁰ Neethling, Pogieter & Visser *Law of Delict* 16.

¹⁰¹ Neethling, Pogieter & Visser *Law of Delict* 20.

¹⁰² Currie & de Waal *Bill of Rights* 159

¹⁰³ Constitution s 36.

¹⁰⁴ *Bernstein v Bester* NO 1996 (2) SA 751 (CC) 71.

- (a) Has the act or conduct infringed the right to privacy in the Constitution? In order to establish an infringement of the constitutional right to privacy, the plaintiff must show that he or she had a subjective, but objectively reasonable, expectation of privacy.¹⁰⁵
- (b) If this expectation is proved, is such an infringement justifiable in terms of the limitation clause?¹⁰⁶

According to section 36(1) of the Constitution, a right may be limited only in terms of a law of general application, and only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality, and freedom. Relevant factors that should be taken into account include: the nature of the right; the importance of the purpose of the limitation; the nature and the extent of the limitation; the relation between the limitation and its purpose; and less restrictive means available to achieve the purpose. The Constitutional Court has pointed out that these factors are not exhaustive, and that the court must engage in a balancing exercise and arrive at an overall judgement on proportionality and should not adhere mechanically to a sequential checklist.¹⁰⁷

2.3.3 Constitutional remedies

In the case of a constitutional infringement of privacy, a court may grant appropriate relief. There are three categories of constitutional remedies: constitutional damages; interdicts; and declarations of invalidity.¹⁰⁸

2.3.3.1 *Constitutional damages*

A court can award damages as a remedy for the violation of a fundamental right, including the right to privacy.¹⁰⁹ These damages should be aimed at effectively redressing the wrong

¹⁰⁵ *Bernstein v Bester* NO 1996 (2) SA 751 (CC) 75.

¹⁰⁶ Constitution s 36.

¹⁰⁷ *S v Manamela* 2000 (1) SACR 414 (CC) 430.

¹⁰⁸ *Currie & de Waal Bill of Rights* 159.

¹⁰⁹ *Currie & de Waal Bill of Rights* 200

suffered by the plaintiff, deterring future constitutional infringements, and ensuring future compliance. In principle, constitutional remedies should be progressive, community orientated, and structural.¹¹⁰

2.3.3.3 *Interdicts*

(a) Interim interdict

Interim relief aims at preserving the status quo pending the final adjudication of a dispute. In general, in constitutional litigation, High Courts apply the common-law criteria; an interdict can be granted where the applicant has demonstrated the requirements, namely: a *prima facie* right; or a well-founded apprehension of irreparable harm if the interim relief is not granted; a balance of convenience; and no other remedy available to the applicant.¹¹¹

(b) Final interdict

A final interdict can be either prohibitory or mandatory. A prohibitory interdict prevents a future course of action. A mandatory interdict attempts to correct the effect of past wrongs, ie, to eradicate inconsistency between the Bill of Rights and societal practices.¹¹²

2.3.4 Limitation of the right to privacy

The constitutional right to privacy is not an absolute right; it is subject to the limitation clause, ie, section 36 of the Constitution.¹¹³ This section provides for the test that needs to be satisfied in order for the infringement of the right to be permitted. As previously indicated, the right to privacy is subject to limitation by a law of general application, to an extent that it is reasonable and justifiable in an open and democratic society, based on

¹¹⁰ McQuoid-Mason *Privacy* 16.

¹¹¹ Currie & de Waal *Bill of Rights* 198.

¹¹² Currie & de Waal *Bill of Rights* 198.

¹¹³ Constitution s 36.

human dignity, equality, and freedom, taking into account all relevant factors including those mentioned in this section.

*S v Makwanyane*¹¹⁴ is the landmark case on the issue of how, when, and why the Constitutional Court should allow the limitation of a fundamental right. In the *Makwanyane* case, the court held that:

The limitation of constitutional rights for a purpose that is reasonable and necessary in a democratic society involves the weighing up of competing values, and ultimately an assessment based on proportionality.¹¹⁵ This is apparent in section 33(1) of the interim Constitution.¹¹⁶ The fact that different rights have different implications for democracy, and in the case of our Constitution for an open and democratic society based of freedom and equality, means that there is no absolute standard which can be laid down for determining reasonableness and necessity. Principles can be established, but the application of those principles to particular circumstances can only be done on a case-by-case basis.

The court emphasised that there cannot be a set rules as to when the court will allow the limitation of a right – every case must be assessed on its individual merits.

*S v Bhulwana*¹¹⁷ summaries the provisions of the limitation clause:

In sum, therefore, the court places the purpose, effects and importance of the infringing legislation on one side of the scale and the nature and effect of the infringement caused by the limitation on the other.

The purpose of any given law or Act is to be weighed against the importance of the fundamental right it stands to infringe.¹¹⁸

¹¹⁴ *S v Makwanyane* 1995 (3) SA 391 (CC), 1995 (6) BCLR (CC). This case dealt with s 33 of the interim Constitution of the Republic of South Africa Act 200 of 1993 (the Interim Constitution). However, the same principles apply to s 36 of the Constitution, 1996.

¹¹⁵ *S v Makwenyane* 1995 (3) SA 391 (CC), 1995 (6) BCLR (CC).

¹¹⁶ Interim Constitution.

¹¹⁷ *S v Bhulawa* 1996 (1) SA 388 (CC) 18.

¹¹⁸ Beech 2005 ILJ 655.

2.4 INTERNATIONAL RECOGNITION OF THE RIGHT TO PRIVACY

The right to privacy is recognised in various international instruments, and has been made enforceable by article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).¹¹⁹

Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms¹²⁰ states that:

- (1) Everyone has the right to respect for his private and family life, his home and his correspondence
- (2) There shall be no interference by public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of the national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Furthermore, it is important to note that the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) created the European Commission of Human Rights and the European Court of Human Rights to oversee the enforcement of the ECHR. Both these structures have delivered significant judgments on the meaning of protecting the right to privacy as stated in article 8.¹²¹

The international instrument referred to above, is relevant to the current discussion, but because of the limits on the short dissertation, cannot be discussed in detail. It will, however, be referred to when necessary.¹²²

¹¹⁹ Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms 4 November 1950.

¹²⁰ Council of Europe European Convention for the Protection of Human Rights and Fundamental Freedoms 4 November 1950.

¹²¹ Privacy and Data Protection Project 124 Discussion Paper 109 (2005) 51.

¹¹⁶ *Bygave Data Protection Law* 30.

2.5 CONCLUSION

Based on the preceding discussion in this chapter, it can be said that despite difficulties in defining the concept of privacy, the right to privacy has still been recognised both internationally and domestically as one of the most important human rights. It is protected when an individual has a reasonable expectation that his or her right will be observed in a particular situation.

Furthermore, the right to privacy provides the basis for seeking a remedy against unlawful interference by outsiders. The most common of these violations relate to the right not to have persons or their homes searched; their property searched; their possessions seized; or the privacy of their communications infringed. However, the right to privacy does not adequately address issues related to the protection of online information or data stored electronically. This is because the data subject (employee in our context) is not accorded active control over his or her personal information.¹²³ Roos points out that common-law principles cannot ensure, for example, that the data subject receives notification of the fact that his or her personal information is being collected or is being processed, or that he or she has the right to access, update, and to correct the information.

With the previous discussion as background, the following chapter focuses on the legislation and case law on data privacy within the employment context in South Africa.

¹²³ Roos 2007 SALJ 423.

Chapter 3

Data privacy legislation in South Africa

3.1 INTRODUCTION

The previous chapter dealt with the nature and the scope of the right to privacy in South African law, specifically as it applies in the employment context. Reference was also made to international instruments protecting the right to privacy. This chapter analyses South African legislation applicable to the privacy of electronic communications and personal information in the workplace.

Common law and a labour-law statute, the Labour Relations Act,¹²⁴ regulate the employment relationship. Grogan argues that “there is an implied term that the parties to the contract shall respect each other’s privacy”.¹²⁵ He further states that the contracts concluded between employers and employees place an obligation on each party to respect the parties’ right to privacy. In South Africa, there are laws that protect individuals’ right to privacy when their information is being processed, as well as the privacy of their communications. These laws are relevant to this discussion in order to trace how legislation developed to cater for the needs of an employee’s right to privacy.

¹²⁴ Labour Relations Act 66 of 1995.

¹²⁵ Grogan *Workplace Law* 53.

3.2 LABOUR RELATIONS ACT

3.2.1 Introduction

The main purpose of this piece of legislation is to regulate the relationship between the employer and an employee.

Section 1 of the Act provides that:

The purpose of this Act is to advance economic development, social justice, labour peace and the democratisation of the workplace by fulfilling the primary objects of this Act, which are –

- (a) to give effect to and regulate the fundamental rights conferred by section 23 of the Constitution of the Republic of South Africa, 1996;
- (b) to give effect to obligations incurred by the Republic as a member state of the International Labour Organisation;
- (c) to provide a framework within which employees and their trade unions, employees and employers and employers organisations can -
 - (i) collectively bargain to determine wages, terms and conditions of employment and other matters of mutual interest; and
 - (ii) formulate industrial policy...

Section 3 provides that:

Any person applying this Act must interpret its provisions -

- (a) to give effect to its primary objects;
- (b) in compliance with the Constitution; and
- (c) in compliance with the public international law obligation of the Republic...

Furthermore, Schedule 8,¹²⁶ item 1(3) provides that:

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 businesses. While employees should be protected from arbitrary action, employers are entitled to satisfactory conduct and work performance from their employees.¹²⁷

¹²⁶ Schedule 8 contains a Code of Good Practice for Dismissals.
¹²⁷ Act 66 of 1995, Schedule 8 1(3).

This provision is of particular interest as it reflects on the balancing of the employers' interest in protecting their business operations, versus the employees' right to privacy in the workplace when personal information is processed.¹²⁸

3.2.2 The need for an electronic communications policy

In order to manage the risk of the infringement of the employee's right to privacy by the employer, the latter should have an electronic communications policy in place. Compliance with the policy should be monitored and appropriate action taken in cases of non-compliance.¹²⁹

In determining the content of the policy and how it should be introduced, the employers should refer to Schedule 8 to the Labour Relations Act¹³⁰ which contains the code of good practice (LRA Code), which sets out the factors to be considered in disciplinary proceedings where an employer seeks to rely on the policy. These are:

- Was the employee aware of the rules and standards?
- Were the rules or standards valid and reasonable?
- Were the rules or standards applied consistently?¹³¹

These three factors deserve further attention.

(a) *Was the employee aware of the rules and standards?*

In terms of the LRA Code, the objective of a rule must be to create certainty and consistency in the application of discipline. This means that the standard of the conduct

¹²⁸ Mabeka *Conduct of an Employer* 89.

¹²⁹ Papadopoulos & Snail *Cyber Law@SA* 179.

¹³⁰ Act 66 of 1995.

¹³¹ Papadopoulos & Snail *Cyber Law@SA* 178.

must be clear, and must be available to employees in a manner that is easily understood.¹³²

The policy should be explicitly incorporated in the employee's contract of employment. However, in the case of *Warren Thomas Griffiths v VWSA*,¹³³ an employee was dismissed because he willfully disobeyed instructions and abused company facilities and internet services. The CCMA was of the view that it is possible to charge an employee with a disciplinary offence, notwithstanding that the offence is not specifically included in the employer's disciplinary code. In *Bamford and Others v Energizer SA Limited*,¹³⁴ which was referred to private arbitration, the arbitrator held that even in the absence of any express rules setting out what type of material could be trafficked on the company's email system, the emails in question did not belong in the workplace.

(b) *Were the rules or standards valid and reasonable?*

In order to assess whether the rules were valid and reasonable, one needs to consider whether the right to privacy existed in the workplace, and whether it was reasonable to limit that right.¹³⁵ As mentioned in the previous chapter, the right to privacy does exist in the workplace. This means that only the reasonableness of the limitation must be determined.

In *Bernstein v Bester NO*,¹³⁶ Ackerman J analysed the concept of privacy and held that privacy is acknowledged in the purely personal realm, but as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks accordingly.¹³⁷ He further held that the scope of the constitutional

¹³² Papadopoulos & Snail *Cyber Law@SA* 179.

¹³³ *Warren Thomas Griffiths v VWSA* Case NO EC 16714 unreported (CCMA 22 June 2000).

¹³⁴ *Bamford and Others v Energizer SA Limited* 2001 12 BALR 1251 (P).

¹³⁵ Papadopoulos & Snail *Cyber law@SA* 180.

¹³⁶ *Bernstein v Bester NO* 1996 (2) SA 751 (CC) 71.

¹³⁷ *Bernstein v Bester NO* 1996 (2) SA 751 (CC) 792G.

right to privacy is limited and extends only to aspects of a person's life or conduct about which a legitimate expectation of privacy can be honoured.¹³⁸

(c) *Were the rules or standards applied consistently?*

*Gouws v Score/Price & Pride Furnishers*¹³⁹ illustrates the importance of ensuring that the rules are applied properly and consistently. In this case, the CCMA held that the dismissal of an employee was substantively unfair in circumstances where other employees were not disciplined, as this created the impression that they condoned the employees' activities. The commissioner held that employers must be consistent in the application of their rules, and that if they fail to discipline one employee for contravening a rule, or allow him or her to do so, they cannot later discipline other employees for contravening the same rule.

(d) *Electronic communication policy*

There should be an electronic communication policy in place and employees must agree to the policy in their employment contracts. It is advisable that every employee receive a copy of the policy at the beginning of his or her employment.¹⁴⁰ The employer should request that employees sign an acknowledgement that they have read and understood the policy and their obligation under it, in order to avoid uncertainty and inconsistency.

The policy should act as a detailed guide explaining the responsibilities of employees when dealing with electronic material in a clear, concise, and readily comprehensible form.¹⁴¹

The content of the policy will be determined by the employer's practices. The LRA code provides that employers should adopt disciplinary rules that establish the standard of

¹³⁸ *Bernstein v Bester* NO 1996 (2) SA 751 (CC) 795D.

¹³⁹ *Gouws v Score/Price & Pride Furnishers* 2001 11 BALR 1155 (CCMA).

¹⁴⁰ De Stadler et al *Protection* 93.

¹⁴¹ De Stadler et al *Protection* 93.

conduct required of their employees. If personal use of electronic resources is allowed, the employer's policy should be clear on the nature and the extent of what is allowed.¹⁴² To protect the company, this policy should further make it compulsory for the employee to attach a disclaimer to any emails sent externally.¹⁴³

Based on the discussion above, it can be said that creating a workplace culture of compliance is a sound move as regards electronic communication. Where the employer has an electronic policy in place, and the employee has agreed to and signed an acknowledgement that he or she has read and understood that policy and his or her obligations under it, simplifies the position of both employer and employee where problems regarding electronic communication arise.

3.3 PROMOTION OF ACCESS TO INFORMATION ACT 2 OF 2000

The Promotion of Access to Information Act (the PAIA)¹⁴⁴ is essentially a freedom of information Act¹⁴⁵ and it is not primarily concerned with data privacy.¹⁴⁶ It was enacted to give effect to an individual's constitutional right of access to any information¹⁴⁷ held by the state or any other person, which is required for the exercise or protection of any right.¹⁴⁸ This Act gives the data subject limited control over his or her personal information in the following ways:

- It allows individuals access to records containing their personal information in both the public and private sectors.¹⁴⁹

¹⁴² Papadopoulos & Snail *Cyber law@SA* 280.

¹⁴³ Papadopoulos & Snail *Cyber law@SA* 280.

¹⁴⁴ Promotion of Access to Information Act 2 of 2000 (the PAIA).

¹⁴⁵ Van der Merwe et al *Information Communications* 442.

¹⁴⁶ However, the link between privacy and access to information is recognised in s 9(b) of the Act which justifies the Act's limitation of this constitutional right by, inter alia, "the reasonable protection of privacy" (Currie & Klaaren *Promotion of Access* 18 para 2.5)

¹⁴⁷ Constitution s 32.

¹⁴⁸ Preamble to the PAIA.

¹⁴⁹ The PAIA s 11 (public bodies) and s 50 (private bodies).

- It requires public and private bodies to take reasonable steps to establish adequate internal measures for the correction of personal information until legislation providing for such correction comes into effect.
- It prohibits the disclosure of a record if it would involve the unreasonable disclosure of personal information relating to a third party.¹⁵⁰

The PAIA¹⁵¹ is relevant in that it grants an employee access to information relating to him or her held by the employer and obtained for a purpose relating to the employment relationship.¹⁵²

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

The RICA was drafted in response to increasing developments and diversity in communication technology, the globalisation of the telecommunications industry, and the convergence of the telecommunication, broadcasting, and information technology industries, which includes satellites, computers, cellular technology, electronic mail technology, and electronic processing of information and data. With the regulation of the interception of electronic communications through the RICA,¹⁵³ the legislature intended, inter alia, to protect employees' right to privacy in the workplace by setting out conditions that employers must fulfil before intercepting their employees' electronic communications.

¹⁵⁰ The PAIA s 34 (public bodies) and s 63 (private bodies).

¹⁵¹ Act 2 of 2000.

¹⁵² The POPI Act does not regulate access to information. The PAIA regulates access to information under s 23.

¹⁵³ Section 1 of the Act defines interception as the aural or other acquisition of the contents of any communication through the use of any means, including any interception device, so as to make some or all of the contents of the communication available to a person other than the sender or recipient of that communication.

3.4.1 Prohibition on interception

Section 2 of the RICA¹⁵⁴ contains a general prohibition on interception. In terms of this section, an employer may not intentionally intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission. Any interception in contravention of section 2 may constitute a criminal offence, which carries a minimum fine of R 2 million or a maximum term of imprisonment of ten years.¹⁵⁵

In terms of the Act¹⁵⁶ the 'interception' of a communication means the acquisition of the contents of any communication so as to make that content, or some of it, available to a person other than the sender or intended recipient. Interception further includes monitoring, inspection of the contents, and its diversion to any other destination.

This means that in an employment context an employer may not intentionally, and without the knowledge or permission of the employee, intercept a communication that has been, or is intended to be, transmitted by telephone or any other electronic device . Furthermore, an employer may not intentionally intercept the conversation or communication of an employee by means of an electronic device. However, the Act allows interception of communications under certain specific circumstances. It is to these situations that we now turn, insofar as they may apply to the employer-employee relationship.

3.4.2 Interception of communications permitted by the RICA

3.4.2.1 *Interception of a communication by a party to the communication*

In terms of section 4 of the RICA, any person who is one of the parties to a communication, may intercept that communication, provided it is not for the purpose of committing an

¹⁵⁴ Act 70 of 2002.

¹⁵⁵ The RICA s 49(1).

¹⁵⁶ The RICA s 1.

offence. In other words, an employer who is a party to a communication with an employee may intercept that communication.

Beech has pointed out that the Act does not define a 'party'. The term will, therefore, bear its ordinary meaning, which would include the sender, recipient, and any other person to whom the communication is sent (copied).¹⁵⁷ One could also argue that by providing the relevant communication system, the employer is a party to any communication sent or received on that system.¹⁵⁸ It is, however, unnecessary to rely on this untested argument in the employment context, as the Act provides an exception specific to the employment context.¹⁵⁹ Furthermore, the employer should respect its employees' right to privacy as regards the contents of email messages and other form of internet communication, unless there are grounds to suspect that some form of abuse is taking place.¹⁶⁰ An example would be when the employee has alleged in an email that a colleague is creating a hostile working environment. The employer would certainly have good grounds for examining the contents of email messages in detail to establish whether there is a basis for disciplinary action.¹⁶¹

3.4.2.2 *Interception of a communication with the consent of the party to communication*

A person (such as an employee) may consent to the interception of his or her communications.

Section 5(1)¹⁶² provides that:

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 interception, unless such communication is intercepted by such person for the purpose of committing an offence.

¹⁵⁷ Beech 2005 *ILJ* 650.

¹⁵⁸ Beech 2005 *ILJ* 656.

¹⁵⁹ The RICA s 6(1).

¹⁶⁰ Modiba 2003 *Merc LJ* 364.

¹⁶¹ Modiba 2003 *Merc LJ* 365.

¹⁶² The RICA s 5(1).

It is clear that the consent must be in writing and must be given prior to the interception. Any one of the parties to the communication may give the consent.

A general consent by an employee as part of his or her terms and conditions of employment in an employment contract, policy, or other relevant document relevant to employment, allowing the employer to intercept his or her personal communications, may be regarded as prior written consent as required by section 5 of the RICA. However, it would be reasonable for the employer to include a 'general consent to interception' as part of the employment contract, to ensure that employees understand the ambit of what they are agreeing to by giving their consent.¹⁶³

3.4.2.3 *Interception of an indirect communication pertaining to carrying on of a business*

Section 6 has specific application in the work environment and the employer-employee relationship. It relates to the monitoring or accessing employees' emails, recording employees' telephone conversations, and monitoring what websites employees access.

Section 6 provides that:

- (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 place in the course of the carrying on of that business,in the course of its transmission over a telecommunication system.
- (2) 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 consent of, the system controller¹⁶⁴
 - (b) for purposes of -
 - (i) monitoring or keeping a record of indirect communications¹⁶⁵ -

¹⁶³ Padayachee *Employee's Right to Privacy* 56.

¹⁶⁴ The term system controller is defined in s 1. In the case of a juristic person, it refers to the chief executive officer or equivalent officer of the juristic person, or any person duly authorised by such person.

¹⁶⁵ The Act defines indirect marketing in Chapter 1 as the transfer of information, including a message or any part of a message, whether in the form of speech, music or other sounds, data,

- (aa) in order to establish the existence of facts;
- (bb) for purposes of investigating or detecting the unauthorised use of that telecommunication system; or
- (cc) where that is undertaken in order to secure, or as an inherent part of, the effective operation of the system;

or

- (ii) monitoring indirect communications made to a confidential voice- telephony counselling or support service which is free of charge, other than the cost, if any, of making a telephone call, and operated in such a way that the users thereof may remain anonymous if they so choose;
- (c) if the telecommunication system concerned is provided for use wholly or partly in connection with that business; and
- (d) if the system controller has made all reasonable efforts to inform in advance a person, who intends to use the telecommunication system concerned, that indirect communications transmitted by means thereof may be intercepted or if such indirect communication is intercepted with the express or implied consent of the person who uses that telecommunication system.

'Indirect communication' is defined in the RICA as

the transfer of information, including a message or any part of a message in the form of speech, music, or other sounds; data; text; visual images, whether animated or not; signal; or radio frequency spectrum; or in any other form or any combination of forms, that is transmitted in whole or in part by means of a postal services or telecommunication.

It is important to note that section 6(1) states that "any person may, in the course of carrying on of any business, intercept any indirect communication ... in the course of its transmission over a telecommunication system." From the words 'in the course of its transmission', it is clear that interception of a communication may only take place in terms of section 6 if the interception is done whilst the communication is in the process of travelling over the internet or corporate intranet.¹⁶⁶ In terms of section 6, the employer must also ensure that a reasonable effort is made to inform the employee who uses the email, that his or her communications might be intercepted. The interception must also be by or with the knowledge of the system administrator.

It is clear that section 5 of the Act under discussion limits the employee's constitutional right to privacy of his or her communications provided in section 14(d). The latter section states that everyone has the right to privacy, which includes the right not to have the

text, visual images, whether animated or not, signals or radio frequency spectrum or in any other form.

¹⁶⁶ Pistorius 2009 *PER* 166.

privacy of his or her communications infringed,¹⁶⁷ in that it provides that any person, including an employer, may intercept an employee's electronic communications *if the employee consents*. Section 6 similarly limits the right of employees to the privacy of their communications in that it allows the employer to intercept the indirect communications of employees in specifically defined circumstances.

As the owner of electronic communication tools provided to the employees for business or work-related purposes and in the interests of efficiency, the employer has a right to protect its property and business interests. This may potentially limit the employees' right to privacy provided the action taken is in accordance with sections 5 and 6 of the RICA.

3.5 PROTECTION OF PERSONAL INFORMATION ACT

3.5.1 Introduction

The main objective of the Protection of Personal Information Act (the POPI Act)¹⁶⁸ is to give effect to the right to privacy provided for in section 14 of the Constitution.¹⁶⁹ The Act aims to do so while bearing in mind that the constitutional values of democracy and openness, and that economic and social progress within the framework of the information society, require the removal of obstacles to the free flow of information, including personal information.¹⁷⁰ The Act regulates the processing¹⁷¹ of personal information by public and private bodies in ways that will align with international standards.¹⁷² The POPI Act applies to any processing of personal information by either a South African, or a non-South African data controller, using equipment in South Africa. This, of course, includes the processing of personal information in the workplace.¹⁷³

For the purpose of this discussion, it is reasonable to infer that the employer would be the responsible party (or data controller), since it is the employer who determines the reason

¹⁶⁷ Constitution s 14(d).

¹⁶⁸ Protection of Personal Information Act 4 of 2013

¹⁶⁹ Constitution of the Republic of South Africa, 1996.

¹⁷⁰ Van der Merwe et al *Information Communications* 234.

¹⁷¹ See footnote 32 for the meaning of processing.

¹⁷² Van der Merwe et al *Information Communications* 435.

¹⁷³ Van der Merwe et al *Information Communications* 435.

for the processing of personal information. Furthermore, employers are obliged to maintain records of personal information on their employees in terms of section 3(1)(a) of the Basic Conditions of Employment Act.¹⁷⁴ This section stipulates that an employer must keep a record containing information on its employees' names, occupations, time worked, remuneration paid, date of birth, and any other prescribed information. Therefore, it is clear that in most workplace situations, the responsible party would be an employer.

3.5.2 Provisions in the POPI Act relevant to this discussion

It is important for employers to look to their legal obligations regarding the processing of personal information in the workplace, and to review whether they are taking adequate measures to safeguard their employees' personal data. This can be done by simply understanding their legal obligations as required under the POPI Act.¹⁷⁵

Section 4 of the POPI Act requires that certain conditions or minimum requirements be met in order for the processing to be lawful.¹⁷⁶ These requirements are as follows:

*Accountability:*¹⁷⁷ This principle requires the employer, as data controller, to ensure compliance with the principles of data protection. It also ensures that the final responsibility for compliance rests with the employer, even in instances where the employer has entrusted the information collection process to an employee or a third party.¹⁷⁸

Processing limitation: This entails that processing of personal information be done lawfully and in the manner that does not infringe on the privacy of the data subject.¹⁷⁹ Further, the amount of personal information processed should be limited to that necessary to achieve

¹⁷⁴ Basic Conditions of Employment Act 75 of 1997.

¹⁷⁵ Act 4 of 2013.

¹⁷⁶ Section 4 of Act 4 of 2013.

¹⁷⁷ Section 8 of Act 4 of 2013.

¹⁷⁸ Roos 2006 *CILSA* 121.

¹⁷⁹ Section 1 of the Act defines 'data subject' as the person to whom personal information relates.

the purposes for which the information is processed.¹⁸⁰ Section 11 of the POPI Act provides that information may be processed only if one of a specific set of conditions is present. These conditions are:

- (a) The data subject has consented to the processing.
- (b) The processing is necessary for the performance of a contract or agreement to which the data subject is party.
- (c) The processing complies with an obligation imposed by law on the responsible party¹⁸¹ to protect the legitimate interests of the data subject.
- (d) The processing is necessary for the proper performance of a public law duty by a public body.¹⁸²

Purpose specification: Personal information must be collected for a specific, clearly defined, and lawful purpose related to the function and activity of the responsible party.¹⁸³ The purpose of processing is determinative of every aspect of the processing of the personal information including: the nature of the information that may be collected; the length of time the data may be retained; whether and what further processing may be performed; and the disclosure of information to third parties.¹⁸⁴ Therefore, the employer may only process personal information for specified and lawful purposes. Furthermore, personal information may not be processed in a manner inconsistent with these lawful and legitimate purposes.¹⁸⁵

Further processing limitation: The further processing of personal information must be in accordance with the purpose for which the information was collected.¹⁸⁶

¹⁸⁰ Van der Merwe et al *Information Communications* 372.

¹⁸¹ Section 1(e) of Act 4 of 2013 defines the 'responsible party' as a public or private body or any other person which alone or in conjunction with others, determines the purpose of and means for processing personal information.

¹⁸² Section 11 of Act 4 of 2013.

¹⁸³ Section 13 of Act 4 of 2013.

¹⁸⁴ Roos 2006 *CILSA* 111.

¹⁸⁵ Bygrave *Data Protection* 61.

¹⁸⁶ Section 15 of Act 4 of 2013.

*Information quality:*¹⁸⁷ Personal information should be relevant, accurate, and up to date with respect to the purposes for which it is to be processed.¹⁸⁸

*Openness:*¹⁸⁹ This principle ensures that the employee is notified when his or her personal information is processed; is informed of the purpose for which that information is processed; is aware of the identity of the recipients of his or her personal information; as well as the identity and regular address of the employer.¹⁹⁰

Security safeguards: In order to comply with this principle, the employer must ensure that personal information is protected by reasonable security safeguards against risks such as loss, unauthorised processing, destruction, use, or disclosure.¹⁹¹

*Data subject participation:*¹⁹² Employees should be allowed to participate in, and have a measure of influence over, the processing of their personal information.¹⁹³ They should have a right to access their data, request correction of incorrect data, and object to specific processing activities involving their personal information.

It is difficult to counterbalance the employer's need for a productive and safe work environment, and the employee's right to privacy if the organisation does not have a data protection policy in place to guard against unauthorised processing.

Section 3 of the Act¹⁹⁴ provides that any other legislation that is stricter than the Act must still apply. In other words, employers cannot rely on the POPI Act alone for the development of their privacy policies and programmes, but must also consider other relevant legislation. Other Acts that stand to be considered are: the PAIA,¹⁹⁵ as an Act promoting freedom of information and data privacy principles – such as access to personal

¹⁸⁷ Section 16 of Act 4 of 2013.

¹⁸⁸ Roos 2006 *CILSA* 114.

¹⁸⁹ Section 19 of Act 4 of 2013.

¹⁹⁰ Roos 2006 *CILSA* 111.

¹⁹¹ Van der Merwe et al *Information Communications* 378.

¹⁹² Section 24 of Act 4 of 2013.

¹⁹³ Roos 2006 *CILSA* 119.

¹⁹⁴ Act 4 of 2013 s 3.

¹⁹⁵ Act 2 of 2000.

information – and prohibiting the granting of access to third party information which could lead to the unreasonable infringement of the privacy of a third party.¹⁹⁶

Section 10 of the POPI Act provides that the responsible parties must obtain the consent of the data subject prior to the processing of his or her information.¹⁹⁷ In the workplace environment, the employee must be actively involved and agree in writing to the processing of his or her personal information.

Section 13 requires the employer to delete personal information that is no longer required, unless it is legally required; to retain the information; or if it is for the purpose of a contract between the employer and the employee; or if the employee has given his or her consent to the retention of the information.¹⁹⁸ Section 13(2) also provides that personal information can be retained for “historical, statistical, or research purposes”.¹⁹⁹

Section 17 of the POPI Act provides that the employer must explain to the employee what his or her information is being used for.²⁰⁰ It has been argued that given the many purposes for which organisations use personal information once it has been collected, it will be difficult to communicate all of this to the data subject in any meaningful way at the time of collection.²⁰¹

Section 22 of the POPI Act implies that the data subject – which in this case is the employee – will be able to ask the employer whether it stores or processes any of his or her personal information, and can submit the request to have his or her information deleted.²⁰² Section 22 further grants the employee the right to request access to his or her information held by the employer.²⁰³

¹⁹⁶ Act 2 of 2000 ss 34 and 63.

¹⁹⁷ Act 4 of 2013 s 10.

¹⁹⁸ Act 4 of 2013 s 13.

¹⁹⁹ Act 4 of 2013 s 13(2).

²⁰⁰ Act 4 of 2013 s 17.

²⁰¹ Chigumba *Employee's Right to Privacy* 32.

²⁰² Act 4 of 2013 s 22.

²⁰³ Act 4 of 2013 s 22.

3.5.3 Action based on the POPI Act

The POPI Act provides data subjects with rights²⁰⁴ and remedies to protect their personal information from being processed unlawfully.²⁰⁵ The Act has far-reaching consequences for responsible parties (employers), and creates strict liability.²⁰⁶ It also creates a form of statutory strict liability by providing in section 99(1) that a civil action for damages may be instituted against the responsible party, whether or not there has been intentional or negligent action on its part.²⁰⁷ Therefore, the employer must ensure that his or her employees comply with the POPI Act as failure by its employee to do so will render the employer accountable.

3.6 Conclusion

Based on the discussion above, it is contended that save for the POPI Act, other legislation in South Africa as discussed above does not provide sufficient protection to data subjects who can no longer control the use of their personal information. However, the Protection of Personal Information Act²⁰⁸ appears progressive and provides mechanisms for the processing of personal information.

²⁰⁴ The right to participate, which gives the data subject a right of access to his or her personal information, the right to correct inaccurate information, and the right to object to the processing of personal information. The right not to be subjected to automated individual decision and the right to object to the processing of information for direct marketing. See Van der Merwe et al *Information Communications* 384.

²⁰⁵ Act 4 of 2013 s 2(c).

²⁰⁶ Act 4 of 2013 s 8.

²⁰⁷ Act 4 of 2013 s 99 (1).

²⁰⁸ Act 4 of 2013.

Chapter 4

United Kingdom perspective

4.1 INTRODUCTION

The protection of personal information is not a new phenomenon in other parts of the world. Accordingly, useful lessons and principles applied in other jurisdiction can be considered in South African law. Section 44 of the POPI Act²⁰⁹ provides that international guidelines which are relevant to the protection of individual privacy, must be taken into account by the Information Regulator when exercising his or her powers. As indicated earlier, this discussion is based on the Data Protection Act, 1998, which was the applicable legislation until its repeal by the new Data Protection Act earlier this year.²¹⁰ The law developed under the 1998 Act remain valid for South Africa who adopted its Act under influence of the 1995 Directive, which was implemented in the UK by the 1998 Data Protection Act. The discussion will also look briefly at the new reforms under the General Data Protection Regulation (the GDPR), which has applied since 25 May 2018.

The focus of this chapter is on the scope and the extent of the right to privacy with respect to the processing of personal data in the workplace environment in the United Kingdom (UK). Accordingly, the chapter provides a discussion and analysis of the legal framework and relevant case law that have contributed to the development of the privacy protection of employees in the UK. The UK was selected for comparison based largely on its adoption of the Data Protection Act.²¹¹ This Act is the UK's implementation of the European Directive 95/46/EC the purpose of which was to create uniform European standards for the collection, storage, and processing of personal information.²¹² The UK has also

²⁰⁹ Protection of Personal Information Act 4 of 2013 s 44.

²¹⁰ Data Protection Act of 2018. This Act became applicable on 25 May 2018.

²¹¹ Data Protection Act of 1998.

²¹² *Carey Data Protection* 6.

enacted secondary legislation containing provisions addressing privacy in the employment relationship and the interception of communications, in the form of the Regulation of Investigatory Powers Act.²¹³ Furthermore, the UK has other sources to assist in improving compliance with Data Protection Act as regards the processing of personal information in the workplace, most notably, the Employment Practice Code²¹⁴ issued by the Information Commissioner in terms of the Data Protection Act.²¹⁵ The purpose of the Code is to translate the legislative provisions into a practical application in the specific information sector involved. Of particular importance is the Article 29 Data Protection Working Party's opinion on data processing at work.²¹⁶ The opinion re-assesses the balance between the legitimate interest of employers and employees' reasonable expectation of privacy.

4.2 PROTECTION OF PRIVACY UNDER COMMON LAW

4.2.1 Privacy protection before the European Convention of Human Rights (ECHR)

English law does not recognise a general right to privacy under common law. Prior the incorporation of ECHR, the United Kingdom had neither legislative nor common-law protection for the right to privacy.²¹⁷

In the absence of a written Constitution and legislation specifically protecting privacy, English law provided protection to aspects of the right to privacy by means of other remedies, such as breach of confidence and breach of contract.²¹⁸

4.2.1.1 *Breach of confidence and misuse of private information*

²¹³ Privacy in the Regulation of Investigatory Powers Act, 2000. It also regulates the powers of public bodies to carry out surveillance and investigation.

²¹⁴ Available at https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf (date of use: 19-07-2016).

²¹⁵ Data Protection Act of 1998 s 51k.

²¹⁶ Opinion 2/2017. Documents of the Art 29 Data Protection Working Party (DPWP) are available at <https://www.pdpjournals.com/docs/88508>. As of 25 May 2018 the DPWP was replaced by the European Data Protection Board (EDPB) (https://edpb.europa.eu/news/news_en).

²¹⁷ Carnegie 1998 *JC/L* 9 311-342.

²¹⁸ Burchell 2009 *EJCL* 12.

The action for breach of confidence may be available when information 'impressed with confidence' is used or disclosed without authorisation. Damages may be claimed to compensate for the loss flowing from the breach.

4.2.1.2 *Breach of contract*

The action for breach of contract is only available if a contract existed between the parties, and the defendant's disclosure of information caused the plaintiff damage.²¹⁹ To found liability for breach of contract, it is necessary to establish that the defendant had knowledge that he or she was inducing a breach of contract, had the intention to cause a breach of contract in the sense that the plaintiff was targeted, and there must have been an actual breach of contract.²²⁰ In an employment context, the employer must have known that his or her action would result in a breach, and must have had the intention of breaching the contract.

An employer who is considering monitoring employees' communications must bear in mind that employee monitoring can raise issues that go to the contractual heart of the employment relationship.²²¹ An employee who has not been properly informed that monitoring is taking place, or who feels that such monitoring is an unjustified invasion of his or her privacy, may argue that the terms of mutual trust and confidence implied in an employment contract, have been breached, and that he or she has been constructively dismissed.²²²

4.3 PROTECTION OF PRIVACY UNDER HUMAN RIGHTS ACT

The UK adopted the Human Rights Act²²³ to implement the ECHR in UK law. The introduction of the Human Rights Act,²²⁴ which came into force in 2000, played an

²¹⁹ Roos *Data (privacy) Protection* 247.

²²⁰ Kill 2007 *Euro L* 2.

²²¹ Sakrouge 2011 *CTLR* 216.

²²² Sakrouge 2011 *CTLR* 216.

²²³ Human Rights Act of 1998.

²²⁴ Human Rights Act of 1998.

important role in the recognition and protection of the right to privacy in the UK.²²⁵ The Human Rights Act implements most of the provisions of the European Convention of Human Rights in UK law, including article 8, which provides a right to respect for private and family life.²²⁶ The Act further stipulates that the Convention rights “are to have effect for the purpose of this Act subject to any designated derogation or reservation”.²²⁷ Legislation should as far as possible, be interpreted in a way that is compatible with the Convention rights.²²⁸ United Kingdom subjects are given the right to bring a cause of action under this Act. This is illustrated in *Molone v United Kingdom*,²²⁹ where the European Court of Human Rights (ECtHR) had to consider whether there had been an infringement of the right to privacy. A warrant authorising the tapping of the applicant’s telephone by the employee was issued without the latter’s consent or knowledge. The applicant was charged with dishonesty in respect of handling stolen items. It was argued that the tapping of the applicant’s telephone contravened article 8²³⁰ which provides a right to respect for private and family life.²³¹ In principle, the right to privacy under the Convention can be applied to the practice of email and internet monitoring of employees in the workplace. The court held that the interception of the applicant’s telephone calls fell within the ambit of the protection of the right to privacy under article 8 of the Convention. Such interception, according to the court, amounted to interference in the right to privacy. The court established that in order for the interference with article 8 to be

²²⁵ Skosana *Privacy and Identity* 163.

²²⁶ Article 8(1) provides that everyone has the right to respect for his private and family life, his home and his correspondence. Article 8(2) provides that there shall be no interference by a public authority with the exercise of this right except in accordance with the law and as necessary in a democratic society in the interest of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

²²⁷ Act of 1998 s 1.

²²⁸ Act of 1998 s 3.

²²⁹ *Malone v United Kingdom* (1983) 5 ECHR R385.

²³⁰ Council of Europe European Convention for the Protection of Human Rights and Fundamental Freedoms 4 November 1950.

²³¹ Article 8(1) provides that everyone has the right to respect for his private and family life, his home and his correspondence. Article 8(2) provides that there shall be no interference by a public authority in the exercise of this right except in accordance with the law, and as necessary in a democratic society in the interest of national security, public safety and economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

legitimate, it must be prescribed by law (written and unwritten) and should be accessible.²³²

In *Campbell v MGN Limited*,²³³ the *Daily Mirror* published photographs showing celebrity model, Naomi Campbell, leaving a meeting of Narcotics Anonymous where she was reportedly undergoing treatment for drug addiction. Campbell claimed damages for breach of confidentiality and compensation under Data Protection Act, 1998. She was awarded compensation in the High Court based on the publication of photographs, which invaded her privacy. Morland J held that even celebrities are entitled to some space of privacy. He also stated that personal data contained in the material published by the *Mirror* had been obtained unfairly and in breach of the Data Protection Act. According to the House of Lords, the action for breach of confidence has been developed under the influence of human rights instruments and decisions of the European Court of Human Rights (ECtHR) to include private information in addition to confidential information. It was thus accepted that the privacy of personal information is worthy of protection.²³⁴

In *Douglas v Hello Ltd*,²³⁵ the court also recognised, for the first time, that a right to privacy can exist in English law independently of the law of confidential information. The case involved the wedding of a famous couple, Michael Douglas and Catherine Zeta-Jones. The couple obtained an interim interdict against the magazine preventing it from publishing photographs of their wedding ceremony. The court held that it had taken into account the provision of the Human Rights Act and article 8 of the ECHR.

²³² Paragraph 69.

²³³ *Campbell v MGN Limited* [2004] UKHL [2].

²³⁴ *Ibid* para [46]. See further Skosana *Privacy and Identity* 166-168.

²³⁵ *Douglas v Hello Ltd* [2007] EG 165 (CS).

In *Copland v United Kingdom*²³⁶ the court stated that emails sent from business premises, and information derived from the monitoring of internet use, could be part of the employee's private life. Collection and storage of that information without the knowledge of the employee would amount to an interference in the employee's rights. The court, however, did not rule that such monitoring would never be necessary in a democratic society.²³⁷

The Human Rights Act is principally concerned with the relationship between the citizens and the state.²³⁸ Therefore, private sector employment is not protected under the Act.²³⁹ It can, therefore, be said that protection of privacy provided by this Act is limited by the fact that the Act is enforceable against public authorities only.²⁴⁰ The Human Rights Act was initially conceived as protection against abuse by the state. Although article 8 imposes a positive obligation on the state to respect and promote the interest of private and family life, the courts have held that individuals are entitled to complain to the state about the infringement of their private life committed by other individuals.²⁴¹ Article 8 also imposes an obligation on the state to take measures to protect individuals from action by non-state actors; one measure would be the establishment of independent judicial system that is responsible for dealing with anyone who is infringing the rights in the Convention.²⁴²

The Act was enacted to regulate the public organisation²⁴³ while excluding acts private organisation. It is clear that only an employee of a public authority would be able to enforce his or her rights directly against his or her employer.²⁴⁴ A person who is aggrieved by an act or omission by a public authority which is in contravention of any right under the Convention, may challenge the act or omission in court.²⁴⁵ If the court finds that the public

²³⁶ *Copland v United Kingdom* [2007] 45 EHRR 37.

²³⁷ [2007] 45 EHRR 253.

²³⁸ Duke 1998 *JCIL* 338.

²³⁹ Johnson 2001 *Cov LJ* 18; Human Right Act s 6.

²⁴⁰ Palmer 2007 *CLJ* 1.

²⁴¹ *McKennit v Ash* [2006] EWCA Civ 1714 [9].

²⁴² Skosana *Privacy and Identity* 166.

²⁴³ The Act does not provide a comprehensive definition of public authority but in terms of s 6(3) of the Human Rights Act, public authority includes any person whose functions are of a public nature.

²⁴⁴ Palmer 2007 *CLJ* 3.

²⁴⁵ Human Rights Act of 1998 s 7.

authority has acted unlawfully by failing to comply with the Convention, the authority will not be subjected to criminal penalties,²⁴⁶ but the court may grant a remedy that is within its normal power and which it considers appropriate.²⁴⁷ An award of damages may only be made in certain narrowly defined circumstances.²⁴⁸

4.4 PROTECTION OF PRIVACY UNDER LEGISLATION

4.4.1 Data Protection Act of 1988

The Data Protection Act, 1988,²⁴⁹ is the UK's implementation of the EU Data Protection Directive²⁵⁰ issued to create uniform European standards for the collection, storage, and processing of personal information. It limits the extent to which personal data²⁵¹ may be processed and allows individuals to access information about them held by the employer. The EU Data Protection Directive aimed to implement the Organisation for Economic Cooperation and Development's (OECD) fair information principles.²⁵² Article 6 of the Directive required a member state to ensure that data was processed fairly and lawfully. The fair information principles were, therefore, incorporated into the Data Protection Act.²⁵³

The first Data Protection Act received royal assent in 1984. It was the first legislation in the UK to address matters such as the collection, storage, and disclosure of personal data held on computers, and had a significant effect on employers' personnel and industrial relations policies and practices.

The general rule is that the Data Protection Act applies to a data controller in respect of personal data, if the data controller is established in the UK. It also applies to a data

²⁴⁶ Human Rights Act of 1998 s 6(7).

²⁴⁷ Human Rights Act of 1998 s 8.

²⁴⁸ Human Rights Act of 1998 s 8(1).

²⁴⁹ Data Protection Act of 1988.

²⁵⁰ Directive 95/46/EC.

²⁵¹ The UK Act uses the term 'data', whereas the SA Act uses the term 'information'. The meanings are, however, synonymous.

²⁵² Foutouchos 2005 *ABPI* 42.

²⁵³ Data Protection Act of 1998 s 4

controller who is not established in the UK, but who uses equipment in the UK.²⁵⁴ If the equipment is used solely for transferring data through the UK, the Data Protection Act does not apply.²⁵⁵ Where the data controller is not established in the UK but uses equipment in the UK, the controller must nominate a representative established in the UK who will be responsible for compliance with the Act.²⁵⁶

In terms of the Data Protection Act the following persons are seen to be 'established in the UK':²⁵⁷

- an individual who is ordinarily resident in the United Kingdom;
- a body incorporated under the law of, or of any part of, the United Kingdom;
- a partnership or other unincorporated association formed under the law of any part of the United Kingdom;
- a person who does not fall within one of the above categories, but who maintains an office, branch, or agency through which he or she carries on any activity or regular practice in the United Kingdom.²⁵⁸

4.4.2 Data protection principles

The data controller must ensure compliance with the data protection principles as provided for in Schedule 1 to the Data Protection Act.²⁵⁹ Data protection principles lie at the heart of data protection law in the UK.²⁶⁰

4.4.2.1 *Personal data must be processed fairly and lawfully*

The requirement in the first principle that the data must be processed fairly and lawfully provides a means by which the employer can give effect to the right to privacy for

²⁵⁴ Wiewiorka *Data Protection* 9; Roos *Data (privacy) Protection* 280.

²⁵⁵ Data Protection Act of 1998 s 5(1).

²⁵⁶ Wiewiorka *Data Protection* 9.

²⁵⁷ Data Protection Act of 1998s 5(3).

²⁵⁸ Data Protection Act of 1998 s 3.

²⁵⁹ Data Protection Act of 1998 s 4(4).

²⁶⁰ Lambert *User's Guide to Data Protection* 102.

workers.²⁶¹ This is also reflected in the Code of Practice in relation to employment²⁶² drafted by the Information Commissioner.

The interpretation provision in Schedule 1 provides that, in determining whether the processing is fair, regard must be had to how the data was obtained. It is clear that the processing will be unfair where any person from whom it has been obtained was deceived or misled as to its intended purpose.²⁶³ This is clear from *Data Protection Registrar v PLP Motors Ltd*.²⁶⁴ PLP Motors recruited an employee who was previously employed by a competitor company. The employee passed on the names and details of his ex-employer's customers to the management department of the defendant company. The relevant details were used in advertising campaigns by the defendant company, and the Data Protection Registrar (now Information Commissioner) received a complaint from an individual who received the advertising material. The defendant company was fined for obtaining personal data unlawfully.

The Act creates a presumption²⁶⁵ that data has been obtained fairly if it has been obtained from the person who is authorised or required by law to supply it.²⁶⁶

For processing to be lawful, at least one of the conditions in Schedule 2 or Schedule 3 (in the case of sensitive data) must be met. These conditions provide the grounds on which data may be lawfully processed.

Schedule 2 to the DPA²⁶⁷ contains general conditions in which the processing of, for example, employee non-sensitive personal data will be legitimate. In order to comply with these, the processing of personal information must fall within one of the following conditions namely:

- The individual whose personal data is involved, has consented to the processing. Therefore, in the employment context, the employee must give express consent,

²⁶¹ Ford 2002 ILJ 1.

²⁶² ILO Code of Practice: Protection of Workers' Personal Data 1997.

²⁶³ Lambert *User's Guide to Data Protection* 102.

²⁶⁴ *Registrar v PLP Motors Ltd (unreported)* cited by Foutouchos 2005 ABP 56.

²⁶⁵ Schedule 1 para 1(2).

²⁶⁶ Carey *Data Protection* 24.

²⁶⁷ Act of 1998 Sch 2.

which can, however, be included in the organisation's contracts of employment as notifications and consent clauses.²⁶⁸

- The processing must be necessary in relation to a contract concluded by the individual.
- The individual has asked for something to be done so he or she can enter into a contract.
- The processing is necessary to protect the individual's vital interest. This condition applies only in cases of life or death, for example, where the employee's medical history is disclosed to a hospital treating him or her after a serious accident.
- The processing is necessary for administering justice, or for exercising statutory, government, or public functions.
- The processing is necessary for the performance of a contract to which the employee is party.
- The processing is necessary for compliance with a legal obligation.
- The processing is necessary to prevent injury or other damage to the health of the employee, or serious loss or damage to his or her property, or to protect vital interests.²⁶⁹

4.4.2.2 *Personal data must be held only for one or more specified and lawful purposes, and not processed in any manner incompatible with what that purpose or those purposes*

This principle gives effect to the EU Data Protection Directive requirement that personal data must be collected for specified, explicit, and legitimate purposes, and may not be processed further in a way incompatible with those purposes.²⁷⁰ Employers would generally be required to stipulate the reasons for holding personal data. Once the Registrar has approved the registration of the data, the second principle has been complied with – provided the data user only process data in accordance with the purposes

²⁶⁸ Lambert *User's Guide to Data Protection* 26.

²⁶⁹ Lambert *User's Guide to Data Protection* 255.

²⁷⁰ Directive 95/46/EC a 6(1)(b).

set out on registration.²⁷¹ Failure by the registrant to maintain an up-to-date and accurate register of personal data-processing activities is a criminal offence.²⁷² To manage the risks, organisations should undertake regular audits of their personal data activities to ensure that registration entries and statements of subject information are up to date and adequately reflect the actual processing of personal data.²⁷³

4.4.2.3. Personal data must not be used or disclosed in a manner incompatible with the purpose for which it is held

Upon registration, data controllers are required to stipulate to whom they intend disclosing personal data they hold. For personnel departments, this requires careful consideration when completing the registration form detailing the categories of people to whom personal data will or may be disclosed.²⁷⁴ These categories may include: associated companies within a group; other employers to whom references about present or past employees may be supplied; and banks, building societies, and finance companies, to whom information of employees' earnings may be supplied.²⁷⁵

Provided these categories of people have been specified on the registration form, and the registration has been accepted by the Registrar, the employer is entitled to process the personal data without seeking the permission of the employee concerned, and without informing the employee that the data has been disclosed.

4.4.2.4 Personal data must be adequate, relevant, and not excessive in relation to the purpose for which it is held

No guidance is provided in the Act on the interpretation of this principle. However, it is sound personnel policy that the personnel information system not be overloaded with irrelevant employee data.²⁷⁶ Irrelevant data refers to personal data concerning an

²⁷¹ Evans *Data Protection Act* 6.

²⁷² Data Protection Act of 1998 s 22.

²⁷³ Webster *Data Protection* 43.

²⁷⁴ Evans *Data Protection Act* 6.

²⁷⁵ Evans *Data Protection Act* 7.

²⁷⁶ Evans *Data Protection Act* 7.

employee's sex life, political affiliation, religion, or other beliefs, and criminal convictions.²⁷⁷ In exceptional circumstances, an employer may collect such personal data, if the data are directly relevant to an employment decision.²⁷⁸

4.4.2.5 *Personal data must be accurate and be kept up to date*

Data will be considered inaccurate if it is incorrect or misleading as to any matter of fact, as opposed to a question of opinion.²⁷⁹

The second leg of this principle requires that data must be kept up to date. The Registrar advised, under the 1984 Act, that the need to update data is determined by the purpose for which the data is held. However, historical records are exempted from this provision. The benefit of this exemption will not be lost merely because the data concerned are disclosed to any person for the purpose of historical research, to the data subject, or to a person acting on his or her behalf, at the request or with the consent of the data subject or a person acting on his or her behalf.²⁸⁰

4.4.2.6 *Data may not to be kept longer than necessary for the purposes for which they were collected*

The fifth principle entails that the retention of data for an unnecessary length of time – taking into account the purpose for which the data were collected – is a breach of this principle.²⁸¹ Again, the Act offers no guidelines for the interpretation of this principle. The principle implements a requirement in the EU Data Protection Directive that personal data should not be retained in a form that permits identification of the data subject, for longer than is necessary for the purposes for which the data were collected.²⁸²

²⁷⁷ ILO Code of Practice: Protection of Worker's Personal Data 1997 s 65.

²⁷⁸ ILO Code of Practice s 65(2).

²⁷⁹ Evans *Data Protection Act* 7.

²⁸⁰ Carey *Data Protection Act* 34.

²⁸¹ Carey *Data Protection Act* 34.

²⁸² Dir 95/46/EC a 6(1)(e).

This principle could potentially have a significant impact on historical information held about former employees, and much will depend on how the court interprets 'necessary' in this context.²⁸³ One of the factors to be considered when determining how long to retain data on former employees, relates to possible claims the employee may make after leaving an organisation's employment.²⁸⁴ Unfair dismissal is subject to a limitation period of six months from the employee's departure.²⁸⁵ Claims for personal injury have a three-, year lifespan²⁸⁶ which may run from the date on which the injury was sustained, in the case of industrial deaths which may only surface twenty or thirty years after the employee's departure, the date when the injury is discovered. This would suggest that it might be necessary to keep former employees' records for a considerable time. In addition, Schedule 1 to the Data Protection Act allows data held for historical, statistical, and research purposes to be retained indefinitely, irrespective of the sixth principle.

4.4.2.7 Personal data must be processed in accordance with the rights of the data subjects under the Act²⁸⁷

The rights of a data subject are set out in the Act²⁸⁸ and apply equally to employees. The employees have a right to a copy of the information comprising their personal data. An employee who requests a copy of his or her personal data under section 7 of the Act, is entitled to:

- confirmation that the organisation/employer holds personal data relating to him or her;

²⁸³ Evans *Data Protection Act* 8.

²⁸⁴ Evans *Data Protection Act* 8.

²⁸⁵ Evans *Data Protection Act* 8.

²⁸⁶ Evans *Data Protection Act* 8.

²⁸⁷ Schedule 1, Part II, para 8 states that a person will breach this principle only if such person:

- (a) Contravenes the right of access provisions in section 7;
- (b) Fails to comply with a justified request to cease processing under section 10 or fails to respond to such a request within 21 days of its receipt;
- (c) Fails to comply with the request under section 11 to cease direct marketing processing.

²⁸⁸ Data Protection Act of 1998 s 7 to 15.

- be advised of the purpose for which his or her personal data is being processed and of the sources of that data.²⁸⁹

4.4.2.8 *Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction of, or damage to, personal data*

This principle is primarily concerned with the security of personal data. Employers are under a legal duty to ensure that appropriate security measures are in place in order to protect the personal data of the employees from loss, damage, or disclosure, whether accidental or as the result of unlawful action.²⁹⁰

In addition to the basic requirement that personal data be held securely, there are two additional requirements. The first relates to staff whose job involves handling personal data. Employers are under the legal duty to ensure that such staff is reliable. The second relates to outsourcing. Employers must ensure that their data processors take appropriate security measures throughout their relationship. Furthermore, employers are responsible for putting in place a written contract with the data processor that must include a specific clause relating to this principle.²⁹¹

The Employment Practice Data Protection Code, published by the Information Commissioner, also offers some guidance on what steps the employer might reasonably be expected to take. Firstly, the employer must ensure that employees:

Are aware of the extent to which they can be criminally liable if they knowingly or recklessly disclose personal data outside their policies and procedure.²⁹²

Secondly, the Employment Code states that the employer must take steps to ensure the reliability of staff that have access to employees' records. This will involve training to ensure that employees understand their responsibilities as regards confidential and

²⁸⁹ Webster *Data Protection* 70.

²⁹⁰ Webster *Data Protection* 83.

²⁹¹ Webster *Data Protection* 83.

²⁹² Employment Code "Record management - High level management" benchmark 5.

sensitive information. Furthermore, a confidentiality clause must be included in such employees' contracts of employment.²⁹³

4.4.2.9 Personal data may not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information

The eighth principle gives effect to article 25 of Data Protection Directive.²⁹⁴ The Directive provides that EU member states should legislate for a restriction on the transfer of personal data to the third countries.²⁹⁵ This restriction entails that such transfer may take place only if the third country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to personal data processing. The eighth data protection principle outlaws the export of personal data to countries outside of the European Economic Area (EEA) and employers may, therefore, generally not transfer information in personal data outside of the EEA, unless an appropriate exemption applies.²⁹⁶

4.4.3 Exemption to the prohibition in terms of Schedule 4

The eighth principle does not prevent trans-border data flows where:

- the data subject has given consent to the transfer;
- the transfer is necessary for entering into a contract between the data controller and the data subject, or for the performance of such a contract;

²⁹³ Employment Code, "Record management - High level management" benchmark 5.

²⁹⁴ EC Directive 95/46/EC art 25.

²⁹⁵ The Directive defines the third countries as non-European member states.

²⁹⁶ *Carey Data Protection* 140.

- the transfer is necessary for the performance or conclusion of a contract between the data controller and a third party, which is entered into at the request of the data subject or in his or her interests;
- the transfer is necessary for substantial reasons of public interest; or
- the transfer is necessary for legal proceedings, for obtaining legal advice, or establishing, exercising, or defending legal rights.²⁹⁷

4.5 RIGHTS OF THE DATA SUBJECT

The data protection regime provides a number of rights to individuals in relation to their informational privacy. Key aspects of these rights are transparency and consent.²⁹⁸ The Data Protection Act stipulates the following rights of the data subject.

4.5.1 Right of access to personal data

The Act provides that a data subject has a right of access to personal data.²⁹⁹ This means that employees may access their personal data on their employers' computers. The Act also requires disclosure to employees of any 'expression of opinion' about the employee, if such information is held. This includes, for example, the rating of an employee's current performance and potential.³⁰⁰

4.5.2 Right to prevent data processing likely to cause damage or distress

The Act also provides a right to prevent processing likely to cause damages or distress.³⁰¹ In order to make use of this provision, the employee must forward to the employer, a notice in writing which specifies why the processing is or will cause damage or distress.³⁰²

²⁹⁷ Data Protection Act of 1998 Schedule 4(3).

²⁹⁸ Lambert *User's Guide to Data Protection* 139.

²⁹⁹ Data Protection Act of 1998 s 7.

³⁰⁰ Evans *Data Protection Act* 16.

³⁰¹ Data Protection Act of 1988 s 10.

³⁰² Carey *Data Protection* 20.

The notice may specify the purpose or manner of processing that is objectionable. The employer must respond within 21 days of receipt of the notice. The response must consist one of the following two options:

- a statement that the employer has complied, or intends to comply, with the request in the employee notice; or
- a statement that the data controller regards part or all of the employee's notice unjustified, and the extent to which the employer has complied or intends to comply with it.³⁰³

4.5.3 Right to compensation for failure to comply with certain requirements

Any employee is entitled to compensation where employer processing has caused unwarranted and substantial damages.³⁰⁴ A contravention of any of the requirement of the Act allows the employee to seek redress in the courts. This process is likely to start with a complaint that has not been correctly handled and then escalate into a claim for compensation.³⁰⁵ Assistance from the Information Commissioner for either party to an application is available, at the discretion of the Commissioner, if the case involves matters of substantial public importance.³⁰⁶ This means that the Information Commissioner would conduct an investigation into the circumstance surrounding the complaint. The outcome is an official view as to whether or not the employer is likely to have been in breach of the data protection Act in the circumstances described.³⁰⁷

³⁰³ Carey *Data Protection* 20 and s 10 of the Act.

³⁰⁴ Data Protection Act of 1998 s 13.

³⁰⁵ Webster *Data Protection* 180.

³⁰⁶ Carey *Data Protection* 25.

³⁰⁷ Webster *Data Protection* 180.

4.5.4 Rights in relation to inaccurate data

A data subject who suffers damages as a result of inaccurate data³⁰⁸ being held by the data user, is entitled to institute action in court for compensation against the data user.³⁰⁹

It is not a contravention of the fourth principle if the data controller accurately records information given by the data subject or a third party.³¹⁰ It is, therefore, important for the employers to distinguish between data generated about the employees internally after employment has commenced, and data supplied by an employee or third parties external to the organisation during the course of employment.³¹¹ Employers can be liable to compensate an employee for the accuracy of factual data generated during the course of employment of an employee. Employers will not be held liable for holding factual but inaccurate data supplied to them by the employee or other third parties.³¹²

4.6 INTERCEPTION OF ELECTRONIC COMMUNICATIONS

The monitoring of electronic communications in the workplace is the main threat to an employee's privacy. The Human Rights Act³¹³ guarantees certain fundamental rights to all citizens. These rights cannot be excluded by agreement. The Regulation of Investigatory Powers Act³¹⁴ (the RIPA) and the Data Protection Act³¹⁵ are regulatory statutes that apply to contract.³¹⁶ The RIPA³¹⁷ is the implementation of European Directive

³⁰⁸ The Data Protection Act of 1998 s 70(2) provides that data are inaccurate if they are incorrect or misleading as to any matter of fact.

³⁰⁹ Act of 1998 s 14 states that inaccurate data may be ordered by a court, on application by the data subject, to be rectified, blocked, erased or destroyed if the court is satisfied that they are inaccurate. This extends to other data which contains an expression of opinion about the data subject which is based on the inaccurate data.

³¹⁰ Schedule 1 para 7 of Part II.

³¹¹ *Evans Data Protection Act 14.*

³¹² *Evans Data Protection Act 14.*

³¹³ Act of 1998.

³¹⁴ Regulations of Investigatory Powers Act of 2000.

³¹⁵ Act of 1998.

³¹⁶ Oliver 2002 *ILJ* 334.

³¹⁷ The Act covers interception of communications disseminated by public postal system, public telecommunications system, and private telecommunication systems. The RIPAs make it a criminal offence intentionally and without lawful authority to intercept any communication in the course of its transmission by public postal system and public telecommunication systems. It is also a criminal

97/46/EC.³¹⁸ The RIPA affects an employer's ability to interfere with electronic communications. It relates directly to the issue of email and internet monitoring by employers, and provides for employers who wish to monitor email and internet use in the workplace.³¹⁹ Section 1(3) of the Act³²⁰ introduces civil liability for the interception of communications over a private system. Section 1(3) effectively creates a privacy right in relation to telecommunications, which applies to an employer's monitoring of telephone calls, emails, and internet use. Section 1(3) also applies to both the employer's internal system, and where that system is used to communicate with persons outside of the workplace.³²¹ Where unlawful interception takes place, both the employee affected and any external sender or recipient of the communication can bring a claim.

In relation to employers, interception can take place where both the sender and the recipient have consented³²² to the interception of the communication, or the employer has reasonable grounds to believe that they have so consented.³²³ It is not clear from the Act whether the consent must relate to interception of the specific communication in question, or whether a more general consent would suffice.³²⁴

The most significant provisions in relation to workplace monitoring are found in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations of 2000 (the Telecommunications Regulations).³²⁵ In response to employer concerns, the regulations have watered down the restrictions placed on the employer by the RIPA. The Telecommunications Regulations provide that to fall within the Regulations,

offence intentionally and without lawful authority to intercept any communication in the course of its transmission by private telecommunication system.

³¹⁸ European Directive 97/46/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector. This Directive has subsequently been repealed by Directive 22/58/EC.

³¹⁹ Oliver 2002 *ILJ* 338.

³²⁰ The Regulations of Investigatory Power Act of 2000 s 1(3).

³²¹ Oliver 2002 *ILJ* 338.

³²² Consent is defined in art 7(a) of the Data Protection Directive 95/46/EC as any freely-given, specific, and informed indication of the data subject's wishes by which he or she signifies his or her agreement to personal data relating to him or her being processed. For consent to be valid, it must also be voluntarily.

³²³ Act of 2000 s 3(1).

³²⁴ Oliver 2002 *ILJ* 338.

³²⁵ The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 available at <https://ico.org.uk/for-organisations/guide-to-data-protection/employment/>.

the interception must be made by or with the consent of the person carrying on a business, for purposes relevant to that person's business, and using that business's own telecommunication system.³²⁶ Institutions may monitor and record communications:³²⁷

- to establish the existence of facts;
- to ascertain compliance with regulatory or self-regulatory practices and procedures applicable to the system controller in carrying on his or her business, or applicable to another person in carrying on his or her business where that person is supervised by the system controller as regards those practices or procedures;
- to ascertain or demonstrate standards which have been achieved, or ought to have been achieved, by person's using the system in the course of their duties;
- in the interests of national security;
- to prevent or detect crime;
- to investigate or detect unauthorised use of telecommunications systems; or
- to secure, or as an inherent part of, an effective system operation.

The Information Commissioner's Office (the ICO) – which is responsible for overseeing data protection in the United Kingdom – issued a code of guidance in 2011 for the employer-employee relationship.³²⁸ The Employment Practices Code states that the obligation of employers under the Data Protection Act requires employers to notify employees of surveillance policies and place limits on the extent of monitoring which can take place.³²⁹

The third part of the Code contains guidelines on how employers can monitor staff emails within the law. Employers have the right to monitor staff emails, provided that the employees have been warned that monitoring is taking place, and the reason for

³²⁶ The RIPA s 6(a).

³²⁷ The RIPA s 6 (b).

³²⁸ ICO The Employment Practices Code (2011). The Code was issued in terms of s 51 of the Data Protection Act of 1998. Employers are obliged to comply with the Act and the code is there to assist them in doing so.

³²⁹ Part 3: Monitoring at Work 65.

monitoring has been explained.³³⁰ The Code of Practice covers a range of surveillance activities such as opening emails or voice mails, checking internet usage, and recording using CCTV cameras.

The Article 29 Data Protection Working Party, established in terms of the 1995 Directive on data protection, issued an opinion on data processing at work.³³¹ The opinion reassesses the balance between the legitimate interests of employers and the reasonable privacy expectations of employees.

The Article 29 Data Protection Working Party³³² has also adopted a working document that provides guidance on the acceptable limits of monitoring of employees' personal information. Its main principle is that any limitation of an employee's privacy should be appropriate to the likely damage to the employer's legitimate interests. It recommends that any monitoring measures must pass four tests.³³³

- Is the monitoring activity transparent to the employees?
- Is the processing activity proportionate to the concerns raised?
- Is the proposed processing of personal data fair to the employee?
- Is the processing activity necessary?

Article 29 of the Data Protection Working Party stipulates that monitoring is permissible where an employer has a transparent policy in place, but also that such monitoring must be fair, necessary, and proportionate.³³⁴

In *Bărbulescu v Romania*,³³⁵ the applicant was employed as a sales engineer. At his employer's request, he created an instant messaging account using Yahoo Messenger, on which to respond to customer enquiries. The employer prohibited the use of company

³³⁰ Part 3: Monitoring at Work 65.

³³¹ Article 29 Data Protection Working Party Opinion 2/2017 on Data Processing at Work WP249.

³³² Article 29 of the Working Party opinion 55/2002 available at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf.

³³³ Article 29 Opinion 55/2002 4.

³³⁴ Brennan 2016 *ALGD* 3.

³³⁵ *Bărbulescu v Romania* (61496/08) [2016] IRLR (ECHR) 235.

resources by employees for personal purposes.³³⁶ The applicant was informed of the regulations and signed the document after acquainting himself with its contents. Bărbulescu's contract of employment was terminated after he had reportedly made use of the Yahoo Messenger account for personal communications. The employer recorded the applicant's Yahoo Messenger communication. When the applicant denied using the Yahoo Messenger account for personal purposes, his employer presented him with a 45 page transcript of his communication as evidence in the disciplinary proceedings and in court.

Two Romanian courts – the Bucharest Country Court and the Bucharest Court of Appeal – upheld the applicant's dismissal. He then appealed to the ECtHR claiming that his emails were protected by article 8 of the European Convention on Human Rights. The ECtHR dismissed his appeal. The court held that employer's conduct had been reasonable, and that the monitoring of his communications had been the only method of establishing whether there had been a breach of his employment contract. It found that the domestic court had struck a fair balance between the applicant's right and the interests of the employer.

It is important to note that *Bărbulescu* recognises that employees have a reasonable expectation of privacy, particularly in the absence of a warning of monitoring.

4.7 GENERAL DATA PROTECTION REGULATION

Although I do not address the new data protection regulations in detail, it is important briefly to highlight the reforms effected by the European Parliament's new Regulation (EU) 2016/679,³³⁷ also known as the General Data Protection Regulation (the GDPR), which entered into force on 25 May 2018.³³⁸ The GDPR updates existing EU data protection law. It replaces the 1995 Directive, but maintains principles and rules established under

³³⁶ The prohibition was based on art 50 which states that "any disturbance of order and discipline on the company premises shall be strictly forbidden, in particular: personal use of computers, photocopies and telephone and fax machines".

³³⁷ Directive 2016/679.

³³⁸ Data Protection Act of 2018.

that Directive. As with any reform, there is both change and continuity. Therefore, companies will have to identify differences between their regulations under the 1995 Directive and the GDPR and apply remedial steps. The GDPR introduces new obligations for employers namely: organisations are required to implement data protection by design and by default; to appoint a data protection officer; and to comply with the principle of accountability. Unlike the previous Directive, the GDPR has direct effect in all EU member states, meaning that there is no need for the adoption of domestic legislation to ensure its application in national courts.

4.7.1 Three main reforms under the GDPR

The issue of personal data became a major concern for companies with the adoption of the GDPR.³³⁹ This Regulation provides for a potential sanction of four per cent of a company's consolidated global turnover in the event of failure to meet its obligations. The GDPR has changed the company climate in that companies are now obliged to consider risks to which they may expose others, including employees, whereas traditionally they considered only their own risk. The GDPR consequently makes impact assessment mandatory.³⁴⁰

4.7.1.1 Compulsory appointment of the data protection officer from companies whose business includes data processing

Article 37 of the GDPR requires the compulsory appointment of a Data Protection Officer. Data Protection Officers are persons who advise on compliance with data protection rules in organisations engaged in data processing. They are a cornerstone of accountability since they facilitate compliance, while also acting as intermediaries between the supervisory authorities and employees, together with the organisation by which they have been appointed.³⁴¹ Article 39 of the GDPR stipulates the primary responsibilities of the Data Protection Officer, namely:

³³⁹ Regulation EU 2016/679.

³⁴⁰ Camus, Chekroun & Hubert-Petit 2018 *IBLJ* 127.

³⁴¹ General Data Protection Regulation art 37.

- to inform and advise the controller (employer) and its employees on the content of new obligations;
- to create and maintain records of processing activities in the organisation;
- to ensure proper application of the GDPRs; and
- to monitor compliance with the GDPR and the national data protection law by carrying out audits and training staff involved in processing operations.

The Data Protection Officer's position involves raising awareness of the new obligations arising from the Regulation – in our context, raising awareness among a company's staff.³⁴² The Data Protection Officer is appointed on the basis of professional qualifications and, in particular, expert knowledge of data protection law and practice, and the ability to fulfil the tasks referred to in article 39.

4.7.1.2 The obligation to protect data as early as the design stage of the data processing system

- *Data protection by design*

Data protection by design is provided for in article 25 of the GDPR. It lays down how controllers and processors, including employers, must implement appropriate technical and organisational measures to ensure compliance with the GDPR.³⁴³ These measures should be implemented both at the time of processing, and when determining the means of processing.³⁴⁴ In implementing these measures the employer must take account of the state of the art, the cost of implementation, the nature, scope, and purpose of personal data processing, and the risks and severity for the rights and freedoms of the data employer

³⁴² Camus, Chekroun & Hubert-Petit 2018 *IBLJ* 127.

³⁴³ General Data Protection Regulations art 25 (1).

³⁴⁴ Article 29 Working Party (2017).

- *Data protection by default*

This provides that the employer must institute appropriate measures to ensure that only personal data that are necessary for the stated purposes will be processed by default. This obligation applies to the amount of personal data collected, the extent of the processing, the storage period, and accessibility.³⁴⁵

4.7.1.3 The obligation to document all personal data processing activities the company performs

Companies must be able to show their compliance with the GDPR whenever required to do so. To show compliance, employers must maintain a record of all personal data processed by the company.³⁴⁶ This is not a new rule; it was included in previous legislation but compliance has been rare.³⁴⁷ In practical terms, companies are expected to indicate data processing activities, the categories of personal data processed, the objective set for the data processing operations, the actors involved in processing this data, and the origin and destination of the data. This would also assist in identifying the possible transfer of data outside of Europe.³⁴⁸

4.8 CONCLUSION

Employers are permitted to process their employees' personal information. However, it is not enough for the employer simply to inform the employee of the processing of his or her personal information. The employer must also be able to show that he or she has complied with the core data protection principles under that Data Protection Act³⁴⁹ to ensure the legitimacy of the processing, and protect the employees' right to privacy provided under

³⁴⁵ General Data Protection Regulations art 25 (2).

³⁴⁶ General Data Protection Regulations art 26.

³⁴⁷ Camus, Chekroun & Hubert-Petit 2018 *IBLJ* 140.

³⁴⁸ Article 29 Working Party (2017).

³⁴⁹ Data Protection Act of 1998.

article 8 of the Human Rights Act.³⁵⁰ Furthermore, to avoid possible liability, employers must also take the new provisions under the GDPR into consideration. Therefore, the companies will have to identify where their regulations and the GDPR diverge and apply remedial steps so that they can be in line with the Regulation.

³⁵⁰ Human Right Act of 1998.

Chapter 5

Conclusions and recommendations

5.1 SUMMARY

This dissertation has focused on the right to informational privacy in the workplace. Informational privacy is a specific aspect of the general right to privacy that has assumed considerable importance.

Chapter 2 focuses on the nature and the scope of the right to privacy in South Africa in terms of common law and the Constitution. It was observed that the right to privacy enjoys dual protection under both section 14 of the Constitution, and in terms of the common law as a personality interest protected by the law of delict. The chapter also looks at the extent of the right to privacy in the employment relationship. It is pointed out that the right to privacy remains challenging in the workplace context, where technology has changed the way organisations perform their day-to-day duties. The right to privacy under section 14 of the Constitution, does not adequately address the issues related to the protection of the privacy of personal information or data stored electronically. It does not allow the data-subject (the employee) active control over his or her personal information.³⁵¹ It is also pointed out that common-law principles cannot ensure that the data subject receives notification of the fact that his or her personal information is being collected or processed, or that he or she has the right to access, update, or correct incorrect information.

Chapter 3 analyses the South African legislation applicable to the privacy of electronic communications and personal information in the workplace. It is noted that, apart from the POPI Act (which is not yet in full operation), current legislation in South Africa does not provide sufficient protection for data subjects. This may be ascribed to the fact that the Labour Relations Act does not address the processing of personal information, but deals

³⁵¹ Roos 2007 SALJ 423.

only with the relationship between the employer and the employee. The Regulation of Interception of Communications and Provision of Communication-related Information Act,³⁵² limits employees' constitutional right to privacy in their communications provided under section 14(d) of the Constitution. The Act provides that any person, including the employer, may intercept an employee's electronic communication if the employee consents to that interception. Section 6 similarly limits the right of the employees to the privacy of their communications by allowing the employer to intercept their indirect communications in specifically defined circumstances.

It is consequently submitted that apart from the POPI Act, current legislation in South Africa does not provide sufficient protection for the data subject, including employees. It is for this reason important that the POPI Act be fully implemented as soon as possible.

Chapter 4 is a comparative overview of the position in the United Kingdom. It is pointed out that in the UK, the right to privacy is not recognised by English common law. The employees' right to privacy in the UK derives from two legal sources: article 8 of the ECHR, which guarantees the right to privacy; and the European Data Protection Directive 95/46 through its application of the Data Protection Act.³⁵³ The Human Rights Act provides for the protection of the right to privacy in the UK. However, the protection provided by this Act is not sufficient from a data protection point of view. Nonetheless, it is clear that the UK has built a strong foundation for data protection through several versions of Data Protection Act,³⁵⁴ together with other resources such as directives, employment practice codes, and case law.

From the above discussion it is clear that employers have a legitimate interest in a productive and safe environment that generally leads to processing of personal data of the employees. On the other hand, employees do not lose their right to personal privacy when they enter their office doors, and they have an expectation of a certain degree of privacy at work. Furthermore, we saw that employers are entitled to process and monitor

³⁵² Act 70 of 2002.

³⁵³ Bond 2015 *Comp & Risk* 4.

³⁵⁴ Data Protection Acts of 1984, 1998, and 2018.

their employees' personal data. However if it is to avoid breaching the employee's right to privacy, the employer must comply with the Data Protection Act.³⁵⁵ The Information Commissioner has issued the Employment Practice Code³⁵⁶ to assist the employers to comply with the Act. Part 3 of the Employment Practice Code, which specifically deals with eight data protection principles, give guidance on relevant considerations when deciding who, for what purpose, and how the processing and monitoring can be carried out without infringing employees' right to privacy.³⁵⁷

5.2 CONCLUSION

Despite protection in terms of common law and the Constitution, from the above discussion it is clear that South Africa has been tardy in adopting an holistic data protection law. The Protection of Personal Information Act was only signed into law by parliament in November 2013. However, the Protection of Personal Information Act³⁵⁸ can be seen as progressive, and could serve as a stepping-stone to data protection compliance in South Africa. It provides a mechanism for organisations, many of whom have already taken steps to comply with data protection laws when processing the personal information of employees.

Regardless of the progress made in South Africa through the implementation of the Protection of Personal Information Act, South Africa³⁵⁹ can still learn from the UK data protection laws, in the main, because both countries recognise the need for employee privacy in that employers are generally required to justify the need to process employees' personal data. South Africa and the UK share common data protection features. The conditions for lawful processing of personal data that form the backbone of the POPI Act are very similar to the principles applicable in the European Union and the UK Data Protection Act. Therefore, understanding and applying the POPI Act does not entail

³⁵⁵ Data Protection Act of 1998.

³⁵⁶ Employment Practice Code of Data Protection.

³⁵⁷ Wright 2009 *DPD* 4.

³⁵⁸ Act 4 of 2013.

³⁵⁹ Act 4 of 2013.

reinventing the wheel;³⁶⁰ the UK has built a strong foundation for data protection laws through the Data Protection Act and other resources such as case law and the Employment Code of Practice. South Africa can benefit greatly from good workplace practice regarding data protection and privacy in the UK and gain a deeper understanding in its application of the eight core data protection principles.

5.3 RECOMMENDATIONS

Based on the above discussion it is seen that emerging data protection in South Africa is strongly influenced by the European Union data protection Directive 95/46/EC a predecessor to the GDPR.³⁶¹ Admittedly, South Africa was a bit late to adopt POPI holistic nevertheless; POPI could be seen as a stepping-stone to global compliance. The study indicates that South Africa has some catching up to do in order to strengthen its framework and improve creditability of its data protection legislation. Although South Africa has similar data protection principles to the UK, there are important key elements that can be adopted from the UK data protection law and the new GDPR to develop viable global data protection legislation. These include:

5.3.1 Privacy by design

The concept of privacy by design is mandate by article 25 of the GDPR which lays down how controllers and processors, including employers, must implement appropriate technical and organisational measures to ensure compliance. It also provides assurance to the employees that their personal information is adequately protected.³⁶² In South Africa privacy by design does not form part of POPI at all, however, it should be included in the future regulations governing data protection in South Africa.

³⁶⁰ Human Rights Act, 1998.

³⁶¹ Bygrave 2010 *SSL* 194.

³⁶² Camus, Chekroun & Hubert-Petit 2018 *IBLJ* 141.

5.3.2 Data protection impact assessments

The GDPR in article 35 mandates data protection impact assessments and the maintenance of evidence or documentation of assessment. The POPI Act does not at present have a similar provision. Once this has been incorporated into our legislation, a tool to measure the privacy impact should be developed by employers

5.3.3 Data portability

In terms of GDPR article 20, data subjects including employers enjoys the benefits of data portability³⁶³ in terms of which they can request that their data be transferred to another controller. This enable the employee to request personal data, which he or she provided to the employer, it also give the employee the right to process such data to another controller without hindrance.³⁶⁴ The POPI Act is silent on this matter. It is suggested that the POPI Act should also adopt a similar provision.

Regardless of the progress made by the POPI Act, it is submitted that it should be amended to include the abovementioned principles as provided for by the EU Regulation. The amendment would bring the POPI Act in line with the global view on data protection and ensure compliance without compromising any of the objectives of the POPI Act.

5.3.4 General recommendations

It is further submitted that employers must ensure that :

- Employees are aware of the new legal duties the Act places on the employer and their own role as employees. In particular, employees should be aware of how data protection compliance is achieved in practical terms. It is also important to make

³⁶³ General Data Protection Regulations art 20.

³⁶⁴ <http://www.gamingtechlaw.com/2016/09/privacy-portability-right-industry.html>

employees aware of the possible consequences of their actions as regards the processing of personal information. Such information can be provided in policies couched in plain English, which should be provided to all new employees with the copy of their contracts of employment. Employees must be empowered to study these policies before signing their employment contracts. Adopting this approach would assist the employer to show that the employee understood the extent to which his or her workplace activities could be monitored and processed.

- Protecting personal information must be part of all agreements with third parties involved in or performing processing activities. Failure to take reasonable steps to protect personal information must result in consequences for the person at fault.
- Employers or organisations should ensure effective and efficient auditing and monitoring processes. Privacy protection can also be introduced as a new section in existing auditing and monitoring processes.
- Organisations should offer regular training and awareness programmes. Key staff should be identified to deal with personal information directly, and conduct targeted training based on their functions. Training should also form part of the induction process for all new employees.

BIBLIOGRAPHY

BOOKS

Bygrave *Data Protection Law*

Bygrave LA *Data Protection Law: Approaching its Rationale, Logic and Limits*
(Kluwer Law International Hague 2002)

Carey P *Data Protection*

Carey P *Data Protection in the UK* (Blackstone Press Limited London 2000)

Carey P *Data Protection*

Carey P *Data Protection – A Practical Guide to UK and EU Law* (Oxford University Press United Kingdom 2018)

Currie & de Waal *Bill of Rights Handbook*

Currie I & de Waal J *The Bill of Rights Handbook* 6th ed (Juta and Company Ltd 2013)

Currie *Promotion of Administrative Justice*

Currie I *The Promotion of Administrative Justice Act - Commentary* 2nd ed (Siber Ink South Africa 2007)

Currie I & Klaaren *Promotion of Access*

Currie I and Klaaren *The Promotion of Access to Information Act – Commentary*
(Siber Ink 2002)

Evans *Data Protection Act*

Evans A *The Data Protection Act: A Guide for Personnel Managers* (Institute of Personnel Management, Britain 1985)

Grogan *Workplace Law*

Grogan J *Workplace Law* (Juta Cape Town 2003)

Gulleford *Data Protection in Practice*

Gulleford K *Data Protection in Practice* (Butterworths London 1986)

Lambert *Users Guide to Data Protection*

Lambert P *A User Guide to Data Protection* (Bloomsbury Professional Croydon 2013)

Loubser et al *Law of Delict*

Loubser M, Midgley R, Mukheibir A, Niesing L & Perumal D *Law of Delict in South Africa* (Oxford University Press Cape Town 2009)

Makulilo (ed) *African Data Privacy Laws*

Makulilo A B (ed) *African Data Privacy Laws* (Springer International Publishing AG Cham 2016)

McQuoid-Mason *Privacy*

McQuoid-Mason DM *Law of Privacy in South Africa* (Juta Cape Town 1978)

Midgley & Niesing *Law of Delict*

Midgley R & Niesing L *Law of Delict* 6th ed (Oxford University Press Cape Town 2016)

Neethling, Portgieter & Visser *Law of Delict*

Neethling J Portgieter JM & Visser PJ *Law of Delict* 2nd ed (Butterworths Durban 1994)

Neethling, Pogieter, & Visser *Neethling's Law of Personality*

Neethling J, Pogieter JM & Visser PJ *Neethling's Law of Personality* 2nd ed (Butterworths Durban 2005)

Papadopoulos & Snail *Cyberlaw*

Papadopoulos S & Snail S *Cyberlaw @ SAIII: The Law of Internet in South Africa* 4th ed (Van Schaik Publishers Pretoria 2012)

Peter *Data Protection*

Peter C *Data Protection in the UK* (BPL London 2000)

De Stadler & Esselaar *Protection of personal information*

De Stadler & Esselaar *A Guide to Protection of Personal Information Act* (Juta Cape Town 2015)

Schwartz & Reidenberg *Data Privacy*

Schwartz PM & Reidenberg JR *Data Privacy Law* (Michie Law Publishers Virginia 1996)

Van der Merwe et al *Information Communications*

Van der Merwe D, Roos A, Eiselen GTS, Nel SS & Pistorious T *Information Communications and Technology Law* 2nd ed (LexisNexis Durban 2016)

Van der Walt & Midgley *Delict*

Van der Walt JC & Midgley JR *Principles of Delict* 3rd ed (LexisNexis Durban 2005)

Woolman & Bishop *Constitutional Law*

Woolman S & Bishop M *Constitutional Law* 2nd ed (Juta Cape Town 2013)

Webster *Data Protection*

Webster M *Data Protection in the Financial Services Industry* (Gower Publishing Limited England 2006)

Weiworka *Data Protection Act*

Weiwiorka E *Data Protection Act 1998* (W Green/Sweet and Maxwell UK 2002)

JOURNAL ARTICLES

Beech 2005 *ILJ*

Beech W "The right of the employer to monitor employees electronic mail, telephone calls, internet usage and other recordings" 2005 (26) *International Law Journal* 650-660

Brainbridge & Pearce 1998 *CLSR*

Brainbridge D & Pearce G "The UK Data Protection Act 1998 – Data subject rights" 1998 (14) *Computer Law and Security Report* 401-406

Brennan 2016 *PDP* 1-5

Brennan D "Monitoring employees' emails – How far is too far?" 2016 (16) *Privacy and Data Protection Journal* 1-5.

Burchell 2009 *EJCL* 1-26

Burchell J The legal protection of privacy in South Africa- a transplantable hybrid 2009 (13) *Electronic Journal of Comparative Law* 1-26

Bygrave 2010 *SSL* 165-200

Bygrave 'Privacy and data protection in an international perspective' 2010 (56) *Scandinavian Studies in Law* 165-200

Camus, Chekroun & Hubert-Petit 2018 *IBLJ*

Camus C, Chekroun D & Hubert-Petit P "Companies and general data protection regulation: What reforms are needed?" 2018 (2) *International Business Law Journal* 125-141

Carnegie 1998 *JCIL*

Carnegie P "Privacy and the press: The impact of incorporating the European Convention on Human Rights in the United Kingdom" 1998 (9) *Journal of Comparative and International Law* 311-342

Collier 2002 *ILJ*

Collier D "Workplace privacy in the cyber age" 2002 (23) *Industrial Law Journal* 1743-1759

Dekker 2004 *SA Merc LJ* 622- 637

Dekker A "Vices or devices: Employment monitoring in the workplace" 2004 (16) *Mercantile Law Journal* 622- 637

Foutouchos 2005 *ABPI*

Foutouchos M "The European workplace: The right to privacy and data protection" 2005 (4) *Accounting Business and Public Interest* 35-97

Ford 2002 *ILJ*

Ford M "Two conceptions of worker privacy" 2002 (31) *Industrial Law Journal* 1-18

Kill 2007 *Euro L*

Kill L "When breach of contract might be ok" *European Lawyer* 2007 (69) 18-19

Lorber 2004 *ILJ*

Lorber S "Data protection and subject access request" 2004 (33) *Industrial Law Journal* 179 - 190

Mischke 2003 *Cont LL*

Mischke C "Workplace privacy, email interception and the law: Does the new legislation limit employers' right to read email?" 2003 (8) *Contemporary Labour Law* 72-79

Modiba 2003 *Merc LJ*

Modiba M "Intercepting and monitoring employees email communications and internet access" 2003 (15) *SA Mercantile Law Journal* 363 - 371

Neethling 2005 *SALJ*

Neethling J "The concept of privacy in South African law" 2005 (122) *South African Law Journal* 18-28

Neethling 2012 *THRHR*

Neethling "Features of the Protection of Personal Information Bill 2009 and the law of delict" 2012 *Tydskrif vir Hedendaage Romeins-Hollandse Reg/Journal of Contemporary Roman-Dutch Law* 241-255

Nyoni & Velaphi 2015 *SAJIM*

Nyoni P & Velaphi M "Data protection law and privacy on Facebook" 2015 *South African Journal of Information and Management* 1-10 available at <http://dx.doi.org/10.4102/sajim.v17i.636> (date of use: 14 January 2017)

Oliver 2002 *ILJ*

Oliver H "Email and internet monitoring in the workplace: Information privacy and contracting-out" 2002 (31) *Industrial Law Journal* 321-352

Palmer 2007 *CLJ*

Palmer S "Public, private and the Human Rights Act 1998: An ideological divide" 2007 *Cambridge Law Journal* 1-12

Pienaar 1998 *PER*

Pienaar GJ "Constitutional provision regarding juristic persons" 1998 (1) *Potchefstroomse Elektroniese Regblad* 1-15

Pistorius 2009 *PER*

Pistorius T "Monitoring, interception and the big boss in the workplace: Is the devil in the details?" 2009 (12) *Potchefstroomse Electroniese Regblad* 1-24

Roos 2006 *CILSA*

Roos A "Core principles of data protection law" 2006 *Comparative and International Law Journal for Southern Africa* 102-130

Roos 2012 *SALJ*

Roos A "Privacy in the face-book era: A South African legal perspective" 2012 (129) *South African Law Journal* 375-402

Roos 2007 *SALJ*

Roos A "Data protection: Explaining the international backdrop and evaluating the current South African position" 2007 (124) *South Africa Law Journal* 400-434

Sakrouge, Minett & Preisked 2011 (8) *Computer and Telecommunications Law Review*

Sakrouge A, Minett K & Preisked D Monitoring employee communications: data protection and privacy issues 2011 (8) *Computer and Telecommunications Law Review* 213- 216

Warren & Brandeis 1890 *Harvard L Rev*

Warren S & Brandeis D "The right to privacy" 1890 (4) *Harvard Law Review* 193-220

Terle 2007 *CLSR*

Terle M "Freedom of information and data protection law - A conflict or reconciliation?" 2007 *Computer Law and Security Report* 514-522

JUDICIAL DECISIONS

South Africa

Barmford v Energizer SA Limited 2001 12 BALR 1251 (P)

Bernstein v Bester NO 1996 (2) SA 751 (CC)

Financial Mail (Pty) Ltd v Sage Holdings Ltd 1993 SA 451 (A)

Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd 2001 (1) SA 545 (CC)

Kidson v SA Association Newspapers Ltd 1957 (3) SA 461 (W)

NM v Smith 2007 (5) SA 250 (CC)

O'Keeffe v Argus Printing and Publishing Co Ltd and Others 1954 (3) SA 244 (C)

S v A 1971 (2) SA 293 (T)

S v Manamela 2000 (1) SACR 414 (CC)

S v Naidoo (1998) 1 BCLR 46 (D)

Seglogelo v Seglogelo 1914 AD 211

CCMA cases

Gouws v Score/Price & Pride Furnishers 2001 11 BALR 1155 (CCMA)

Moonsamy v The Mailhouse (1999) 20 ILJ 464 (CCMA)

Warren Thomas Griffiths v VWSA Case NO EC 16714 unreported (CCMA 22 June 2000)

United Kingdom and European Court of Human Rights

Bărbulescu v Romania (61496/08) [2016] IRLR (ECHR)

Douglas v Hello Ltd [2001] 1 FLR 982 CA

Goodwin v United Kingdom 22 Eur Ct HR (ser A) [123] 1996

Halford v United Kingdom (20605/92) [1997] IRLR 471, (1997) 24 EHRR 523

Malone v United Kingdom WL 215891 (Eur Comm HR) (1983) 5 EHRR 385

CONSTITUTION

Constitution of the Republic of South Africa, 1996

LEGISLATION

South Africa

Basic Conditions of Employment Act 75 of 1997

Electronic Communications Transaction Act 25 of 2002

Employment Equity Act 55 of 1998

Interim Constitution of the Republic of South Africa Act 200 of 1993

Labour Relations Act 66 of 1995
Promotion of Access to Information Act 2 of 2000
Protection of Personal Information Act 4 of 2013
Public Services Act 103 of 1994

United Kingdom

Contempt of Court Act 1981
Human Rights Act 1998
Data Protection Act of 1998
Privacy in the Regulations of Investigatory Powers Act 2000
Regulation of Investigatory Powers Act 2000

INTERNATIONAL DATA PROTECTION INSTRUMENTS

Council of Europe

European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos 11 and 14, 4 November 1950 ETS 5

Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data No 108/1981

Organisation for Economic Cooperation and Development

Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data, Paris 23 September 1980

Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy 12 June 2007

European Union

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, 1998

Regulation 2016/679 on the protection of natural persons with regard to the processing of data and on the free movement of such data (General Data Protection Regulation)

Art 29 DP WP Opinion 2/2017 on Data Processing at Work WP 249 8 June 2017

United Nations

UN General Assembly Universal Declaration of Human Rights 10 December 1948

African Union

Convention on Cyber Security and Personal Data Protection 2014

THESES AND DISSERTATIONS

Chigumba *Employee's Right to Privacy*

Chigumba P *The Employee's Right to Privacy versus the Employer's Right to Monitor Electronic Transmissions from the Workplace* (LLM dissertation University of Kwazulu Natal 2013)

Godwe Protection of Privacy

Godwe *The Protection of Privacy in the Workplace: A Comparative Study* (LLD thesis University of Stellenbosch 2011)

Mabeka Conduct of the Employer

Mabeka NQ *When does the Conduct of the Employer infringe on an Employee's Constitutional Right to Privacy when Interpreting or Monitoring Electronic Communications?* (LLM dissertation University of the Western Cape 2008)

Naude Data Protection in South Africa

Naude A *Data protection in South Africa: The impact of the Protection of Personal Information Act and recent International Developments* (LLM short dissertation University of Pretoria 2014)

Padayachee C Employee's Right to Privacy

Padayachee C *Employee's Right to Privacy versus Employer's Right to Monitor Electronic Communication in the workplace* (LLM Dissertation University of Kwa-zulu Natal 2015)

Roos Data (privacy) Protection

Roos A *The Law of Data (privacy) Protection: A Comparative and Theoretical Study* (LLD Thesis University of South Africa 2003)

Skosana Privacy and Identity

Skosana MT *The Right to Privacy and Identity on Social Network Sites: Comparative Legal Perspective* (LLM Dissertation University of South Africa 2016)

OTHER SOURCES

South African Law Reform Commission “Privacy and Data Protection Project 124”
Discussion Paper 109 (2005)

International Labour Organisation Code of Practice: Protection of Workers’ Personal Data
(1997)

INTERNET SOURCES

The Employment Practices Code (2011) available at
https://ico.org.uk/media/fororganisations/documents/1064/the_employment_practices_code.pdf.

<http://www.gamingtechlaw.com/2016/09/privacy-portability-right-industry>.

PROFESSOR NEVILLE BOTHA

B Juris, LLB (Pret) LLD (Unisa)

Professor Emeritus, School of Law University of South Africa

Advocate of the High Court

South African Representative Permanent Court of Arbitration

Editor: Annual Survey of South African Law

South African Mercantile Law Journal

Comparative & International Law Journal for Southern Africa

Cel: 082 820 1414

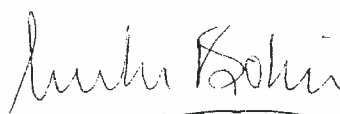
Tel: 012 362 0376

e-mail: Neville.Botha7@gmail.com

12 September 2018

TO WHOM IT MAY CONCERN

I hereby confirm that the LLM dissertation entitled: **LEGAL PRINCIPLES REGULATING THE PROCESSING OF PERSONAL INFORMATION IN THE WORKPLACE** submitted by UNATHI PEARL NXOKWENI (Student number 43803873) has been fully edited in accordance with the requirements of the University.

 Prof Neville Botha